Iot Based Smart Wallet Security and Fake Currency Detection System

P. Vijayakumar, Saravanan G, Adithya Narayan, Deepak B, Ragul S, Tamilselvi, Rajashree. R, T. Poongkuzhali, Xiao-Zhi Gao

Abstract: The main objective is to create a security system for wallet based on RFID technology and also keep an account of how much money is coming inside and going out of the wallet which is done using tcs3200 colour sensor by which we can have an account of the amount of money spent and update the same on the mobile app. So, this project basically alerts the person if the wallet is missing from his/her pocket and also shares the location of the same and also gives the information of how much he/she has spent. The major components used in this paper include Raspberry PI, RFID Reader, RFID Tag, GPS Module, and TCS3200 Colour Sensor. Whenever the RFID card is placed near to the reader, the RFID reader obtains the UID (unique key) information about the card. The location of the wallet is obtained using the GPS Module. This detail is notified to user when the wallet is not connected. The status obtained by the RFID reader and the GPS module is collected by Raspberry PI. Using the PI's WIFI, the details are posted onto the cloud. All the details posted onto the cloud are accessed via the APP and also through a website portal in case of any emergency

Keywords: RFID Technology, Cloud, Android App, WIFI, Raspberry Pi, Internet of Things, Wallet, Fake currency detection method.

I. INTRODUCTION

In today's world of smart living, the smart wallet, presented in this paper, provides a better solution to keep track of our precious possessions and monitoring them in real time. As the world moves towards a tech-savy direction, the novel smart wallet system discussed here facilitates the user to perform location tracking, cash flow monitoring, presence monitoring etc in one device. The innovative design combines the technology such as RFID technology and the cloud computing to monitor the status of the wallet in real time. An emergency alert system is also developed and is integrated with an Android application with a user interface. Smart wallet system is composed of two independent modules, the reader module and the RFID based

P. Vijayakumar, Associate Professor, Vellore Institute of Technology, Chennai, Tamilnadu, India.(email: vijayrgcet@gmail.com)

Saravanan G, UG Student, Vellore Institute of Technology, Chennai, Tamilnadu, India.

Adithya Narayan, UG Student, Vellore Institute of Technology, Chennai,Tamilnadu, India.

Deepak B, UG Student, Vellore Institute of Technology, Chennai,Tamilnadu, India.

Ragul S, UG Student, Vellore Institute of Technology, Chennai,Tamilnadu, India.

Tamilselvi, Senior Lecturer, T.S Srinivasan Centre for Polytechnic and Advanced Training, Chennai,Tamilnadu, India.

Rajashree. R, Assistant Professor, Dr. SJS Paul College of Engineering & Technology (Former), Puducherry,Tamilnadu, India.

T. Poongkuzhali, Assistant Professor, Sri Ganesh College of Engineering & Technology (Former), Puducherry,Tamilnadu, India.

Xiao-Zhi Gao, Professor, University of Eastern Finland, Finland.

authentication module. Whenever the RFID authentication module is placed within the vicinity of the reader module, a safe signal (status signal) is generated by the Raspberry Pi and is sent to the Firebase [1] (Real time cloud database). This status is then retrieved by the Android app [3] and the status is displayed via a user interface. If the reader module is not placed within the vicinity, an alert status is sent to the firebase; this is again retrieved by the Android app and is displayed with an emergency notification. When the app gets an alert signal, it further fetches information about the tracking location of the wallet which is provided by the GPS module attached to the wallet. Other feature of Smart Wallet system is the cash flow monitoring which is employed with the Colour sensor module and Pi. An infrared sensor is used to check if there is any flow of cash from outside the wallet. When the infrared sensor is triggered, the Colour sensor is switched on and the Colour code is sensed. If the Colour code is within the range of a particular kind, then it is added to the balance of the user. The details of the cash flow are also posted on the app dashboard. The rest of the paper is organised as follows, Section II presents the related works pertaining to real time smart security. Section III presents the proposed methodology and the Section IV briefs about the components used in the proposed novel Smart Wallet.The procured results are included in Section V..

