INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 4 ISSUE 2 (2018) PAGES 3021 - 3024
RECEIVED : 28.02.2018 PUBLISHED : 29.03.2018

March 29, 2018

CARDLESS TAKEAWAY USING FINGER PRINT

[1]Krithika .V, Department of Computer Science and Engineering, Kumaraguru College of Technology, Coimbatore.

[2]Lotica Iyer, Department of Computer Science and Engineering, Kumaraguru College of Technology, Coimbatore.

[3]Madhumitha .V, Department of Computer Science and Engineering, Kumaraguru College of Technology, Coimbatore.

ABSTRACT

In today's fast moving world, customers spare no time for payments once they are done choosing products from retail shops or meals at a restaurant. The main objective of this project is to develop a finger print based billing system for billing application. Most of the shops are suffering due to billing and return payment for customers during the time of sales. This makes customer more uncomfortable during the time of transactions. Some of the customers will be regular to some shops, even they may purchase in the shop regularly. These users can register in this application for regular usage. The registration has been done via finger print sensor and centralizing the data in the application. A banking application will be interface with this application for payment detection. After registration, now user can do payment through their finger print. The amount will get reduce directly from the user's bank account. Now the transaction has been make simple with a Biometric device.

Keywords: Finger Print Authentication, Bio metric process, Virtual banking process, centralizing the data.

1. INTRODUCTION

Biometric technology can strengthen security of a POS (Point of Sales) system by deploying a superior authentication method. A fingerprint scanner, being the most cost effective, secure and easy to install biometric authentication method, can add an extra layer of security to a POS system. Fingerprint authentication might look like new technology on smart phones and tablets, but as a matter of fact, it is relatively old and has been used at various fronts where secure authentication or identification is required.

Since POS systems process a number of credit / debit card transactions, they are always a target for information theft. Adding fingerprint authentication to a POS system ensures user accountability if any incident takes place. Traditional Login ID and passwords based protection pose more chances of compromising sensitive data like card details in comparison with fingerprint authentication. With fingerprint biometrics, users cannot use someone else's credentials to login into the POS system. If a user tries to manipulate the system or install a malware, it can be easily caught.

Fingerprint authentication with proper surveillance can also encounter cases of employee thefts. It also eliminates buddy punching and increases payroll efficiency. Fingerprint authentication for logging into a POS system can deter any malicious attempts to steal information or abusing the system. All the areas of a POS system, where password authentication is a requirement, can be replaced with fingerprint authentication. It provides superior security as compared to passwords, which can be shared, forgotten and even stolen. Once integrated with the software and hardware, fingerprint scanner takes charge of POS security and all personnel have to scan their fingerprint before they can access or use the POS terminal. Use of fingerprint scanner in a point of sale system also makes it future-proof for fingerprint based payments, which are expected to gradually replace card based payments.

2. RELATED WORKS

Biometrics identify people by measuring some aspect of individual anatomy or physiology (such as your hand geometry or fingerprint), some deeply ingrained skill, or other behavioral characteristic (such your handwritten signature), or something that is a of the two (such as your voice).[15] Biometric authentication technologies such as face, finger, hand, iris, and speaker recognition are commercially available today and are already in use.[16] A biometric system is essentially a pattern recognition system that operates by acquiring biometric data from an individual, extracting a feature set from the acquired data, and comparing this feature set against the template set in the database. Depending on the context, a biometric system may operate either in verification mode or identification mode: [17] In the verification mode, the system validates a person's identity by comparing the captured biometric data with her own biometric template(s) stored system database. In such a system, an individual who desires to be recognized claims an identity, usually via a PIN Personal Identification Number), a user name, a smart card, etc., and the system conducts a one-to-one comparison to determine whether the claim is true or not (e.g., "Does this biometric data belong to Bob?"). Identity verification is typically used for positive recognition, where the aim is to prevent multiple people from using the same identity. [19] In the identification mode, the system recognizes an individual by searching the templates of all the users in the database for a match. Therefore, the system conducts a one-to-many comparison to establish an individual's identity (or fails if the subject is not enrolled in the system database) without the subject having to claim an identity (e.g., "Whose biometric data is this?"). Identification is a critical component in negative recognition applications where the system establishes whether the person is who she (implicitly or explicitly) denies to be. The purpose of negative recognition is to prevent a single person from using multiple identities. Identification may also be used in positive recognition for convenience (the user is not required to claim an identity). While traditional methods of personal recognition such as passwords, PINs, keys, and tokens may work for positive recognition, negative recognition can only be established through biometrics. [19].

3. FINGER PRINT WORKING MODEL

Biometric payment technology allows the consumer to pay with the touch of a finger on a fingerprint scanner linked to a payment file. The fingerprint template is typically linked to a router and transmission media necessary to clear the transaction through an automated clearinghouse. While many biometric payment transaction providers focus on grocery, home improvement and convenience stores, others have indicated interest in quick-serve eateries, car wash locations and select vending operations. Biometric payment providers (e.g., Pay-by-Touch and BioPay) require completion of a preenrollment process in which index fingers are scanned and driver's license and banking information is recorded in an account database. This process reportedly takes less than two minutes. In addition to transaction settlement, biometric payment providers may also link captured transactions to loyalty reward programs, gift cards, discount coupons and Web access services.

