Effective Credit Card Forgery Prevention Using Multilevel Authentication

1M. AJAY CHOWDARY
U.G Student, Department of Computer Science & Engineering
Sathyabama Institute of Science and Technology, Chennai, India
ajayazu9@gmail.com

2M. KUNDAN
U.G Student, Department of Computer Science & Engineering
Sathyabama Institute of Science and Technology
Chennai, India
pranjaldhar234@gmail.com

3DR. A. VIJI AMUTHA MARY
Assistant Professor, Department of Computer Science & Engineering
Sathyabama Institute of Science and Technology
Chennai, India
vijiamumar@gmail.com

Abstract. In the present system, credit card forgery is frequently happening, there is no big security is implemented at all. In the proposing system, Multi level security is implemented. It includes the Hex Keypad, GPS, and RFID. The secure information inside can be further secured with secondary system that consisting of formal fingerprint scanner. Modifying process is our Implementation, rather having multiple sensors integrated output in one process, which is actually time consuming, and we implement RFID with Keypad Matrix. 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 made by the attackers when Credit card is lost or when your details are hacked.

Keywords. Credit card, Hex Keypad, RFID, GPS, Mobile, OTP.

1. Introduction

Credit card fraud happens every day in various places in a variety of ways. But we can create some obstacles and make it tougher for someone to forgery your cards and card numbers. In this paper, we are proposing Mastercard imitation counteractive action by utilizing multilevel verification by utilizing keypad network, OTP alongside location and RFID. The client should enroll his/her points of interest like Visa number, account number, name, and so on which is put away on the server. While the exchange is in the process the OTP is sent alongside location if the exchange location is coordinated with it then the exchange will be fruitful. This can keep the Visa phony by unapproved people. The figure Fig 1 shows the fraud complaints by the numbers in recent years.
2. Existing System

You will register our details to the bank, when a transaction takes place with our card it connects to the bank server checks details and sends back to the merchant receiver then the transaction will be successful/unsuccessful depending upon the card information sent by the bank server. American Express and Discover are the installments organize and the Visa backer, so they favour charge card exchanges themselves. Visa and MasterCard, nonetheless, don't issue charge cards and should contact the Mastercard backer. The charge card guarantor sends back an approval code for the exchange. On the off chance that your charge card is declined, you won't get a reason for the purpose of an offer, only a message that the card was declined. You'll need to contact your card guarantor specifically to discover why your card was declined. The store's bank sends their interchanges electronically either through the telephone line or through the web. You may have been to a store or eatery and heard the shrieking and static from the charge card terminal speaking with the trader bank. Presently you realize what's happening.

3. Literature Survey

Because of the improved ability of foes, electronic frameworks are presently progressively powerless against falsifying and theft. The larger part of fake frame works today are of a cloned write, which has been on the ascent in the current years. Guaranteeing the security of such frameworks is of extraordinary worry as a foe can make a secondary passage or embed a malware to sidestep security modules. The unwavering quality of such frameworks could likewise be sketchy as the parts utilized as a part of these frameworks might be fake and additionally of mediocre quality. It is of prime significance to create arrangements that can keep a foe from making these non-real frameworks. In this paper, we show a novel framework level common validation approach for both the equipment and firmware. The equipment confirms the firmware by checking the checksum amid the catalyst. Then again, firmware checks the personality of the equipment and can't create amend comes about unless it gets a novel equipment unique mark, which we call as framework ID. We propose two secure conventions, TIDP and TIDS, to develop the framework ID and verify the framework by utilizing this novel ID. We demonstrate that our approach is impervious to different known assaults. [1]

A particular administration of testing, discovery, and shirking must be made to handle the overall episode of fake ICs. The electronic part inventory network has been incredibly influenced by across the board fake occurrences. We introduce a few techniques against fake measures to keep this broad falsifying, and we additionally consider the adequacy and confinements of these hostile to forging systems. [2]
As electronic gadgets wind up omnipresent and interconnected, individuals are progressively depending on coordinated circuits (ICs) for performing security-touchy errands and additionally dealing with delicate data. Another PUF circuit configuration in light of ring oscillators, which has preferences in the simplicity of usage and dependability over beforehand proposed outlines. [3]

4. Proposed System

In the proposing framework, Multi-level security is actualized. These incorporate with the HEX KEYPAD, OTP WITH LOCATION, and RFID. The resources in the internal vault are additionally secured with an optional framework totally isolated from the essential, comprising of a unique finger impression scanner.