II. RELATED WORKS

Kamesh Santhanam [8] describes physical mechanisms to detect fake currency. In this paper to detect fake currency the author has used two step verification; one is with ultraviolet light and the other is by using polarization property of light. In both the methods, a beam of light is projected onto the currency and based on the resultant beam, the currency is differentiated. Only if the result of both the methods are positive the given currency is regarded as genuine or else its fake. Rathee [9] describes the use of image processing for the identification of fake notes. In this paper, an image processing algorithm has been developed to extract features of the currency note like the security thread, intaglio printing, all these features are weighted based on pre-set decision scores. The cumulative of the feature extraction is then compared with a threshold, based on that the result of whether the note is fake or real is inferred. The author has used root mean square (rms) error to evaluate their system which yielded only 1%. Murthy [10] also describes the use of

image processing algorithms for the identification of fake notes. In this paper, the author proposes a system where the images of real note are stored as reference notes. Also, all the parameters of the reference note are calculated. When an image is read by the system, it is pre-processed for the system to extract only the note portion and is compared with the reference notes. This process is repeated for both sides of the note to check for any counterfeit. The major advantage of this system is that it has low system complexity and low processing time. Darade [7] has described image segmentation models for the identification of fake notes. In this paper, the apply proposes the system which consists of the following operations; converting the image into grey scale image, the edges of the images are calculated to find the boundaries in the image, based on that the image is segmented. The features of the final version of the segmented images are extracted and it is compared with the already stored feature details of the reference data, when the result of comparison is greater than a threshold, a decision is made on whether the given note is fake or real.

Sakalauskas [2] has proposed an effective realization for an e-wallet system, the proposed system uses Elgamal Asymmetric Encryption Scheme for digital signatures generation and verification. SHA 256 algorithm is used for defining Payment parameters. Also, in this paper various cryptographic functions which might be used for the realization of e-wallet system has been tested for satisfying general security requirements. Ma [1] has described the application of human verifiable authentication schemes with respect to the smart wallet. According to the proposed system, a human verifiable authentication scheme is embedded into the wallet that is used to communicate between the smart wallet application and the smart wallet payment server. The proposed process consists of the following steps; key setup – when the connection is established between the applications a session key is created. Then the user selects the authentication scheme for handshaking. Payment completion is also done using these keys created. This paper has demonstrated the secure session technique for smart wallets. Paper [3] had discussed about the development of a smartcard system, which consists of two parts: Card Management System (CMS) and Application Management System (AMS). This CMS implements the Public Key Infrastructure (PKI) to ensure data security, also completes the life cycle of smart cards. The card management system and card application systems share one centralize database. The application management system had developed allows multi-application to be added to the card. Also, the three applications implemented are: identification, e-wallet, and access control. In paper [4], Akram had proposed a framework which enables a user to acquire a new smart card as she desires where she can migrate, restore, can access over all of her applications. The recovery of a smart card-based service will take a day to a week, within this time the service provider may lose his/her access from the user because they won't be able to access the respective services. So basically, she can recover from her lost digital wallet in a secure, efficient, seamless and ubiquitous manner. In paper [6], Yavuz discusses about the e-voting using blockchain with the smart contracts. It is used in the developments of safer, cheaper, more secure, more transparent systems. Ethereum and its network is considered to be the most suitable one, due to its consistency, and provision of smart contracts logic. They have implemented and tested a sample e-voting application as a smart contract for the Ethereum network using the Ethereum wallets and the Solidity language, where an Android platform is considered to allow voting for people in absence of an Ethereum wallet. This method is a transparent way for e-voting.

III. TRADITIONAL WALLET SECURITY AND FAKE CURRENCY DETECTION SYSTEM

In the system [2], the author demonstrates the security using two parts of electronic circuitry; one part is a small and elongated magnet which is placed in the wallet. The other part is the electronic circuitry and audio producing device in which the circuit activating switch is held open as long as the wallet with its magnet is in proximity to the second part. When the wallet and the signalling device are separated sufficiently, the magnet no longer holds the activate switch open and the switch closes thus producing the audio signal. The drawback of this system is it is entirely dependent on the physical circuitry, which could easily be broken by the intruders

IV. PROPOSED SMART WALLET SECURITY AND CURRENCY DETECTION SYSTEM

The proposed system will operate in two mode of operations. First system is used to protect the wallet using RFID technology and second system is used to detect the currency value using color sensor technology as shown in Fig.1 and Fig. 2 respectively.

