Online Credit Card Transaction Using Finger Print Recognition

1) Dr.M.UmamaheswariPh.D
Prof & HOD
Bharath University
Chennai-73, Tamil Nadu,India

2) S.Sivasubramanian M.Tech
Sr.Lecturer
Bharath University
Chennai-73,Tamil Nadu,India

3) B.Harish Kumar
II.M.Tech (CSE)
Bharath University
Chennai-73,Tamil Nadu ,India

Abstract:
Internet shopping, a strong alternative to traditional “go, see, touch and buy” shopping, has been one of the mostly used facilities of the Internet. Security in online payment systems has been a wide research area since the early days of the Internet and several approaches have been devised by various Organizations. But, none of the system overcome the weakness in those system. Several online shopping systems serve internet users all around the world and enable people to get the products they need with a small effort. This paper proposes a new solution that combines finger print recognition with online credit card transactions. Here the proposed system provides more security then existing system with finger print recognition because of finger print is unique. Here no need to remember the more passwords, your finger is your password.

Keywords: Internet shopping; finger print recognition; credit card transaction; Muti factor authentication(MFA).

Introduction:

Internet shopping Users browse the online stores and obtain their needs with minimum effort compared to traditional retailing systems. The difference occurs in the manner of payment while using a POS (point of sale) device to perform a payment with their credit cards in offline retailing, consumers provide their personal data together with credit card details over the Internet in order to complete an online payment. However, most people do not volunteer giving such details because of financial risks. To avoiding this draw back we are using the finger print recognition in online transactions, because of finger print is the unique one in the humans entire life.

Finger prints provides more authentication due to its feasibility, distinctiveness ,performance, accuracy, reliability and acceptability. The finger print is one of the popular biometric method used to authenticate human beings.

Purpose of prior research:
Due to the problems of e-commerce transaction people trying to research new methodologies Generally we are using two methodologies.

1. Master Card Secure Code
2. Virtual Credit card number

Master Card Secure Code:

In this methodology Visa’s “Verified by Visa” program, which has been then adopted by Master Card and by JCB International as “J/Secure”. This program introduces a password protection mechanism to online credit card transactions. The approach is based on a protocol called 3D Secure. In this protocol, the credit card issuer bank approves the fund transfer after authenticating the cardholder via a previously defined password for which the user is prompted during an online credit card transaction. However, being an easy to use system especially for the users, the strength the protocol offers by password approach has also become the weakness because of phishing and key loggers The side effect to the user is keeping the password secret.

Virtual Credit card number:

In this approach, a credit card holder is assigned a virtual credit card that shares the same account as the cardholder’s physical credit card. It can be used in online transactions as a traditional credit card until its expiry date. The virtual card has a card number, a CVC number, an expiry date and a flexible monetary limit that can be redefined by the user prior to a transaction and reset periodically. The advantage offered by a virtual credit card is that, even if the credit card number is stolen together with other details, it cannot be used until the user redefines a new temporary limit for a new transaction. Though decreased, the theft possibility occurs between the time span starting with a limit redefinition and ending with a transaction or periodical reset. An alternative to virtual credit card, which can be used several times, is the “Single Use Card Number”. In this approach, the card-issuing bank provides the user a single use card number, which expires after single use in a transaction. This approach limits fraud possibility; and defeats the key loggers because of single use. However, this approach forces the user to perform a purchase with this number as soon as possible, because keeping the number secure becomes a challenge for the user.

Advantages of Finger print recognition in credit card transaction:

What is Fingerprint Scanning?
Fingerprint scanning is the acquisition and recognition of a person’s fingerprint characteristics for identification

purposes. This allows the recognition of a person through quantifiable physiological characteristics that verify the identity of an individual.

There are basically two different types of finger-scanning technology that make this possible. One is an optical method, which starts with a visual image of a finger. The other uses a semiconductor-generated electric field to image a finger.

There is a range of ways to identify fingerprints. They include traditional police methods of matching minutiae, straight pattern matching, moiré fringe patterns and ultrasonic.

