PREVENTING FRAUD TRANSACTION USING FINGERPRINT VERIFICATION

[1]Mr. Hardik C. Soneria,[2]Ms. Nikita M. Agrawal, [3]Mr.Mohd Farhan A. Achchhu
[1]Assistant Professor,[2]Student,[3]Student
[1]Information Technology Department,
[1]Laxmi Institute of Technology, Sarigam, India

Abstract: Along with great increase in credit & ATM Card transactions, credit & ATM card fraud has become increasingly widespread in recent years. One-time password (OTP), a commonly used two-factor authentication is considered an effective deterrent against criminals trying to steal money from your bank account through online transaction. The proposed paper work investigates that the efficacy of applying Fingerprint verification and Face recognition of the user from his device itself to prevent ATM card fraud problems. The different techniques & classification methods, i.e. Fingerprint verification and face recognition are tested for their applicability in counterfeit or fake detection. The proposed system provides a useful framework to detect & prevent a fraud & to choose the best model to recognize the credit & ATM card fraud risk. The authentication mechanism is useful to prevent illegal transaction by fraudsters through fake calls and secure users cash card from being used by fraudsters by providing more security i.e. only by judging person only by his/her face as well as fingerprint recognition.

***Index Terms* - OTP (One-Time Password).**

I. INTRODUCTION

In present, scenario when the term fraud comes into a talk, credit card follows in the banks and the financial frauds done by the fraud calls & various frauds clicks to mind so far. With the great increase in credit cards, ATM CARDS & E-transactions fraud has increasing excessively in recent years. Fraud detection & prevention includes analyzing of the spending behavior of users or customers order purpose, uncovering, or escaping of undesirable behavior. As credit card becomes the most general mode of payment or both online as well as regular purchase, fraud related with it also accelerates.

Fraud presents noteworthy cost to our financial prudence measure worldwide current techniques based on Biometrics Technology like Fingerprint and Face recognition, has been introduced for detecting & preventing credit/ATM card fraudulent transactions through fake calls. The study shows AI, cryptographic techniques which are used for fraud prevention there by implementing as/which ask secret, questions i.e. enhancing multiple layers of security for wrapping the pin no in previous stages using cryptographic algorithm, by which a fraud can also be prevented. As per as the literature survey & study of paper in the field of artificial Intelligence(AI), Genetic algorithm, Neural network it has been analyzed & observed that the technologies are meant for fraud detection but not for prevention whereas on other hand using biometrics technologies like facial and fingerprint, frauds can be prevented.

We can divide biometric technology into broad categories according to what they measure: Devices based on physiological characteristics of any person and Systems based on behavioral characteristics of any person.

Biometrics techniques can be easily adopted along with the traditionally used techniques in financial organizations such as banks, at retail locations to be used with smart cards, ATM machines, credit cards and debit cards, and anywhere you are able to perform a financial transaction. It may work as standalone or in combination with the PIN to securely identify user as the genuine owner of the card and the person who has permission to exchange the money.

II. RESEARCH METHODOLOGY

Due to the outstanding growth in Information and Communication Technology (ICT), security of information is becoming of more challenging in day by day life even as there are many ways and methods available to malfunction of information security. Phishing is one of the great challenge and threats for website authentication now days. A phishing can be understanding as a type of social engineering damage, in this attacker or hacker designs user’s credentials by faking a fraud call of any trusted well known bank or any other financial organization. Fake calls are the biggest issue and it is extremely popular among the fraudsters.

Net banking or internet banking system needs more consideration for the development and execution of some reliable security system approach. This requisite needs to plan and develop a competent security system that works very efficiently by which consumers can be validated, verified and granted access to the Internet banking. By using biometric technology, we may decrease all types of frauds including phishing etc. Currently, when financial system is going through very much insecurity, many companies are now started realizing the profit of investment to develop and implement biometric security system.

There are many ways for biometric scanning's e.g. retina scan, face recognition, vein geometry, fingerprint identification etc., available and in practice. These can be summarized as:

2.1 Fingerprint Verification

The fingerprints of any person remains the same throughout the life and no two fingerprints are ever same. But for this, to work accurately it requires clean hands without having any injuries to their prints otherwise it will prevent proper identification.

2.2 Face Recognition

One of the most flexible methods as it can be done without the person being aware that they are being scanned.