3.1 Smart Wallet Security System

For wallet protection, RFID technology is used where a RFID reader is placed in the pocket and an authenticated corresponding tag is given to the user and is placed in the wallet itself. The RFID reader is connected to the Raspberry PI. Whenever the tag is nearby the reader and is authenticated i.e. UID of the tag matches with issued tag's UID a "Connected" signal is posted onto the cloud (Firebase). Whenever the RFID reader senses no tag or unauthorised tag, a "Missing" signal is posted onto the cloud along with the live location of the Wallet using the GPS module connected to the Wallet. These details are then retrieved by a mobile app indicating the status of the wallet, if a wallet is found missing, a notification is also given to the user.
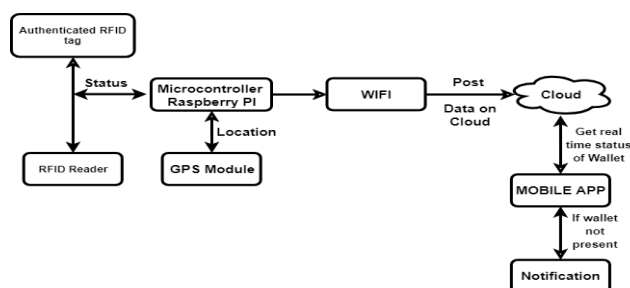

Fig. 1 Smart Wallet Protection System

The following components are involved in the smart wallet security system to protect the wallet from the theft and it also gives the alert through mobile app: Raspberry PI , RFID Reader and Tag, IR Sensor, RGB Sensor, Firebase – Cloud, GPS and Android Mobile app interface

RFID: The RFID system consists of two devices (i.e) reader and a tag. The tag is attached to the object that is to be identified. The read and write functionality contained by the tag make the data stored on RFID tag to be updated and protected. The reader consists of a signal transmitter and receiver. The RFID reader transmits carrier signals and receives backscattered signals from the tag via their antennas; this is the underlying operation behind this system.

Raspberry PI : The proposed system employs a Raspberry PI model B board [4]. It is based on the ARM Cortex-A53 processor and acts as the brain of the proposed system. It is a credit card sized minicomputer. Raspberry pi board includes a 40 pins header consisting of 26 General Purpose Input Output (GPIO) pins, two 5v pins, two 3.3v pins, 8 ground pins and two ID EEPROM pins. We have utilised SDA, SCK, MOSI, MISO, GND, RST and 3.3v pins to setup connections with RFID reader.

GPS: GPS stands for Global Positioning System and used to detect the Latitude and Longitude of any location on the Earth, with exact UTC time (Universal Time Coordinated). GPS module is the main component in our vehicle tracking system project. This device receives the coordinates from the satellite for each and every second, with time and date.

3.2 Smart Currency Detection System

For the Currency Detection feature, we use two modules: RGB Sensor and Laser Diode. Two laser diodes (Infrared) are used, when the currency notes enter, the first laser gets cut followed by the second one which indicates it's coming inside the wallet and vice versa for going out of it, we add the value in the first case and deduct it from the total amount when it goes out. And the RGB sensor which is basically a colour sensor reads the denomination by decoding to the value of red, green and blue in tandem. If a currency is found, the detail of the currency is fetched and is updated in the cloud database (Firebase) through the PI's WIFI connection. The updated data is then retrieved by Mobile APP and relevant analytics of money spent is shown to the user as shown in Fig. 2.
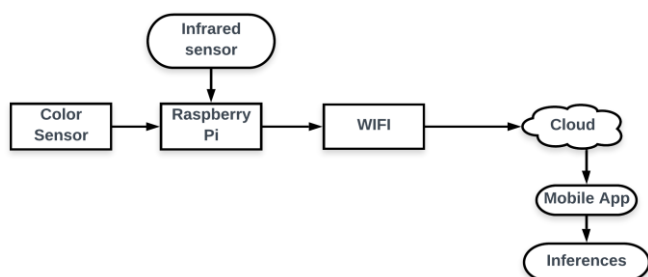
Fig. 2. Flow of currency detection module

Color Sensor:

The color sensor is used to detect a wide variety of colors mainly red, green, and blue based on their wavelength. TCS230 color sensor module is being used in the proposed system for the identification of currency notes.

Raspberry Pi :

The proposed system employs a Raspberry PI model B board [4]. It is based on the ARM Cortex-A53 processor and acts as the brain of the proposed system. It is a credit card sized minicomputer. Raspberry pi board includes a 40 pins header consisting of 26 General Purpose Input Output (GPIO) pins, two 5v pins, two 3.3v pins, 8 ground pins and two ID EEPROM pins. We have utilised SDA, SCK, MOSI, MISO, GND, RST and 3.3v pins to setup connections with RFID reader.

Infrared Sensor :

An infrared sensor is an electronic device that emits in order to sense some aspects of the surroundings. An IR sensor can measure the heat of an object as well as detects the motion. These types of sensors measure only infrared radiation, rather than emitting it that is called as a passive IR sensor.

