PoS Security With Biometric Fingerprint Credentials

Mr. Vinoth Kumar A[1], Mr Siva Balan[2]
[1, 2] Department of CSE
[1, 2] New Horizon College of Engineering, Bangalore, Karnataka, India

Abstract- *Credit and debit card data theft is one of the earliest forms of cybercrime. Still, it is one of the most common nowadays. Attackers often aim at stealing such customer data by targeting the Point of Sale (for short, PoS) system, i.e. the point at which a retailer first acquires customer data. Modern PoS systems are powerful computers equipped with a card reader and running specialized software. Increasingly often, user devices are leveraged as input to the PoS. To elucidate the system in brief, multiple layered verification process would be carried out to make the system more secured. That is, Biometric fingerprint technology is added to the POS system. Our solution improves over up to date approaches in terms of flexibility and security.*

Keywords- Point of Sale(PoS), Fingerprint technology, verification, credit/debit card

I. INTRODUCTION

Since information of users can leak easily, many authentication approaches are proposed to secure data and systems. Authentication method should be able to "declare anyone that they are who they claim to be". However, it is not important in authentication process that what identity is authorized for. Even though Personal Identification Number (PIN) and password are standard approaches that are normally used by many companies for authentication, these methods are still vulnerable. PIN and password may be forgotten or lost. Moreover, they can be disclosed and stolen by intimates or colleagues. Some systems use an object such as passport or ID card to identify a user. It is practical in use but also is very easy to be stolen or copied. Therefore, biometrics which is unforgettable and more unique becomes a choice for secure process. Biometric technologies can be used is fingerprint. Fingerprint recognition or fingerprint authentication refers to the automated method of verifying a match between two human fingerprints. Fingerprints are one of many forms of biometrics used to identify individuals and verify their identity. The member's finger print will be compared with the cardholder fingerprint which is stored in the respected bank database. If both the finger print matches the transaction will be approved.

II. EXISTING SYSTEM

A typical system might consist of terminals at the point of sale, i.e. on the retailer's premises. The function of these terminals is to communicate with various financial institutions. Someone wishing to use the Electronic funds transfer at point of sale(EFTPOS) system will normally be issued with a plastic card bearing a magnetic stripe. In addition they will be issued with some personal identification data (PID), typically four decimal digits. When they wish to make a purchase from a retailer they will present their plastic card whose magnetic stripe is read by the terminal, thus giving the terminal card holder related data such as account number, expiry date and so on. The card holder also, separately, enters their PID. The terminal will now communicate with the card issuer's computer (CIC), whose function is to ratify, or not, the transaction. This entails checking that the card is valid, that that account contains sufficient funds for the transaction and that the PID entered does correspond to that card. Thus it should be clear that the PID acts as a signature to authenticate the card holder to the card issuer. It is therefore imperative that the PID should be kept secret and that it, or any derivative of it, should be enciphered for transmission. Furthermore it must be guaranteed that none of the information is corrupted or intentionally changed during transmission.

III. RELATED WORK

There are several previous researches concerning about verification process when doing online payment transaction. Many studies related to this research.

A. Credit/Debit Card Security

Credit/debit card is used between customer and merchant in payment process. Payment process using credit card can be separated into (1) Card present transaction and (2) Card not present transaction. Many methods were invented to secure credit card when making these transactions.

For card present transaction, a card and a cardholder are presented at point of sale. Electronic Data Capture (EDC) is used to process transaction. Cardholder is required to sign a signature to provide an evidence of the identity of the cardholder when processing a transaction. A drawback of this method is that if the card has been stolen, the cardholder can be another person that is not the owner of the card. Signature

can be copied easily from signature panel at back of the card . To solve this problem, PIN verification method was invented. The cardholder is required to enter a PIN when processing a transaction. However, drawback of this method is that PIN can be guessed very easily because some people commonly use number such as birth date or phone number. If the PIN is far different from common number then it is very easily to forget.

For card not present transaction, other approaches were invented to secure transaction. As card not present transaction normally occurs when a customer makes a payment through e-commerce channel, fraud may be very difficult to be detected. Payment transaction is also processed by a merchant without both of the cardholder and the card. Static password is sometimes used to authorize transaction. Drawbacks of this method are the same as PIN and password, which is forgettable. Therefore, another secure method, One Time Password (OTP), is used. OTP is a set of alphanumeric characters sent to customer by Short Message Service (SMS) when making online payment transaction. Bank generates this password and sends it to registered mobile phone number when the customer presses "Request OTP" button. Since SMS is sent to registered mobile phone number which belongs to the real cardholder, the person who is not the owner of the card cannot continue the payment process. Even though OTP seems to be very safe and secure, it is not robust to Malware based impersonation attack, Phishing attack, and Malware based reply attack.

B. Enhanced Privacy and security

The use of fingerprint security in payment cards make it even more personal and private. Fingerprint provide a strong and unique binding between the cardholder and his personal information on the card which is useful in identifying the rightful owner of the card. The fingerprint cannot be borrowed, lost or stolen like a PIN and so strengthen the authentication of an individual's identity. Fingerprint security would ensure that only the rightful cardholder can have authorized access to the personal information stored inside the card. Fingerprint security will also increase trustworthiness of POS and ATM terminals, as the authentication process remain secure.

Security is one of the major concerns for payment cards, implementing fingerprint security will enhance security as it allows for the verification of "who you claim to be" (information about cardholder stored in payment cards) based on "Who you are" (user's live fingerprint template).

