ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 2, March 2018

Credit Card Forgery Using Multilevel Authentication Based on POS

V.P. Gladis Pushuparathi[1], P.Dhoshini[2], N.D.Sangeetha[2], A.Sindhuja[2]

Associate Professor, Department of Computer Science and Engineering, Velammal Institute of Technology. Chennai, Tamil Nadu, India[1]

UG Student, Department of Computer Science and Engineering, Velammal Institute of Technology, Chennai, Tamil Nadu, India[2]

UG Student, Department of Computer Science and Engineering, Velammal Institute of Technology, Chennai, Tamil Nadu, India[2]

UG Student, Department of Computer Science and Engineering, Velammal Institute of Technology, Chennai, Tamil Nadu, India[2]

ABSTRACT: Credit card forgery is one of the major ethical issue in credit card industry. As credit card becomes the most popular mode of payment for both online as well regular purchase. Credit card frauds are increasing day by day regardless of the various techniques developed for its detection. Hackers are so expert that they are new ways for committing illegal transactions each day which demands constant innovation for its detection techniques as well. Credit card fraud occurs when user's card is stolen by the unknown persons, that information can be used for unauthorized online purchase and some other situation. A technique is required to detect such events. Many techniques are existing to detect such frauds. One of the technique used is skimming. When a credit or debit card is swiped through a skimmer, the device captures and stores all the details stored in the card's magnetic stripe. The stripe contains the credit card number and expiration date and the credit card holder's full name. Thieves use the stolen data to make fraudulent charges either online or with a counterfeit credit card. But these existing techniques are not efficient to provide better performance to detect such credit card fraud events. In the proposed system, rather having multiple sensors integrated output in one process, which is actually time consuming, RFID with fingerprint for any online and Point Of Sale based payment system for E-Commerce are implemented. One Time Password and multilevel authentication are used for tracking user's location. Payment is made to the receiver only if both the user's card and mobile are in the same location. This paper will avoid payment is made by attackers when credit or ATM card is lost.

KEYWORDS: Location tracking, RFID, Fingerprint Sensor

I. INTRODUCTION

Credit card forgery is made frequently when our card is theft by someone or if someone know our pin number. So more number of possibilities are there to made fraud on our card, for that we are implementing a new system to secure our card through IOT. The Internet of Things (IoT) was of a vision in which all physical objects are tagged and uniquely identified using RFID transponders or readers. In our system we are using RFID card to fetch the card number through the RFID reader. When the user shows the card on the reader value will be pass through the cable to our local system. The hardware of project requires different power supplies. 5 v. the interfacing devices will get the supply from main microcontroller through the keypad matrix we are giving pin number to register the pin. On each key pressed on a keypad, the index of the key is passed to a user-defined function.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 2, March 2018

User is free to define what to be done with the input.LCD (Liquid Crystal Display) screen is an electronic display module and find a wide range of applications. A 16x2 LCD display is very basic module and is very commonly used in various devices and circuits. A 16x2 LCD means it can display 16 characters per line and there are 2 such lines. In this LCD each character is displayed in 5x7 pixel matrix. This LCD has two registers, namely, command and data. LCD is the display to show card number on the board. When we show the card on the reader value will be show on the LCD board. PIC control board is entire hardware which will connect with the keypad matrix to get the values from the user. It is high performance RISC CPU machine. ONLY have 35 simple word instructions. Operating speed: clock input (200MHz), instruction cycle (200nS).Up to 368×8bit of RAM (data memory), 256×8 of EEPROM (data memory), 8k×14 of flash memory. Wide operating voltage range (2.0 – 5.56) volts.2 8 bit timer and one 16 bit timer is available 10bit multi-channel A/D converter synchronous serial Port (SSP) with SPI (master code) and I2C (master/slave). 100000 times erase/write cycle enhanced memory. 1000000 times erase/write cycle data EEPROM memory. After the verification of the pin number and POS purchase will be made. Through the OTP verification location will be get and to the server and match it with the POS, if it valid purchase will made.