IV. RESULTS AND DISCUSSION

4.1 Hardware Implementation

Fig. 3 shows the implemented hardware connections of the Smart Wallet Security system, this system when connected to WIFI transmits the GPS and the RFID status to the cloud i.e. Firebase and it is then received by the Android App as shown in Fig 3. Similarly, for the currency detection the hardware implementation is shown in Fig.4, as and when the system detects movement of notes, the same is reflected in Firebase and is then received by the Android App as shown in Fig.4.

**Fig. 3 Smart wallet security implementation**
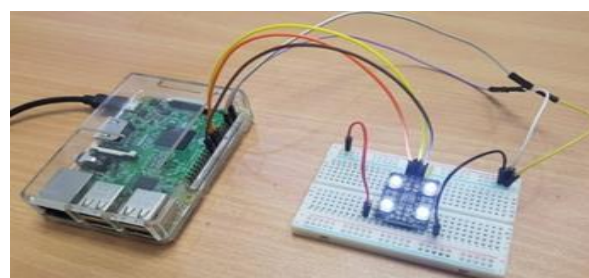
Fig. 4 Currency Detection Implementation

4.2 Cloud Database Scheme

The Firebase database schema is shown in Fig. 5. There are two major entries, last_update and wallet_log. The last_update entry stores the latest uploaded data of the wallet which is shown in the app. And, the wallet_log entry stores

all the updates about the wallet. This could be used for future safety purposes.
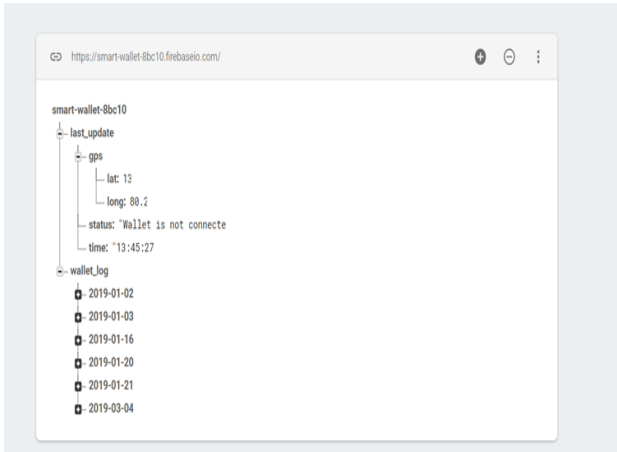
Fig. 5 Firebase Cloud Database schema

*4.3   End User Application*
4.3.1   Smart Wallet Security System

Fig. 6 shows the Android app along with the alert notification. When the authentication module is not placed in the vicinity of reader module, the wallet fetches the alert status from the cloud (Firebase) and is displayed on the app interface as "Wallet in Not connected". Also, the GPS location of the wallet is displayed which could be used to locate the wallet.
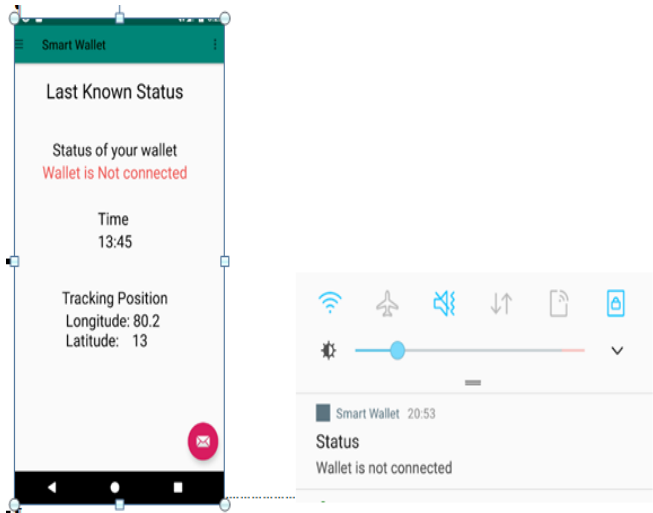
Fig. 6 Realtime status of wallet