IV. PATTERN-BASED (OR IMAGE-BASED) ALGORITHMS

Pattern based algorithms compare the basic fingerprint patterns (arch, whorl, and loop) between a previously stored template and a candidate fingerprint. This requires that the images can be aligned in the same orientation. To do this, the algorithm finds a central point in the fingerprint image and centers on that. In a pattern-based algorithm, the template contains the type, size, and orientation of patterns within the aligned fingerprint image. The candidate fingerprint image is graphically compared with the template to determine the degree to which they match.

V. SYSTEM DESIGN AND IMPLEMENTATION

The complete system can be considered a package comprising of both PoS machine and fingerprinting scanner. Figure 1 shows the complete flow of the system. PoS ensures the point of sale screen contains only what a cashier needs at their disposal to serve customers. Once the credit/debit is card is swiped in the PoS machine, the PoS control panel then checks the permission level of the user and determines whether account access should be allowed. If the card is valid, then it will ask for the finger printing. During the authentication process fingerprint is scanned at the reader side and a template is generated which is then encrypted and send to the card for matching.

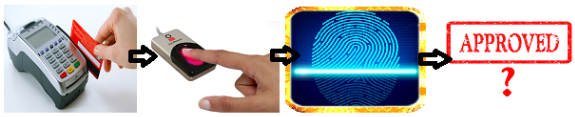

Figure 1. System Design

Fingerprint basically consists of ridges (raised skin) and furrows (lowered skin) that twist it to form a distinct pattern. When an inked imprint of finger is made, the impression created is of ridges while furrows are the unlinked areas between the ridges. There is one other important characteristic of fingerprint called 'minutiae', are what is unique to the individual. Fingerprint security in payment card industry has gained significant interest among researchers as a solution for identification of legitimate users. Matching Algorithm is an algorithm that verifies biometric data with templates. The figure 2 shows the verification control flow between the Pos and the Card issuer.

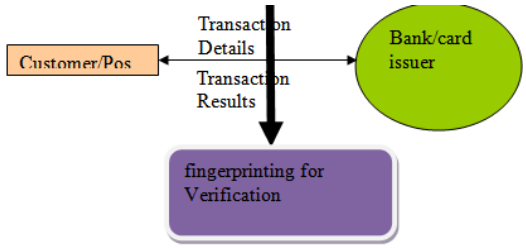

Figure 2. Control Flow for fingerprinting verification between PoS and Bank.

Cardholder authentication can be performed by the payment card comparing the live template with the template stored in the account. Once the cardholder finger print matched with the respective bank database template stored, the transaction will be authorized.

VI. CONCLUSION

Moving from one security mechanism to another has never been easy, it requires time, cost and other factors. The most important thing need to be considered is the risk associated with it, especially when it comes to payment cards. In this approach template of the fingerprint is stored in database of the card issuer. The user needs to present a matching template in order to authorize transaction. The user finger print should be matched with card issuer database template stored.

VII. FUTURE WORK

In future paper we will work on technology where we can built both PoS and fingerprinting as single device with more secured and easy transaction

VIII. ACKNOWLEDGEMENT

We thank all people who participated in our primary experiments. Their comments turned out to be very helpful for this paper.

REFERENCES

[1] Gittipat Jetsiktat, Sasipa Panthuwadeethorn, Suphakant Phimoltares "Enhancing User Authentication of Online Credit Card Payment using Face Image Comparison with MPEG7-Edge Histogram Descriptor" Advanced Virtual and Intelligent Computing (AVIC) Center Department of Mathematics and Computer Science, Faculty of Science, Chulalongkorn University, Bangkok, Thailand.

[2] Himanshu Vats, Ron Ruhl, Shaun Aghili "Fingerprint Security for Protecting EMV Payment Cards" The 10th International Conference for Internet Technology and Secured Transactions (ICITST-2015).

[3] Syed Mahmud Hasan, Md. Tahmid Rashid, Md. Shadman Sakib Chowdhury and Dr. Md. Khalilur Rhaman "Development of a Credible and Integrated Electronic Voting Machine Based on Contactless IC Cards, Biometric Fingerprint Credentials and POS Printer" 2016 IEEE Canadian Conference on Electrical and Computer Engineering (CCECE).

[4] Allan Pedersen Navi Partner " Designing a Secure Point-of-Sale System" Technical University of Denmark.

[5] Carl J. Debono, David Busuttil " A Secure Wireless Point of Sale System" Technology Department Vodafone Malta Ltd Naxxar, Malta.

[6] Common Criteria for Information Technology Security Evaluation, version 2.2. Part 1: Introduction and General Model, Jan. 2004. CCIMB-2004-01-001.

[7] International Standard ISO/IEC 24787 Information technology — Identification cards — On-card biometric comparison [Online] Available:http://webstore.iec.ch/preview/info_isoiec24787%7Bed1.0% 7Den.pdf. [Accessed: Feb. 15, 2015].

[8] H. Gravnas, “User’s trust in Biometric Authentication Systems,” M.S. thesis, Department of Computer Science and Media Technology, Gjovik University College, Stockholm, Sweden, 2005.

[9] G. Jetsiktat, S. Panthuwadeethorn, and S. Phimolthares, “A Comparison Study of Image Descriptors on Low-Resolution Face Image Verification,” In the Proceeding of the 2014 Annual Summit and Conference on Asia-Pacific Signal and Information Processing Association, pp.1-6, Siem Reap, December 2014.