6th International Conference on Multidisciplinary Research (ICMR-2019)
Osmania University Campus, Hyderabad (India)
30th-31st May 2019 www.conferenceworld.in
Conference World
ISBN : 978-93-87793-89-7

Credit Card Fraud Detection and prevention using Multi-Biometrics

Asma M. Patel

Research Scholar of Computer Science Department

Shri J J T University, Jhunjhunu, Rajasthan (India)

ABSTRACT:

A remarkable progress in the E-commerce market leads to number of credit card transactions, for online as well as offline. As technology and uses are growing, credit card frauds are also increasing. As today number of ready tools are available, it gives benefits to an attacker to perform Credit card frauds, while it is other hand difficult to detect and prevent. In real life, fake payment transactions could be combined with genuine transactions. Simple pattern matching or single technique are not often sufficient to detect the fraudulent transactions. It require hybrid approach that combine more than one methods. Additionally frauds can be performed via malicious websites, suspicious mails, malware and lack of security from developer's site. As Aadhar is already integrated with banks and it use biometrics mechanism. Currently fingerprint is using as a customer's identity but it has some limitations. In this paper, we proposed multi-Biometrics recognition technology that add more security to an existing biometric system. The techniques used are fingerprint, Iris and face to secure transaction. It provides more security and difficult for hacker to attack, because it generates combine result of biometrics verification. Thus, biometric systems provides higher levels of security by integrate with web applications that require user authentication and verification.

KEYWORDS *- Biometrics, Credit Card Fraud, Fingerprint recognition, Face recognition, Iris Recognition.*

1. INTRODUCTION

Cash less transactions or plastic money is provides advantage to customers for performed financial and banking transaction using their credit/debit card. Since the need of cashless transactions are increasing, every merchant and bank allow to perform transaction using plastic money. As facility increasing, risks are also increased. Customer's silly mistakes can trap their sensitive data or confidential data into wrong hands. Also other risks are loss of a card, card theft, static PIN guessing or sharing and cards details sharing by card owner. Credit card fraud can occur in a number of ways. As existing systems are using static PIN number of card access. The limitations of PIN is overcome by fingerprint as it is unique for each. But it doesn't give security if person's clone copy is available with hacker and many

ISBN : 978-93-87793-89-7

more. To overcome the limitations stated above we have proposed techniques of Multi-Biometric authentication. Indian government already integrates banking system with Aadhar card. Aadhar is storing multi-biometrics data like Fingerprint, Iris and Face. So here we are using this three biometrics data. As it is unique for each person. Fingerprint recognition verify user fingerprint with stored templates and generates result. If it is valid it goes to next verification i.e. Iris. If it matched data then system goes for last verification i.e. face. If all of these three data are matched with stored templates it generates combined result of user's authorization and verification.

2. Existing System

Existing system is working on three different security mechanisms that are PIN, OTP and Fingerprint. Working of individual mechanism are as follow:

2.1 PIN:

A personal identification number is a card holder's personal identification number using for online or offline transactions. It is a secret numeric password. It is a static password normally have four digits. When user initiate transaction this PIN is shared by user with system that can authenticate the user. If the number is matched with stored system data than and only user is approved to access. It is a four digit number that is come in combination of 0000-9999. That are easy to guess, and all the systems are giving three limit of attempt for verification. If user fails during this card is blocked for 24 hours. The Common mistakes performed by users that leads to disadvantages are lost PIN, forget PIN, share PIN to others, etc.

2.2 OTP:

It is stands for One Time Password. It is a six digit code that is randomly generates on users mobile number via SMS or via mail. Card manufacturing companies enhances the security by providing OTP. It removes the issue of fake uses as it verifies user's transaction by eliminating static password. But the limitations are OTP can bypass by using ready tools, if users does not have mobile network connection or mobile battery dead than face to get code. As well as it is easy to remember so any one can notice and use it.