2.3 Scanning of Retina

The pattern of the blood vessel at the back of every eye is absolutely unique and is never changing. The disadvantage of this system is that it takes around 15 seconds of cautious attention to complete a good scan.

2.4 Scanning of Hand Geometry

It will work in insensitive working environments. It is not measured as intrusive and often used in industrialized environment.

2.5 Vein Geometry Recognition

This is also a very good type of security scan. In vein geometry the geometry of veins in a hand is analyzed and identification and authorization can be done on the basis of result.

2.6 Iris Scanning

This is also very difficult to reproduce and stays the same with your entire lifetime. But obviously it is difficult for children and the sick people.

2.7 Voice Analyzing

This method of security biometric can be implemented and tested without the person's awareness.

From above listed Biometrics Scanning techniques there are two techniques which can be used for user verification while making online transactions from mobile device or personal computer. There are still the chances of fingerprint spoofing or creating fake biometrics, but it is absolutely easier to make a fake call and ask users details for making illegal transactional.

III. FAKE CALL FRAUDS

What we are discussing here is related to phishing, also known as voice phishing. Several instances have occurred wherein people receive phone calls that appear to be from their bank. The caller usually pretends to be a bank representative or someone from the bank's technical team. In most cases, the caller sounds professional and provides a convincing reason for calling the customer. After giving a false sense of security, the caller then tricks the victim into giving away their personal and confidential data such as:

3.1 Credit/debit card number

3.2 The card's CVV number [Card Verification Value]

3.3 Expiry date

3.4 Secure password

3.5 One-Time-Password (OTP)

3.6 ATM pin

3.7 Internet Banking login ID and password

With all such crucial information at hand, the fraudster can easily carry out illegal financial transactions using the victim's name due to which they will suffer.