Numerous sensors coordinated yield in one process, which is really tedious, we actualize RFID with Keypad Matrix or POS based installment framework. OTP is likewise confirmed from the Android utilization of the client to track the location of the first client. The installment is made to the beneficiary just if both the User’s Card and Mobile are in a similar location. This framework will maintain a strategic distance from installment made by aggressors when a Credit card is lost, copied or hacked.

4.1 User Registration

Users have to register their details in login page. Users have to give their name, account details and credit card number in login page. User registration is for authentication purpose that is to verify whether he is the original user or the other person. This module is shown in Fig 2.

![Smart Bazaar](image)

Fig.2. User Registration of Credit Card

4.2 Main Server

A server is a computer program running to serve the requests of other programs, 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. Also the server will monitor all the user access. The server will likewise store the client get to subtle elements in the database. It will monitor the user movement and transaction.

4.3 Android Application

The android application is for verifying the user whether he/she is the authorized person. User has to give the OTP on mobile application, then the current location will be taken from application and send it to the server along with OTP.
4.4 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 on machine. Key pad id is verified by the server then after verification OTP is send to the user mobile. If it is not correct transaction will be unsuccessful. The setup is shown in Fig 3.

![Fig.3 Hardware Components](image)

4.5 Hardware and Software/Verification &Transaction

Here both the hardware and software are verified by the server to check whether the user is authorized person. Once the location sent from the mobile and location of purchase made by the person is matched, then the transaction is successfully made. The flow diagram is shown in Fig 4 and the architecture diagram of Credit card forgery is shown in Fig 5.

![Fig.4 Flow Diagram of Multilevel Authentication verification](image)
5. Result

By this procedure when the exchange happens both the versatile and exchange place ought to be same then the exchange will be triumphs. In the event that the two areas are diverse, exchange will be a disappointment. While entering OTP from keypad network, the shrouded tag should coordinate alongside the area to finish an exchange.

6. Conclusion

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.

References

[1] SMA: A System-Level Mutual Authentication for Protecting Electronic Hardware and Firmware Ujjwal Guin, Member, IEEE, Swarup Bhunia, Senior Member, IEEE, Domenic Forte, Member, IEEE, and Mark M. Tehrani, Senior Member, IEEE
[2] Asha P, Albert Mayan J, Canessane A (2018),“Efficient Mining of Positive and Negative Itemsets Using K-Means Clustering to Access the Risk of Cancer Patients”, Communications in Computer and Information Science, ICSCS 2018, Kollam, 2018, pp. 373-382.
[3] Albert Mayan, J, Surya B, Pranoy Prabhakar, Princekumar,“Department–Student Library Using Twig Pattern Query Processing Over Admin-User Login Privilege”, Pak. J. Biotechnol. Vol. 13, pp. 489-493, (2016)
[4] Physical Unclonable Functions for Device Authentication and Secret Key Generation G. Edward Suh, Srinivas Devadas 2007, San Diego,
[5] Anti Theft Control System Design Using Embedded System Department of Instrumentation And Control Sri Sai Ram Engineering College Chennai India.
[6] Ubiquitous smart home system using android application Shiu Kumar, Department of Information Electronics Engineering, Mokpo National University, 534-729, Mokpo, South Korea
[7] Albert Mayan J, Anto Praveena M D, Telkar Bharath Rao, Uravakonda Uday Sagar(2018),“Optimized test data generation over suspicious implementation of oracle problem”, IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI-2017), pp. 2559-2563.
[8] “Blood donation and life saver app”, 2017 2nd International Conference on Communication and Electronics Systems (ICCES), Annish Brislin M R, J Albert Mayan, R Aroul Canessane, M R Anish Hamlin, pp. 446 - 451, 2017
[9] Online Toll Gate Payment System using RFID, Viji Amutha Mary A, ARPN Journal of Engineering and Applied Sciences, Vol. 13, No. 13, 2018.
[10] Jabez J, Gowri S, Vigneshwari S, Albert Mayan J and Srinivasulu S (2018), "Anomaly Detection by Using CFS Subset and Neural Network with WEKA Tools", Smart Innovation, Systems and Technologies, Vol. 107, pp. 675–682.

[11] Kamalesh M. D., Albert Mayan J., Felix Y., Sumanth B. S., & Sai Tej B. (2018), "Magrisys: A Smart And Ubiquitous Controlled – Environment Agriculture System ", 2nd International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud), pp: 1-5, 2018