2.3 Fingerprint Authentication:

Biometrics are user own parts that is unique for each and every human in the world. Fingerprint is one of the mechanism used to identify user and verify users identify. Process is bifurcate into two parts that are enrolment and verification. At the time of enrolment users fingerprint is scanned by scanner. It analyse pattern. Patterns stored in database in a coded form for security. At the time of verification user have to put finger on scanner. Scanner scan finger and check it against the code stored in database or template. If both are matched the person is genuine else rejected. Limitations are if hacker carry's a

ISBN : 978-93-87793-89-7

clone copy of victims finger then authentication fail. Apart from that if user is suffer from issues like injury, swelling, cuts, hand gloves pattern does not verify fingerprint and verification is fail.

3. Proposed System

To overcome the limitations of the existing systems, we proposed a system that provides more security and prevention. Process is complete through three phases of biometrics verifications. The first phase is verify the identity of the user using Fingerprint recognition, second phase is verify user identity by Iris recognition and the third phase is verify the user face for authentication process. It generates combine result of three phase. If first is verify then and only it goes for second verification. If second verify then and only it goes for third recognition. It combines result of all the phases and generates combine result of verification.

At first the user will have to insert card or card details. The details are verifies with database. If exists, then user is redirect to next process of authentication using there different biometrics data. If first is verify Fingerprint with stored templates. If valid then and only it goes for second verification. Second it verifies Iris with stored templates. If second verify then and only it goes for third recognition i.e. Face. Face data is matched with stored templates. If it is valid it than generates combine result of verification.

3.1 Model Explanation:

i) **Fingerprint matcher:**

Fingerprint matcher function is activated when user's fingerprint is scanned. Fingerprint matcher first compare user's scanned fingerprint with stored template. If matched redirect to next verification else generates error.

ii) **Iris matcher:**

Iris matcher function is activated when user's Iris is scanned. Iris matcher first compare user's scanned Iris data with stored template. Analyse the properties and if scanned data is matched redirect to next verification else generates error.

iii) **Face matcher:**

Face matcher function is activated when user's Face is scanned. Face matcher first compare user's scanned Face data with stored template. Analyse the properties and is If matched redirect to next verification else generates error.

iv) **Combined Result:**

It generates combined result of all the above there different biometric verification process**.** If all data are valid than allow to performed transaction else rejected**.**