II. LITERATURE REVIEW

In 2017, SanketGoyal[1], et al proposed a model to develop a multilevel security system. To reach or access innermost circle, three stages of security system endorsement will be necessary, making it the primary level of security. The valuables in the inner vault are further secured with a secondary system completely separate from the primary, consisting of a fingerprint scanner. Any security breach detected will alert the authorities with the help of a GSM shield, therefore taking the necessary response immediately. Continuous surveillance with online streaming is also demonstrated using raspberry pi and a digital camera, further safeguarding the valuables.

In 2015, P.Vigneswari[2], et al used raspberry pi board which itself acts as a mini computer. Whenever a person enters into the room, the fans and light will automatically switch on. At the same time camera is also switched on and it takes the image of the person who has interrupted. The user is alerted by sending an SMS with the link using GSM modem. The image can be viewed by clicking on this link. In the absence of a person the fans and lights will automatically be switched off.

In 2014, S.Prasad[3], et al proposed home security system captures information and transmits it via a 3G dongle to a smart phone using web application. Raspberry pi operates and controls motion detectors and video cameras for remote sensing and surveillance, streams live video and records it for future playback. It can also find the number of persons located with the help of the Infrared sensor.

In 2014, K.Gopalakrishnan[4], et al proposed an image capturing technique in an embedded system based on raspberry pi board. Considering the requirements of image capturing and recognition algorithm, raspberry pi processing module and its peripherals, implementing based on this platform, finally actualized embedded image Capturing using Raspberry pi System (EICSRS). Experimental results show that the designed system is fast enough to run the image capturing, recognition algorithm, and the data stream can flow smoothly between the camera and the raspberry pi board.

In 2013, Galibkalal[5], et al Patil proposed smart phones can communicate to any other devices in an ad-hoc network with a connectivity options like bluetooth or Wi-Fi etc. Different devices and the appliances in the home like lightings, fan, home security and motor are now being connected to the Internet so that it can be controlled remotely using the smart phones or tablets. Not only devices can be controlled, but home environment can also be continuously monitored for maintaining certain desired temperature or monitoring amount of energy consumption.

In 2011, V.P.GladisPushparathi[6], et al proposed video surveillance system, video streams from cameras are sent to a control centre and operators monitor the videos. But human operator monitoring of the views every moment of every day is almost impossible; Mobile video surveillance represents a new paradigm that encompasses, on the one side,

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 2, March 2018

video acquisition and, on the other side, especially at the same time image viewing, addressing both computer-based and mobile-based surveillance.

Some of the demerits from the above mentioned paper are enhanced capability of adversaries, electronic systems are now increasingly vulnerable to counterfeiting and piracy. Poorly designed objects, absence of policies or lack of control over the location disclosure mechanism enable untrusted entities to obtain the location of another entity.The voice alarm circuit not added to this system.

III. PROPOSED SYSTEM

Multi-level security is implemented to reduce the credit card forgery. These include the Hex Keypad, Bluetooth, and RFID. Multiple sensors integrated output in one process, which is actually time consuming, RFID with fingerprint is implemented for any online or POS based payment system. OTP is also verified from the android application of the user so as to track the location of original user. Payment is made to the receiver only if both the user's card & mobile are in the same location. This system will avoid payment is made by attackers when credit or ATM card is lost. The fig.3.1. showsthat user will give the finger print on the finger print sensor. And that value will be send the cable we used and that value will be displayed on the screen. And user will give the PIN number through the keypad matrix and OTP will server and location of both place will fetch and confirm the location and transaction.

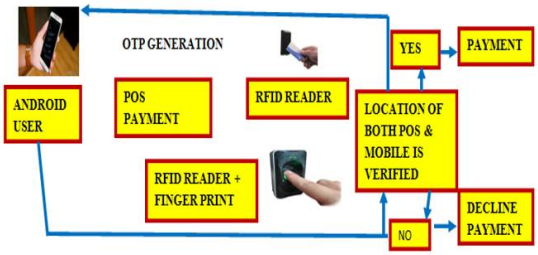


Fig.3.1.Architecture Diagram

A. User Registration

User registration is for authentication purpose to verify whether he is the original user. Users have to register their details in android application. Users have to give their name account details and credit card number in application. A registered user is a user of a website, program, or other system who has previously registered. Registered users normally provide some sort of credentials (such as a username or e-mail address, and a password) to the system in order to prove their identity, this is known as logging in. Systems intended for use by the general public often allow any user to register simply by selecting a register or sign up function and providing these credentials for the first time. Registered users may be granted privileges beyond those granted to unregistered users.