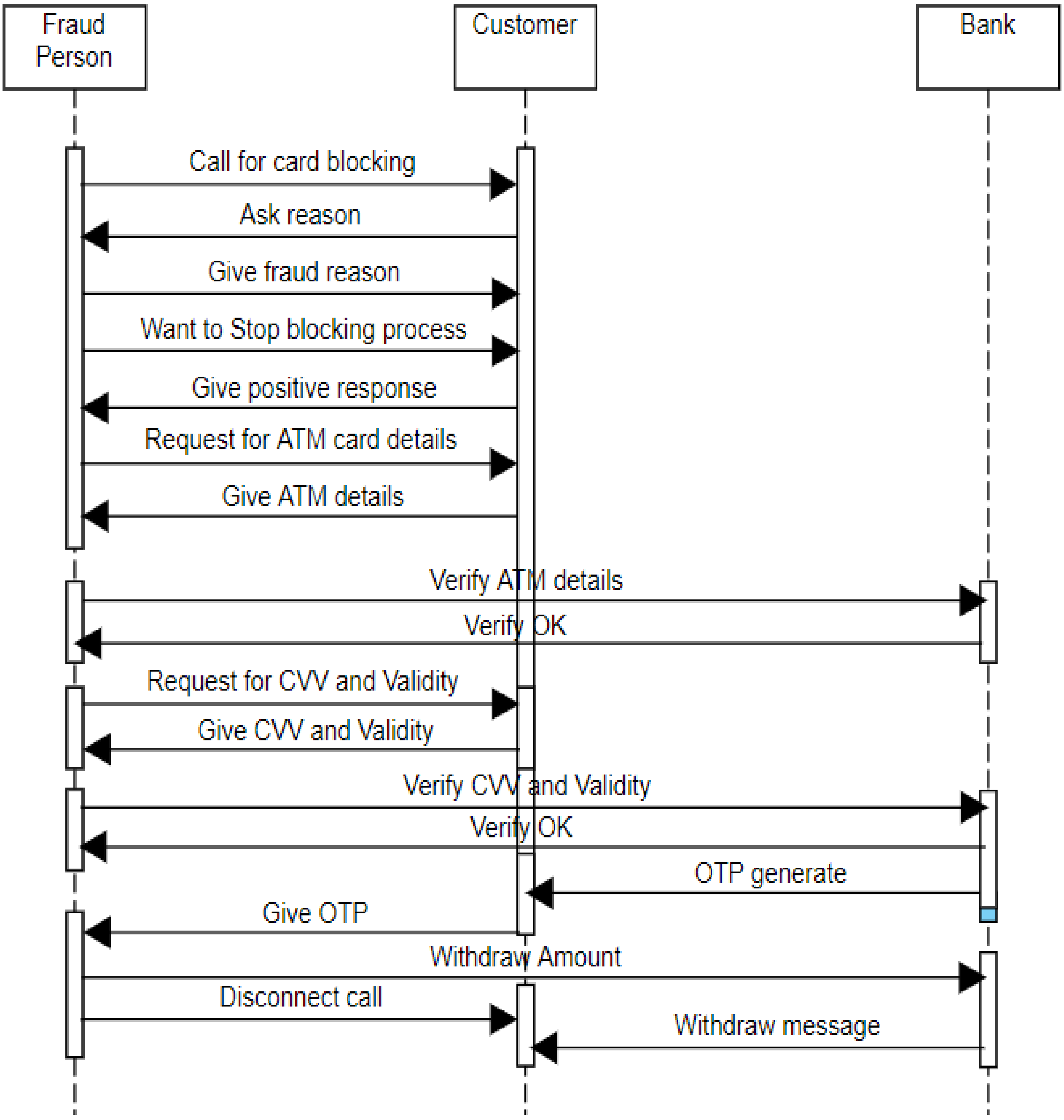

Figure 1

The sequence diagram explains about the sequence of events which will happen if the fraudsters are successful.

1) Fraudster will call the customer as a bank manager saying that your ATM card is going to block.

2) Customer will ask about the reason of blocking the card.

3) Fraudsters will give any random reason and with that it will also ask for if the customer wants to stop the process or not.

4) Customer will give positive response in fear of card, getting blocked.

5) Fraudster will ask for bank details.

6) Customer will give all the details of his/her ATM account.

7) Now, as fraudster has all the details, it will directly access the account and will verify the details from the bank.

8) Bank will verify them and if the details are right, it will allow access to the account.

9) Fraudster will ask the customer for CVV number, date validity to proceed.

10) Customer gives the response accordingly.

11) Fraudster will now verify the given card details from the bank.

12) Bank will verify again and also with the verification will generate an OTP (One-Time Password) on the customer's number.

13) Fraudster will ask for OTP from customer and customer will give the OTP.

14) After getting the OTP fraudster will withdraw the amount from his/her bank and will then disconnect the call.

15) Bank will give withdrawal message to the customer.

In this way, the customer will become victim of the ATM fraud.