4.3.2 Smart Wallet Currency Detection

Fig. 7 shows the Android app which displays the current total amount present in the wallet and the last currency note that was detected by the system. These details are also retrieved from the cloud database which was transmitted by the Raspberry Pi connected with the colour sensor.
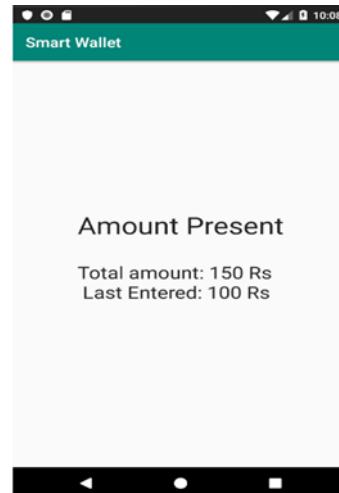
Fig. 7. Currency Status of wallet

The proposed system will improve the security level of the wallet by providing the alarm and also giving the notification about the loss of wallet from the pant packet. RFID card reader helped the system for notification and also GPS will give the location of the wallet in the mobile app. The system also shows the currency status of the wallet and detects the fake currency with the help of color sensor present tin the wallet. The proposed system also incorporates the advantage of Internet of Things with firebase cloud data storage system. It will also give the clear tracking details of amount spent throughout the month or day. The above mentioned features will overcome the existing problems like pickpocketing, robbery and fake rupees notes.

V CONCLUSION

A new system has been developed called the Smart Wallet having two applications, primary one being the security and currency detection, the other. This would help us avoid losing our wallet and if at all we lose, helps us tracking the location of the same. And moreover also helps us keep track of the amount of money we've spent over a period with all required analytics and is displayed in the app.

REFERENCES

1.   G. I. Ma, H. C. Lee, J. H. Yi, H. Ki, D. Choi and S. H. Jin, "Human verifiable authentication schemes geared to smart wallet applications," 2011 IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, 2011, pp. 141-142.
2.   E. Sakalauskas, J. Muleravicius and I. Timofejeva, "Computational resources for mobile E-wallet system with observers," 2017 Electronics, Palanga, 2017, pp. 1-5.doi: 10.1109/ELECTRONICS.2017.7995226
3.   M. Mohandes, "A smart card management and application system," 2010 IEEE International Conference on Progress in Informatics and Computing, Shanghai, 2010, pp. 1220-1225. doi: 10.1109/PIC.2010.5687971
4.   R. N. Akram, K. Markantonakis and K. Mayes, "Recovering from a Lost Digital Wallet," 2013 IEEE 10th International Conference on High Performance Computing and Communications & 2013 IEEE International Conference on Embedded and Ubiquitous Computing, Zhangjiajie, 2013, pp. 1615-1621.doi:

10.1109/HPCC.and.EUC.2013.227

5. T. S. Perry, "Electronic money: Toward a virtual wallet," in IEEE Spectrum, vol. 34, no. 2, pp. 18-19, Feb. 1997. doi: 10.1109/MSPEC.1997.570819

6. E. Yavuz, A. K. Koç, U. C. Çabuk and G. Dalk?l?ç, "Towards secure e-voting using ethereum blockchain," 2018 6th International Symposium on Digital Forensic and Security (ISDFS), Antalya, 2018, pp. 1-7.doi: 10.1109/ISDFS.2018.8355340

7. S. R. Darade and G. R. Gidveer, "Automatic recognition of fake Indian currency note," 2016 International Conference on Electrical Power and Energy Systems (ICEPES), Bhopal, 2016, pp. 290-294. doi: 10.1109/ICEPES.2016.7915945

8. Upadhyaya, V. Shokeen and G. Srivastava, "Counterfeit Currency Detection Techniques," 2018 8th International Conference on Cloud Computing, Data Science & Engineering (Confluence), Noida, 2018, pp. 394-398.

9. N. Rathee, A. Kadian, R. Sachdeva, V. Dalel and Y. Jaie, "Feature fusion for fake Indian currency detection," 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, 2016, pp. 1265-1270.

10. S. Murthy, J. Kurumathur and B. R. Reddy, "Design and implementation of paper currency recognition with counterfeit detection," 2016 Online International Conference on Green Engineering and Technologies (IC-GET), Coimbatore, 2016, pp. 1-6.

11. M. S. Uddin, P. P. Das and M. S. A. Roney, "Image-based approach for the detection of counterfeit banknotes of Bangladesh," 2016 5th International Conference on Informatics, Electronics and Vision (ICIEV), Dhaka, 2016, pp. 1067-1072.

12. Google Firebase, http://firebase.com

13. Tommasini, Giorgio. "Wallet anti-theft device." U.S. Patent No. 4,780,704. 25 Oct. 1988.

14. https://developer.android.com/training/basics/firstapp/index.html

15. https://www.raspberrypi.org/