CSCanada
International Business and Management
Vol. 16, No. 2, 2018, pp. 48-51
DOI:10.3968/10838

ISSN 1923-841X [Print]
ISSN 1923-8428 [Online]
www.cscanada.net
www.cscanada.org

Biometric Fingerprint Replaces PIN code on Point of Sale Machines in the Kingdom of Bahrain

Yousuf Janahi[a],*

[a]College of Administrative Sciences, Applied Science University, Kingdom of Bahrain, Manama, Kingdom of Bahrain.
* Corresponding author.

Received 10 September 2018; accepted 22 November 2018
Published online 26 December 2018

Abstract

Payment for goods and services in most of the outlets in the Kingdom of Bahrain can be made through cash, credit card, cheques, and also through ATM card (Automatic Teller Machine), electron cards (VISA/ MASTER, etc) by using Point Of Sale (POS) machines. POS is one of the most popular methods and requires swiping your card and entering your personal identification number (PIN) in the key pad of the POS machine. A POS machine is a single factor for authentication which is an inadequate process for many customers. This paper reports an investigation on I.T professionals and bank customers toward the acceptance of such technology using a biometric fingerprint instead of a PIN code. A qualitative method is used in this paper to gain an insight into user's feedback and perception on the existing and proposed solution.

Key words: Banking; Information Security; Biometric; Fingerprint

Janahi, Y. (2018). Biometric Fingerprint Replaces PIN code on Point of Sale Machines in the Kingdom of Bahrain. *International Business and Management, 16*(2), 48-51. Available from: http://www.cscanada.net/index.php/ibm/article/view/10838
DOI: http://dx.doi.org/10.3968/10838

INTRODUCTION

POS systems and peripherals are increasing dramatically in numbers from year to year in Bahrain. Plastic card theft has left consumers afraid of fraudulent use as the majority of merchants do not verify the identity of the card holder, especially if it is a credit card which does not need the customer to enter their PIN code if 3D secure was not in use. This paper discusses adopting a biometric technology having a better authentication when using a plastic card. Biometric technology is growing very rapidly in US and Europe and being readily accepted by the customer. Hence a survey is conducted with both customer and I.T professionals in order to identify to what extent biometric technology may be accepted by the customer in Bahrain. The findings should be useful for enhancing security methods. The discussions should be of considerable interest to bank markets, information technology planners, retailers, researchers and the consumers.

1. BIOMETRIC SYSTEM

Biometric-based personal authentication systems that use physiological (e.g., fingerprint, face) or behavioral (e.g., speech, handwriting) traits are becoming increasingly popular, compared to traditional systems that are based on token (e.g., key) or knowledge (e.g., password) (Jain & Pankanti, 2006). Biometrics are an automatic identification which includes fingerprint, voice iris, retina, hand, face, handwriting and keystroke (Wayman, Jain, Maltoni, & Maio, 2005). Fingerprints are one of the most mature biometric technologies and are considered legitimate proofs of evidence in courts of law all over the world (Jain & Pankanti, 2006). The past 20 years has seen the introduction of a variety of personal computer-friendly fingerprint scanners with ever decreasing price points, making them more and more affordable for use in a wide variety of commercial applications (see figure 2) (O'Gorman, 2000). Biometrics by themselves are insufficient as an information security mechanism (Chandra & Calderon, 2005). The architecture of a fingerprint-based automatic identity authentication system consists of four components; user interface, system database, enrollment module, and authentication

module (Jain & Pankanti, 2006). The implementation of automated fingerprint identification system (AFIS) in 1960 established the first application of biometrics where the Automation of identity verification was based on the ten print cards. In 1980's forensic DNA profiling was discovered where identity Verification was done on the basis of DNA reference material using a Computerized DNA database (Saini and Kapoor, J. Forensic Med, 2016).

2. FINGERPRINT MODELING

A biometric system may be called either a verification system or an identification system. Verification conducts one-to-one comparison to determine whether the identity claimed by the individual is true (am I whom I claim I am?) but an identification system recognizes an individual by searching the entire template database for a match (who am i) (Wayman, Jain, Maltoni, & Maio, 2005).

In the forensic context, a test sample obtained from a crime scene is referred as crime scene sample, traces material and questioned item whereas the reference sample that is compared against the crime scene sample is named controlled material or known item. Some of the trace samples (biological traces, finger marks, earmarks, bite marks and lip marks) are collected physically while others are acquired digitally (face, voice, body measurements and gait) (Saini and Kapoor, J. Forensic Med, 2016).