B. Main Server

A server is a computer program running to serve the requests of other programs to the clients. Thus, the server performs some computational task on behalf of clients. The clients either run on the same computer or connect through the network. Here the server will store all the user's information in the database. In the server, the detection sensors are connected, so that they can control. Also the server will monitor all the user access. The server will also store the user access details in the database. It will monitor the user movement and transaction.

C. POS Hardware Setup

POS is Point Of Sale which means where the purchase is made by user. Here the user will give their pin number machine (keypad matrix) by showing RFID card or fingerprint on machine. Keypad id is verified by the server

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 2, March 2018

then after that verification OTP is send to the user mobile. If it is not correct transaction will not occur. Fingerprint scanners generate an image of the ridges and valleys that make up a fingerprint. But instead of sensing the print using light, the capacitors use electrical current.

D. Android Application

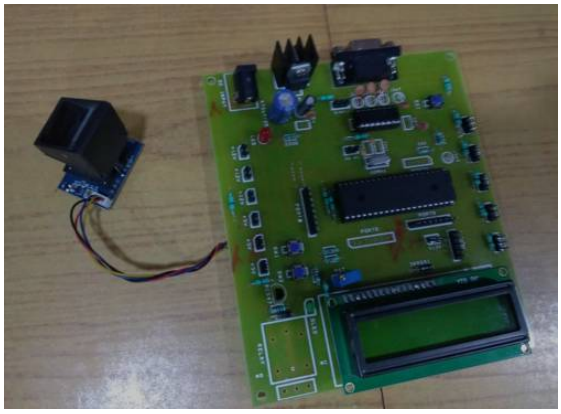
The android application is to verify the user whether he/she is the authorized person. User have to give the OTP on mobile application, then the current location will taken from application and send it to the server.

E. Hardware and Software Verification and Transaction

Here the both hardware and software is verified by the server to check whether the user is authorized person. Once the location send from the mobile and location of purchase made by the person is matched then the transaction will successfully made.

IV. RESULTS

The fig.4.1. Shows that the device is connected with a fingerprint sensor and with a keypad matrix with in single device. When the user gives their fingerprint in the fingerprint sensor system, it will fetch the fingerprint of the user and check this fingerprint with the existing fingerprint and verify it and made transaction successfully.



The fig.4.1. Shows that the device is connected with a fingerprint sensor and with a keypad matrix with in single device. When the user gives their fingerprint in the fingerprint sensor system, it will fetch the fingerprint of the user and check this fingerprint with the existing fingerprint and verify it and made transaction successfully.

After that an OTP is generated. The generated OTP is sent to the registered mobile number of the user through SMS and user have to enter that OTP in the keypad matrix. When the OTP is sent to the user's registered mobile number the server will fetches the location of the user and it will be transferred to the server. POS location and the location of the user should be same, it should be verified by the server and the amount will be transferred from the user account to the merchant account.

V. CONCLUSION

Credit card forgery is commonly happening to avoid this method is effective using this no one can use the users card without his/her knowledge Thus the paper represents that maximum level of card forgery is reduced by this method. Point of Sale (POS) process will verify the card transaction from where the sale was made.Through this an effective method was identified by the application for credit card forgery.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 2, March 2018