Practical Applications for Fingerprint Scanning:

There are a greater variety of fingerprint devices available than any other biometric. Fingerprint recognition is the front-runner for mass-market biometric-ID systems. Fingerprint scanning has a high accuracy rate when users are sufficiently educated. Fingerprint authentication is a good choice for in-house systems where enough training can be provided to users and where the device is operated in a controlled environment. The small size of the fingerprint scanner, ease of integration - can be easily adapted to keyboards, and most significantly the relatively low costs make it an affordable, simple choice for workplace access security.

Plans to integrate fingerprint scanning technology into laptops using biometric technology include a single chip using more than 16,000 location elements to map a fingerprint of the living cells that lay below the top layers of dead skin. Therefore, the reading is still detectable if the finger has calluses, is damaged, worn, soiled, moist, dry or otherwise hard-to-read finger surfaces--a common obstacle. This subsurface capability eliminates any attainment or detection failures.

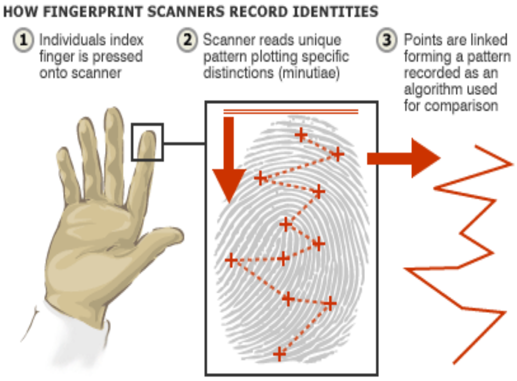
Accuracy and Integrity:

With any security system, users will wonder,… can fingerprint recognition system be beaten? In most cases, false negatives (a failure to recognize a legitimate user) are more likely than false positives. Overcoming a fingerprint system by presenting it with a "false or fake" fingerprint is likely to be a difficult deed. However, such scenarios will be tried, and the sensors on the market use a variety of means to circumvent them. For instance, someone may attempt to use latent print residue on the sensor just after a legitimate user accesses the system. At the other end of the scale, there is the gruesome possibility of presenting a finger to the system that is no longer connected to its owner. Therefore, sensors attempt to determine whether a finger is live, and not made of latex (or worse). Detectors for temperature, blood-oxygen level, pulse, blood flow, humidity, or skin conductivity would be integrated.

Fingerprint Matching:

Among all the biometric techniques, fingerprint-based identification is the oldest method which has been successfully used in numerous applications. Everyone is known to have unique, immutable fingerprints. A fingerprint is made of a series of ridges and furrows on the surface of the finger. The uniqueness of a fingerprint can be determined by the pattern of ridges and furrows as well as the minutiae points. Minutiae points are local ridge characteristics that occur at either a ridge bifurcation or a ridge ending.

Fingerprint matching techniques can be placed into two categories: minutae-based and correlation based. Minutiae-based techniques first find minutiae points and then map their relative placement on the finger. However, there are some difficulties when using this approach. It is difficult to extract the minutiae points accurately when the fingerprint is of low quality. Also this method does not take into account the global pattern of ridges and furrows. The correlation-based method is able to overcome some of the difficulties of the minutiae-based approach. However, it has some of its own shortcomings. Correlation-based techniques require the precise location of a registration point and are affected by image translation and rotation.


HOW FINGERPRINT SCANNERS RECORD IDENTITIES
1 Individuals index finger is pressed onto scanner
2 Scanner reads unique pattern plotting specific distinctions (minutiae)
3 Points are linked forming a pattern recorded as an algorithm used for comparison

Authentication:

Authentication factors for MFA are usually grouped into these three categories: 1) what you know (e.g.,password), 2) what you have (e.g., token), and 3) who you are (e.g., biometric) [4]. Combination of these categories decreases the vulnerability that arises when each authenticator is used alone in an authentication scenario. It implements the three categories of MFA as follows. 1) “What you know” is the PIN of the credit card, 2) “What you have” is the smart card that is Master card are Visa card, and 3) “Who you are” by using finger print humans details can be identify from the database the smart card or a central database for authentication and play the key role in identification.

E-ID system:

An **identity document** (also called a **piece of identification** or **ID**) is any document which may be used to verify aspects of a person's personal identity. If issued in the form of a small, mostly standard-sized card, it is usually called an **identity card** (**IC**). In some countries the possession of a government-produced identity card is compulsory while in others it may be voluntary. In countries which do not have formal identity documents, informal ones may in some circumstances be required.

