Credit Card Fraud Detection Using Biometric Fingerprint Authentication

Ms. Anju Kumari[1], Ms. Deepti Tamhane[2], Ms. Komal Rani[3], Ms. Ashwini Walunj[4], Prof.Vandana Chavan[5]
Department of Computer Engineering
[1,2,3,4,5] PG Scholar, Dr.D.Y.Patil School of Engineering, India

Abstract- *Establishing the identity of a person is becoming critical day by day in our vastly inter-connected society. People fake their identity and do a lot of illegal scams whose bad impacts can be seen in every individual's life. People are very much dependent on the technologies these days as new technologies are providing lots of comfort to everyone but as we know bad things always comes with the good one, likewise the credit card also comes with the disadvantages of getting it scammed by fraudsters. Credit card frauds occur when an unknown party impersonate himself as the authenticated cardholder and does the transaction without allowing the real owner to know about it. Credit card frauds not only lead to loss of money but it also affects the individuals in many ways, like criminal activities, etc. So in order to deal with these issues we have come across an approach named as Biometric-based (fingerprint) authentication which is secure enough to stop the credit card frauds to some extent. So, in this paper we will explore how credit cards with additional fingerprint verification can provide strong payment authorizations.*

Keywords- authentication, authorization, biometric, credit card frauds.

I. INTRODUCTION

Credit Card Fraud is one of the challenging and serious threats to this modern and developed society [3]. With the increase in advancement of technologies, the rate of frauds has increased up to a level that it is slowly degrading the economic condition of the world. If these scams are not controlled now, then it will be difficult for us to control it later. So, all the developing and already developed countries should start focusing on the issues related to the credit card usage. In this paper we are going to discuss about the proposed system that we are going to build, in order to eliminate frauds related to credit card and gain some of the user's lost trust on technologies. In the existing system, the level of authentication is not secure as there is only one phase of authentication i.e. password and receiving the OTP on the mobile number which is already present in the database and which can be easily stolen by someone. So, we have proposed a system which will have two levels of authentication i.e. password and fingerprints of the cardholder. For this we are using biometric-based authentication to secure our credit card transactions.

Biometric is one of the most secured technologies used by government to secure their system because for any organizations security is one of the main concerns [1].

Biometric-based authentication along with password stored in the system has many advantages as compared to the traditional password which were used earlier because it is providing more security than the previous one and it cannot be easily hacked by someone. Fingerprint of each individuals is unique even a twin baby born on a same day has different fingerprints. So, if a fraudster thinks he can easily copy someone's identity and do the scams is not possible because of this new technology. Biometric authentication uses different biometric keys like fingerprint scanning, iris detection, face recognition, hand geometry, etc. which is very hard to be copied and duplicated by someone. And moreover a person doesn't need to remember the password all time.

In our proposed system, we are using biometric-fingerprint authentication approach which will accept fingerprints of the users at the time of making any transaction and will authenticate it before proceeding further [2]. If the fingerprints matches with the stored fingerprints of database then bank server allows the customers to proceed further with the goods and services and if bank server does not find matching fingerprints then will take action against it. In this way fraudsters can be caught and the decorum of credit card uses can be maintained.

II. PRELIMINARIES

Credit card:-

Credit card is a government-issued card which is used either for online transaction or offline payment. It is a very suitable alternative for cash payment as users just need to swipe the card and provide details to the merchants and the payment is done easily. It is similar to debit card in appearance but provides customers with one advantage of letting him/her to buy things and pay later. It has an electro-

magnetic chip which contains all the details and volatile memory in it.

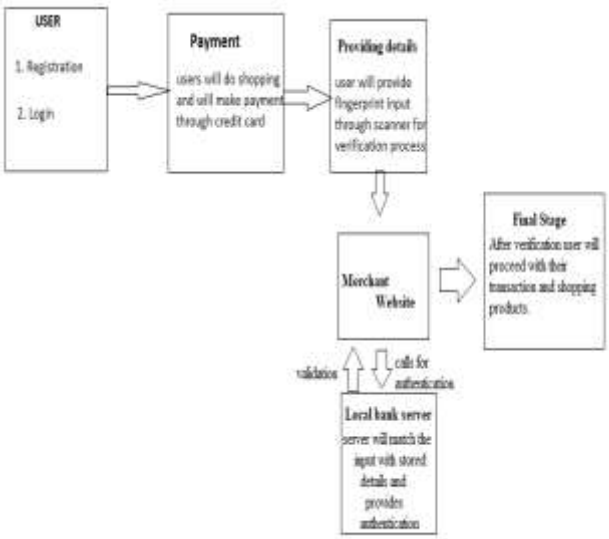
Credit card frauds:-

Credit card frauds are the frauds associated with the credit card where fraudster fetches all the information related to credit card and cardholder, and performs illegal scam by doing transaction of big amount which is beyond the limit that has been sanctioned to the cardholder at the time of issuing the card by government.

Biometric based authentication:-

Biometric-based authentication is a key to the problems associated with credit cards. As the credit card has provided us the easiest way of making payment at anytime and anywhere, it has come into the sight of fraudsters who claims himself as the real cardholder and does the transaction of their choice[3]. So, to deal with such problems biometric-based authentication is one of the key which can be taken into consideration by the business institutions. It uses customer's fingerprints, faces, irises, hand geometry, palm-prints and so on, as a password along with credit card details at the time of making payments to the merchant websites [4]. Biometric-based authentication technique is much efficient than the others approach as it provides high security in terms of identity as it uses biometric keys which are very difficult to copy and share by fraudsters.