IV. Results and Discussion

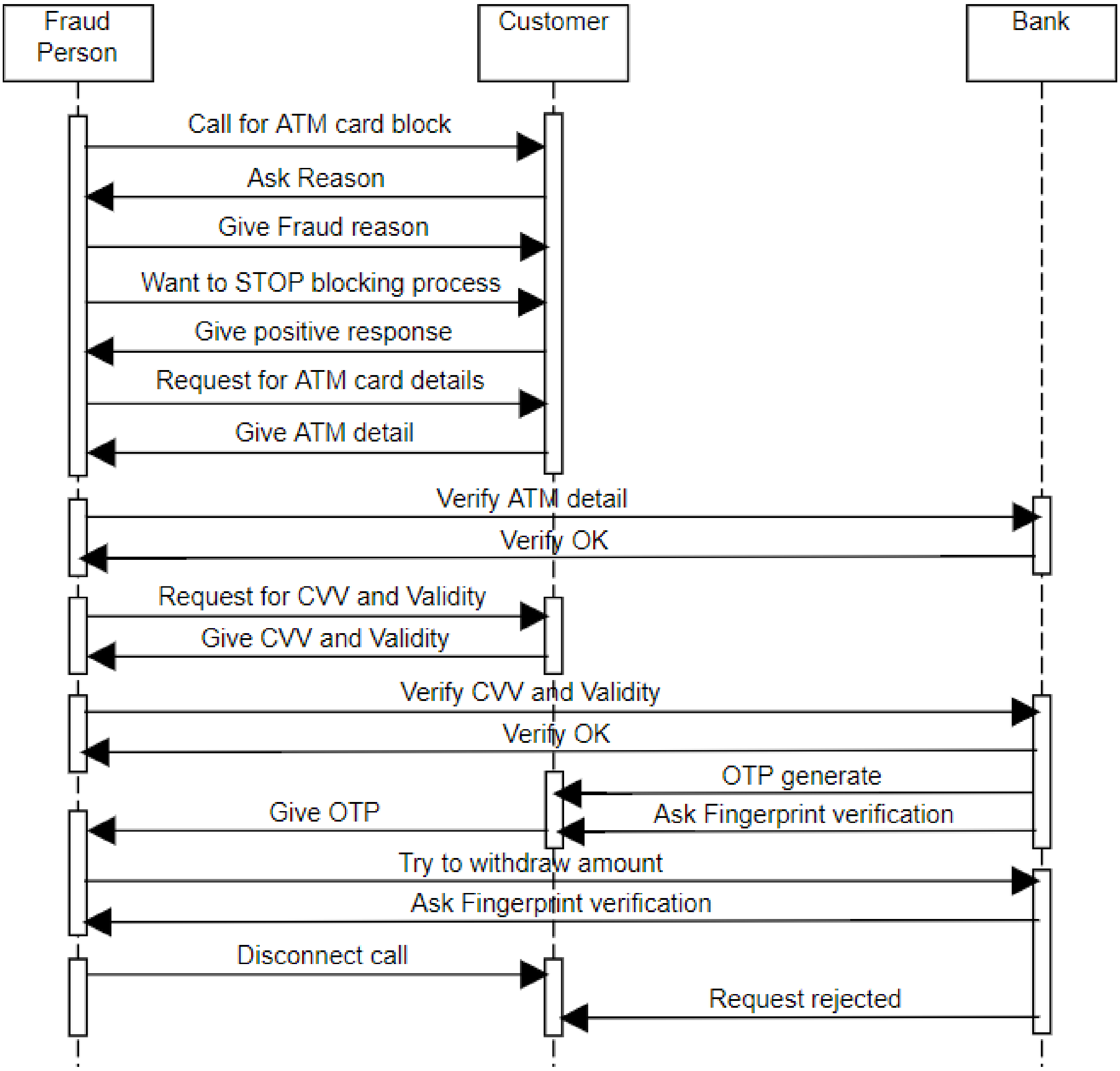

Figure 2

To prevent the ATM fraud, in the second diagram it will ask for fingerprint verification and face recognition in order to avoid becoming a victim and also for advance security in the current system.

V. ADVANTAGES

These security controls enable the banks to reduce fraudulent transactions, reduce legal risks and achieve regulatory compliance, cardholder trust & confidence. It could provide Better risk/ fraud management. It could enhance trust and confidence which could result more usability of ATM.

VI. LIMITATIONS

The above approach made in this paper isn't feasible in context of time and availability of particular tasks. As a future work, Face Recognition could be providing more security and a user friendly environment developed.

VII. ACKNOWLEDGMENT

Accordingly, now-a-days, there are many security breaches which lead the customer gaining huge damage and becoming a victim by losing his/her money which they have earned with hard work. To avoid the security problems and huge damage, in this project, we will propose an extra layer of security in the current ATM system to avoid any fraud with customer. The Fingerprint verification and Face recognition has revolutionized the way people perceive security generally. If the system will introduce along with the existing system and technology, there will be great security and a very well developed protected system where customer can feel secure without any fear and worries of getting theft or losing his/her hard work.

REFERENCES

[1] Anil K. Jain, Ruud Bolle, Sharath Pankanti, Biometrics: personal identification in networked society.

[2] Biometrics Institute Industry Survey 2012, URL: www.biometricsinstitute.org

[3] Siddiqui, Ahmad Tasnim; Muntjir Mohd.; A Study of Possible Biometric Solution to Curb Frauds in ATM Transaction, IJASCSE, November 2013

[4] “Casey schaufler , Friedrich von Schiller”, Banking and Bookkeeping, Security Engineering: A Guide to Building Dependable Distributed Systems

[5] Anderson, R. 2007. The Credit Scoring Toolkit: theory and practice for retail credit risk management and decision automation. New York: Oxford University Press.

[6] Brause, R., Langsdorf, T. & M Hepp. 1999b. Neural Data Mining for Credit Card Fraud Detection, Proc. of 11th IEEE International Conference on Tools with Artificial Intelligence.

[7] A. Shen, R. Tong, and Y. Deng, "Application of classification models on credit card fraud detection," June 2007.

[8] http://www.infosys.com/FINsights/Documents/pdf/issue10/financialtransactions.pdf

[9] M. Fahim Zibran, Biometric Authentication: The Security Issues, Technical Report #2012-02, University of Saskatchewan, Canada [18] Ayhan EMRE, Biometric Security Technologies.