REFERENCES

[1] SanketGoyal, Pranali Desai, and VasanthSwaminathan,"Multi-Level Security Embedded With Surveillance System,"*IEEE Sensors Journal.*, vol. 17, no. 22, pp.7497-7501, Nov.2015.
[2]P. Vigneshwari, V. Indhu, R. R. Narmatha, A. Sathinisha, and J. M. Subashini, "Automated security system using surveillance," *Int. J. Current Eng. Technol.*, vol. 5, no. 2, pp. 882–884, Apr. 2015.
[3]S. Prasad, P. Mahalakshmi, A. J. C. Sunder, and R. Swathi, "Smart surveillance monitoring system using raspberry PI and PIR sensor," *Int. J. Comput. Sci. Inf. Technol.*, vol. 5, no. 6, pp. 7107–7109, 2014.
[4]K. Gopalakrishnan, V. S. Kumar, and G. Senthilkumar, "Embedded image capturing system using raspberry pi system," *Int. J. Emerg. Trends Technol. Comput. Sci.*, vol. 3, no. 2, pp. 213–215, Apr. 2014.
[5]A.R. Al-Ali and M. Al-Rousan, "Java-based home automation system", IEEE Transactions on Consumer Electronics, vol. 50, no. 2, pp. 498-504, 2004.
[6]V. P. GladisPushparathi and P. Rajkumar "Motion detection system based interactive surveillance system for mobile clients," IPCSIT., vol.4,pp.177-181, 2011.
[7] V. K. Sadagopan, U. Rajendran, and A. J. Francis, "Anti theft control system design using embedded system," *Proc. IEEE*, Jul. 2011, pp. 1–5.
[8] R. Piyare, "Internet of Things: Ubiquitous home control and monitoring system using Android based smart phone," *Int. J. Internet Things*, vol. 2, no. 1, pp. 5–11, Mar.2013.
[9] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, "Internet of Things: Vision, applications and research challenges," *Ad Hoc Netw.*, vol. 10, pp. 1497–1516, Sep. 2012.
[10] D. Shah and V. Bharadi, "IoT based biometrics implementation on raspberry Pi," *Proc. Comput. Sci.*, vol. 79, pp. 328–336, Mar. 2016.
[11] P. Kumar and P. Kumar, "Arduino based wireless intrusion detection using IR sensor and GSM," *Int. J. Comput. Sci. Mobile Comput.*, vol. 2, no. 5, pp. 417–424, May 2013.
[12] A. Jacobsson, M. Boldt, and B. Carlsson, "A risk analysis of a smart home automation system," *Future Generat. Comput. Syst.*, vol. 56, pp. 719–733, Mar. 2016.
[13] N. K. Sonawane, P. D. Wwaghchavre, and K. A. Patel, "Bluetooth based device automation system using cellphone," *Int. J. Comput. Appl. Inf. Technol.*, vol. 7, no. 1, pp. 136–141, Oct./Nov. 2014.
[14] S. Kumar, "Ubiquitous smart home system using Android application," *Int. J. Comput. Netw. Commun.*, vol. 6, no. 1, pp. 2–3, Jan. 2014.
[15] A. C. Sari, A. Rahayu, and W. Budiharto, "Developing information system of attendance and Facebook status for Binus University's lecturer using raspberry pi architecture," *Proc. Comput. Sci.*, vol. 59, pp. 178–187, Mar. 2015.
[16] M. N. Jivani, "Gsm based home automation system using app-inventor for Android mobile phone," *Int. J. Adv. Res. Elect., Electron. Instrum. Eng.*, vol. 3, no. 9, pp. 12121–12128, Sep. 2014.
[17] V. Vujovi´c and M. Maksimovi´c, "Raspberry pi as a sensor Web node for home automation," *Comput. Elect. Eng.*, vol. 44, pp. 153–171, May 2015.
[18]D. Javali, M. Mohsin, S. Nandanwar, and M. Shingate, "Home automation and security system using Android ADK," *Int. J. Electron. Commun. Comput. Technol.*, vol. 3, no. 2, pp. 382–385, Mar. 2013.
[19]Dhawan, S. Thakur, Aditi Sharma, "Voice Recognition Wireless Home Automation System Based On Zigbee", *IOSR Journal.*, vol. 6, no. 1, pp. 65-75, Mar.2013.
[20]B. Yukesekkaya, A. A. Kayalar, M. B. Tosun, M. K. Ozcan, A. Z. Alkar, "A GSM Internet and Speech Controlled Wireless Interactive Home Automation System", *IEEE Transactions on Consumer Electronics*, vol.52, pp. 837-843, Aug. 2006.