ISBN : 978-93-87793-89-7

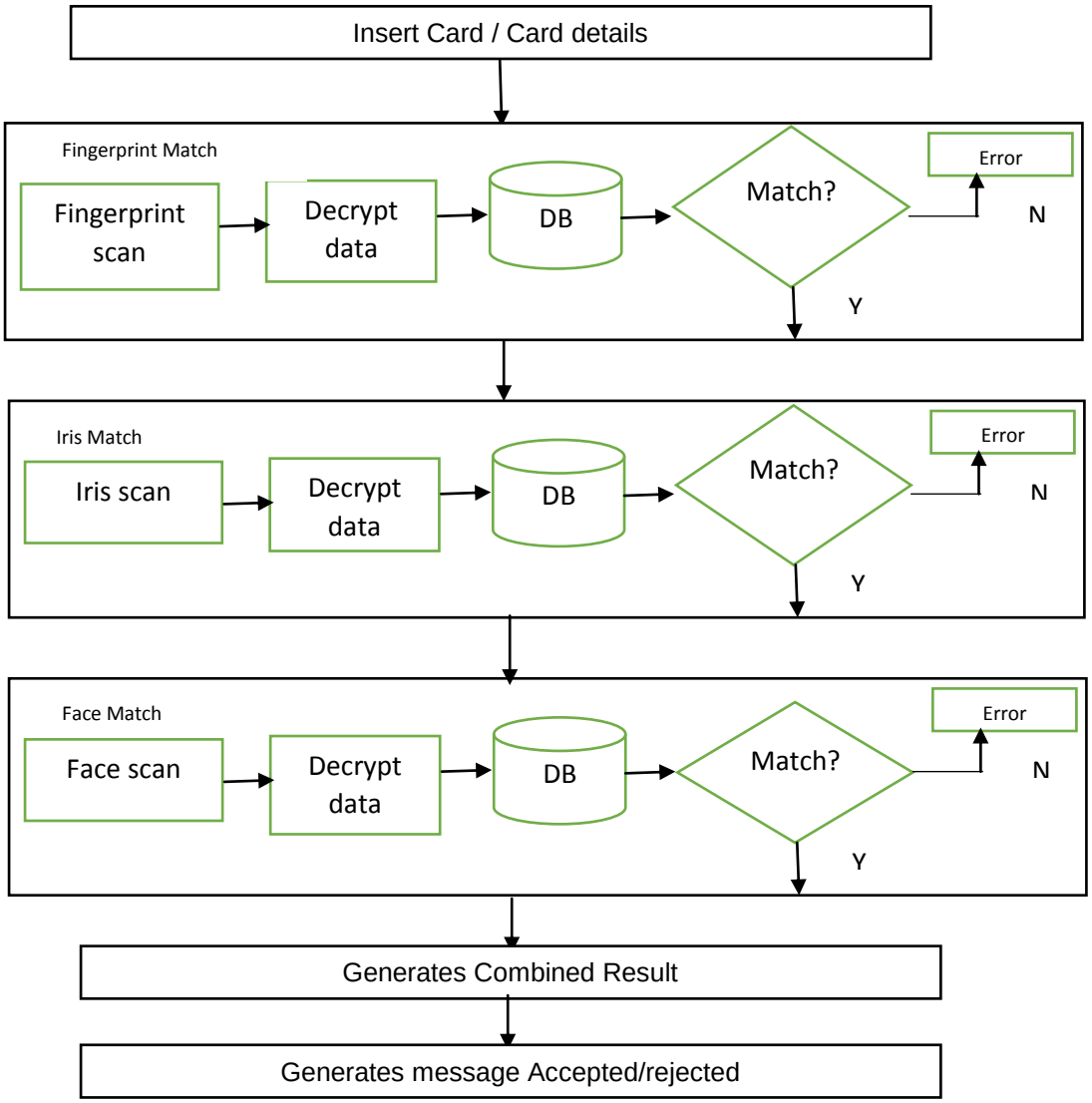

Figure: Working of Proposed Model

4. Future Work:

As biometrics are individual user's identity it gives more security to user. But it has some limitations like if hacker having clone copy of user's biometrics data then verification is not successful. For more security we can add security code (i.e. OTP) and location matching module. As biometrics suffers from other limitations like in case of injury, swelling, part is covered, lances, cuts, etc. verification gets fail. So we can add voice recognition phase for more security.

ISBN : 978-93-87793-89-7

References:

1. A.Ragavan, J. S. (2016). BIOMETRIC MECHANISM FOR ENHANCED SECURITY OF ONLINE TRANSACTION IN ANDROID SYSTEM:A DESIGN . *International Journal of Recent Trends in Engineering & Research* , 5.
2. AashleshaBhingarde, A. K. (2015). Credit Card Fraud Detection using Hidden Markov Model . *International Journal of Advanced Research in Computer and Communication Engineering* , 2.
3. Akshay Prakash, G. M. (2016). Credit Card Transaction Using Face Recognition Authentication . *International Journal of Innovative Research in Computer and Communication Engineering* , 7.
4. Alka Herenj, S. M. (2013). Secure Mechanism for Credit Card Transaction Fraud Detection System . *International Journal of Advanced Research in Computer and Communication Engineering* , 5.
5. Anita B. Desai, R. D. (2013). Data mining techniques for Fraud Detection . *International Journal of Computer Science and Information Technologies*, 4.
6. Anju Rohilla, I. B. (2015). Credit Card Frauds: An Indian Perspective . *Advances in Economics and Business Management* , 7.
7. Daniel Ugoh, M. N. (2015). Reducing Internal Banking Fraud using Smart Cards and Biometrics as Access Control Tools . *International Journal of Advanced Research in Computer and Communication Engineering* , 4.
8. Deepak Pawar, S. R. (2016). DETECTION OF FRAUD IN ONLINE CREDITCARD TRANSACTIONS . *International Journal of Technical Research and Applications* , 3.
9. shu Trivedi, M. M. (2016). Credit Card Fraud Detection. *International Journal of Advanced Research in Computer and Communication Engineering* , 4.
10. Ishu Trivedi, M. M. (2016). Credit Card Fraud Detection. *International Journal of Advanced Research in Computer and Communication Engineering* , 4.