FINGER PRINT AUTHENTICATION

Fingerprints are important. By 1998, fingerprint recognition products accounted for 78% of the total sales of biometric technology. These products look at the friction ridges that cover the fingertips and classify patterns of minutiae, such as branches and end points of the ridges. Some also look at the pores in the skin of the ridges. Fingerprint recognition devices for desktop and laptop access are widely available from many different vendors at a low cost. [15] The relatively small size allows the sensor to be integrated in other devices (e.g., mice, keyboards). This biometric technology uses the pattern of friction ridges and valleys on an individual's fingertips. These patterns are considered unique to a specific individual. The same fingers of identical twins will also differ. A user does not need to type passwords - instead, only a touch to a fingerprint device provides almost instant access (typically less than 1 sec.). A typical enrollment identifier may include 2 finger samples (e.g., 1 KB) although smaller finger samples are also used. One of the challenges of fingerprint technology is individuals that have poorly defined (or tenuous) ridges in their fingerprints. [16]

4. PROPOSED ARCHITECTURE

A. System Input The input of our system is simply Finger print of the user. The Finger Print is taken by the System. The Embedded System have Thumb Scanner which takes finger-print of Thumb. It scans valleys and ridges on the thumb. It locates the points on the thumb where two ridges are separated or meeting together. B. Transaction Based on the Authentication, the system will allow access to the user. In the biometric authentication system, identification and verification is done at the same time. After getting verification, the system will ask for the product and it shows the price of it. After getting Confirmation, system automatically deducts the amount from the bank which is attached to that UID (Unique Identification) Number. Output and Analysis After Transaction, the system will generates the bill with information like Product details, Price, etc., at the same time, the bank sends the acknowledgment to the user via SMS service. After that, the system will be closed and it will be ready for next user. Organization of the system will generates the reports which can help to improve it by analysing them.

CONCLUSION

The Proposed system using Biometrics, the security and potential of existing E-payment system will be enhanced. This system will be generic and it can be used by multiple services like payment of hotels, restaurants and etc. Due to this, paying users will be able to make fair and accurate decisions for payments. Optimized strategies extracted from these decisions can be developed to increase potential and profit of Organization. Hence, this paper presented a type of this kind of epayment system i.e., biometric e-payment system that can be easily implemented. Meanwhile, the full implementation of such a model will help to achieve our objectives like security, efficiency, reliability and easy-to-use e-payment system by many people in the world.

REFERENCE

[1] http://www.zdnetasia.com/news/security/0,39044215,62011592,00.htm

[2] http://www.zdnetasia.com/news/security/0,39044215,61965886,00.htm

[3] http://fingerprint-it.blogspot.com/

[4] Alex Halperin: “Biometrics: Payments at Your Fingertips”, Wednesday, March 29, 2006.

[5] Julia Scheeres: “Will It Be Cash, Check or Finger?”

[6] David H. Chang: “Fingerprint Recognition through Circular Sampling,”

[7] http://www.techdirt.com/articles/20060125/0922251.shtml

[8] Matthew Boyle, Wal-Mart, “Costco weigh merits of allowing customers to pay by scanning fingerprints:”

[9] Ellen McCarthy: “Washington Post Staff Writer”.

[10] MARK ALBRIGHT: Times Staff Writer

[11] Should Minneapolis get tougher on panhandlers? http://twincities.bizjournals.com/twincities/stories/2005/05/09/daily57.html

[12] Jennifer Maselli: “Supermarket's biometric system will scan shoppers' fingertips”

[13] Michael L. Kasavana : “Biometric Scanning Offers Vending New Payment Options”

[14] SalilPrabhakar, Anil Jain: “Fingerprint Identification”

[15] Ross Anderson's: “Chapter 13th Biometrics of Security Engineering”.

[16] Fernando L. Podio: “Personal Authentication Through Biometric Technologies”

[17] Anil K. Jain, Arun Ross and SalilPrabhakar: “An Introduction to Biometric Recognition” IEEE Transactions on Circuits and Systems for Video Technology, Special Issue on Image- and Video-Based Biometrics, Vol. 14, No. 1, January 2004.

[18] Dileep Kumar, Dr.YeonseungRyu, Dr.Dongseop Kwon: “A Survey on Biometric Fingerprints: The Cardless Payment System” IEEE ISBAST April, 2008.

[19] L. O'Gorman, “Seven Issues With Human Authentication Technologies”, Proc. of Workshop on Automatic Identification Advanced Technologies (AutoID), pp. 185-186, Tarrytown, New York, March 2002.

[20] http://www.secprodonline.com/articles/52819/