III. ARCHITECTURE



IV. IMPLEMENTATION

The proposed system is divided into three parts:-

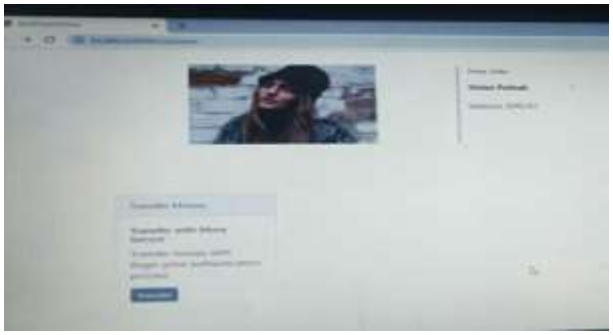
[1] Registration Phase
[2] Login Phase
[3] Authenticate phase

Registration phase:-

This phase includes the registration of customer with bank server and creation of customer's identity. While creating customer's identity we provide details like customerID, Name, EmailID, contact, AdressID to the admin. And while doing registration with bank we provide customer's accountNo. , cvv of credit card, branchID of bank, and most importantly customer's fingerprint.

Login phase:-

In this phase, customer Logs into its transaction page using usernames and password for making payments to merchant.



Authenticate phase:-

This phase performs the authentication of customer with bank server. Here merchant sends request to bank to authenticate the customer who has fed all the credit card details along with its fingerprint and is ready to do transactions. Bank server checks whether customer is eligible to do transaction or not. And after authenticating the customer, bank sends respond to merchant and then merchant grants the transaction.

V. LITERATURE SURVEY

On the basis of the five important elements of e-fraud i.e. criminal, mode of attack, target system, target entity and impact K. A. Akintoye et al [6] put forward electronic payment system on the basis of concepts of e-crime and e-fraud. For the development and correctness the model will make understand the mechanics and context of e-fraud more effectively.

To make the electronic payment systems secure for the use by clients like the buyers and the retailers PyaePyae Hun [7] suggested its architecture .The security architecture of the system is designed by RC5 encryption / decryption algorithm. This eliminates the fraud that take place today with stolen credit card numbers. The symmetric key cryptosystem RC5 can secure typical transaction data like account numbers, amount and other information.

Dileep Kumar et al [8] have proposed after survey on biometric payment system that instead of cards biometric payment system can be used for different forms of payment system. This will reduce the hectic of remembering the passwords and pin numbers of the cards. Biometric payment system is riskless and safe and very secure to use as there are no passwords or private codes to memorize as compare to credit card payment system, wireless system and mobile system etc.

Chin-Chen Chang et al [9] in suggest a novel remote password authentication scheme that removes the security flaws of Hwang-Li's scheme [10]. The suggested scheme provides common verification between the remote system and the user such that the server spoofing attack can be ineffective. Using the proposed scheme the efficiency of the authentication is increasing enabling the user to select and modify his/her password at any time.

VI. CONCLUSION

There are many technologies which can deal with the frauds going on nowadays in terms of credit card but one of the best approach is biometric fingerprint authentication technique because every individuals have unique fingerprints and it cannot be copied or stolen by someone and moreover the pattern of fingerprints is so complicated that if a fraudsters wants to do frauds by providing fake fingerprints it can easily be caught by the machine. Machine uses cryptography algorithm for the authentication of user's fingerprints. So, with the help of these technologies credit card frauds rate can be brought down in near future and people can trust more on the security of credit card.

VII.ACKNOWLEDGEMENT

The success of any task is never intended to an individual but it is the effort of all the people around us. And also success of any work depends totally on support, guidance, encouragement received from the mentors and well wishers.

So, we would like show our overwhelming gratitude to all the people who were directly or indirectly involved in making this paper. Specially, we would like to thank our **Dr. Pankaj Agarkarand** our internal guide **Prof. Vandana Chavanunder** whose guidance we had the privilege of doing this work and whose constant support and inspiration at all the faces of paper lead us to the successful completion of it.

REFERENCES

[1] Jain, A.K., Ross, A., Prabhakar, S.: An introduction to biometric recognition. IEEE Trans. on Circuits and Systems for Video Technology 14 (2004) 4–20

[2] Jain, A.K., Uludag, U., Ross, A.: Biometric template selection: a case study in fingerprints. In: Proc. of 4th Int'l Conf. on Audio- and Video-based Biometric Authentication (AVBPA). Volume LNCS 2688, Guildford, UK, Springer (2003) 335–342

[3] Giampaolo Bella, Stefano Bistarelli, and Fabio Martinelli, "Biometrics to Enhance Smartcard Security Simulating MOC using TOC", Institute of Informatics & Telematics, CNR, Pisa, Italy.

[4] A. Ross, A. K. Jain, "Biometric Sensor Interoperability – A case study in Fingerprints," International ECCV workshop on Biometric Authentication (BioAW), Prague, Czech Republic, LNCS vol. 3087, pp. 134-145, May 2004.

[5] http://www.popcenter.org/problems/credit_card_fraud/PDFs/Bhatla.pdf, June 2003.

[6] K. A. Akintoye, O. I. Araoye, "Combating E-Fraud on Electronic Payment System", International Journal of Computer Applications (0975 – 8887), Volume 25– No.8, Jul y 2011.

[7] PyaePyae Hun. "Design and Implementation of Secure Electronic Payment System (Client)", World Academy of Science, Engineering and Technology, 48, 2008.

[8] Dileep Kumar, YeonseungRyu. "A Brief Introduction of Biometrics and Fingerprint Payment Technology", International Journal of Advanced Science and Technology, Vol. 4, March, 2009.

[9] Chin-Chen CHANG and Jung-San LEE, "An efficient and secure remote authentication scheme using smart card", Information & Security, An International Journal, Vol.18, 2006, 122-133.

[10] Hwang and Li, "A New User Authentication Scheme Using Smart Cards".