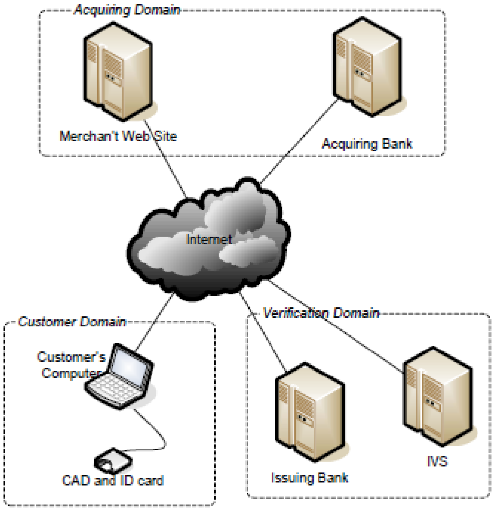
The EID System is actually three separate services:

Identity Management Service – Provides for the creation and management of identity accounts (commonly called EID accounts) for the entire university community.

Authentication Service – Provides an EID credential (e.g., password) verification service and supports login session management for web-based campus services.

Directory Service – Provides "lookup" services for EID identifiers, affiliations, and other information of interest across campus.

Working Procedure:



The following steps are followed when we are doing e-shopping by using finger print recognition.

Steps:

Client: Enter the particular website and select the particular products or service and request an order.

Merchant: Provide products and services to the customer; and create an ODP(order details package) and send it to customer.

Client: view the order details and type the credit number.

Merchant: check the credit card number and the details of the customer. Give the response to the client if it ok means.

Client: Then enter the pin number & Finger print recognition.

Merchant: verify the pin number & biometric if it matches means take the amount from the customer credit card.(or) your not the correct user of the credit card.

Conclusion:

Security in online payment systems has been a wide research area since the early days of the Internet and several approaches have been devised by various organizations. However, there has been no certain solution overcome the deficiencies in these systems completely. we have introduced a solution based on the rapidly developing smart card based biometric systems; and given a sample implementation on e-ID system. The sample implementation is explained with a successful steps. The proposed framework might be used in countries that use biometric system with some modifications according the specific implementation details of their e-ID solutions. Although the solution is not global because of the e-ID system differences for each country, it provides high security and safety for both the customer and the merchant in local e-commerce systems.

References:

[1]Q. Xiao, *Security Issues in Biometric Authentication*, Workshop on Information Assurance and Security. United States Military Academy, West Point, NY, USA: Proceedings of the IEEE, 2005.

[2] Verified By Visa, *A simple password protected identity checking service*. http://www.visaeurope.com/merchant/handlingvisapayments/cardnotpresent/verifiedbyvisa.jsp 03.12.2009

[3] MasterCard SecureCode, *Credit Card Security: Safe & Secure Online Shopping*.http://www.mastercard.com/us/personal/en/cardholderservices/securecode/index.html 03.12.2009

[4] JCB Global Site, *E-Commerce Solution J/Secure*.http://www.jcb-global.com/english/solution/ec.html 03.12.2009

[5] An article by Miles Brignal, *Verified by Visa scheme confuses thousands of internet shoppers*, Money news & features, The Guardian, 21 April 2007. http://www.guardian.co.uk/money/2007/apr/21/creditcards.debt 03.12.2009

AUTHOR'S PROFILE

Dr.M.Umamaheswari,M.C.A.,M.Phil.,M.Tech.,Ph.d. works as the professor & Head of department of CSE of Bharath University, Chennai, Tamil Nadu. She has more than 12 years of teaching and research experience and her areas of specialization are Computer Networks, Networks Security and Data Mining.

Mr.S.Sivasubramanain,M.SC.,M.Tech., pursuing Ph.d. as an Asst.professor from Department of CSE of Bharath University, Chennai, Tamil Nadu. He has more than 8 years of teaching and research experience and his areas of specialization are mobile computing, Database Management System, Computer Networks, Networks Security and Data Mining.

Mr.B.Harish Kumar . Now pursuing M.Tech in Computer Science & Engineering at Bharath University