The model creation implements some patent-pending security features to protect the users of the fingerprints, therefore the first feature is to create models with the capability of distinguishing between enrollment templates and authentication models. Another security feature is that the original fingerprint image is destroyed and cannot be obtained after it is converted into a unique mathematical template or model1. Fingerprints were much harder to recognize than the face images due to the lack of many distinct features. While everyone has unique fingerprints, it is more challenging for a computer to distinguish them since they all hold similar lines. Furthermore, with even a slightest amount of noise, a fingerprint of one person may become more similar to a fingerprint of another person due to overlap of the lines in the matched areas (Bouchaffraa & Amira, 2008).

3. APPLICATIONS OF FINGERPRINT RECOGNITION

Fingerprint recognition is a rapidly evolving technology that has been widely used in forensics such as criminal recognition and prison security, and has a very strong potential to be widely adopted in a broad range of civilian applications.

Traditionally, forensics applications have used manual biometrics, government applications have used token-based systems, and commercial applications have used knowledge-based systems (Wayman, Jain, Maltoni, & Maio, 2005). The emerging interaction is expected to be influenced by the added value of the technology, the sensitivities of the user population, and the credibility of the service provider. The current research aims to predict where and how fingerprint technology would evolve and be mated with applications, but it is certain that fingerprint-based recognition will have a profound influence on the way we will conduct our daily business (Wayman, Jain, Maltoni, & Maio, 2005).

4. PRIVACY, SECURITY AND AUTHENTICATION

Biometric Identity Assurance Services (BIAS) standard stresses the importance of securing distributed systems since web services interaction is usually performed through open networks or intranets (Sanchez-Reillo, Heredia-da-Costa, & Mangold, 2018). There is a little doubt that in the coming years, more government agencies will begin using biometric technology to increase the perception of security and to assist their service delivery systems (Nuger & Wayman 2005). When considering the security of a fingerprint recognition system, the entire system must be looked at, and not only attacks with artificial fingerprints (Sandstorm, 2004). Referred to the specific implementation of BIAS, it would be interesting to add encryption of biometric data being transferred, as they are the most valuable assets (Sanchez-Reillo, Heredia-da-Costa, & Mangold, 2018).

The authentication phase has three steps, Initial step is the input: The user inputs his/her fingerprints and password to verify the authorized user. This step and first step of the registration phase are the same. Step 2. Create new template: Create new fingerprint template based on present input information to compare to the fingerprint template stored in the server. Step 3. Comparison: to comparison the stored fingerprint template and the new one in step 3. The existing fingerprint recognition system compares two fingerprint templates by rotation, until most minutiae are matched. However, this scheme compares two fingerprint templates, only once due to standardization (Sanchez-Reillo, Heredia-da-Costa, & Mangold, 2018). In case of card less ATM plastic cards, biometric uses typical biometrics authentication process in which involves: Firstly the creation of the user's biometric sample i.e. fingerprint recognition (Middle finger) etc. and its storage in the user database in respective account holder's bank. During the actual authentication, the user is required to provide a sample of the same nature i.e. finger print etc.

1 BIO-Key International, a fingerprint based biometric algorithm, and how it can be incorporated into today's identification and security solutions, 2003.

with its Personal Identification Number (PIN) and selected bank branch in café Centre (ATMs) then system will generate code called virtual account identification (V-ID). This is usually sent across in encrypted form (e.g. using SSL) through network to the server. On the server side, the user's current sample is decrypted and compared with the one stored in the database. If the two samples match to the expected degree on the particular values, the users is considered as authenticate user and proceed further for transactions, otherwise user is considered as invalid user and then terminates session.

5. KINGDOM OF BAHRAIN

The majority of people in Bahrain are using POS wherever they do shopping and this becomes an essential element of the payment method. National Bank of Bahrain, Credimax and Ahli United Bank are the authorized acquirers in the market for all POS terminals distributed at most merchant outlets in Bahrain. For the last two years the Central Bank of Bahrain (CBB) has regularized that all banks must be capable of using other ATM and POS machines regardless of being their customer. CBB has instructed all banks in the Kingdom any surcharge of using own or other banks ATM unlike POS transactions; a surcharge of 3% charged on the merchant. In January 2006, there was a fraud incident in Bahrain by two fraudsters who used cameras and fake screens at the ATMs to capture information on people's cards[2]. The first payment method in Bahrain is cash. Cash is often less expensive to accept. The cost to a merchant of accepting cash payments are primarily attributable to reconciling cash drawer balances, insurance required for cash transportation, and security. The second method is cheques which are preferred by many consumers. Cheques are still a convenient payment option, however many merchants do not accept cheques from personal accounts as this has resulted in many cases where individuals had insufficient credit in their accounts. The third method is paying through credit cards which are accepted in most merchant outlets using POS machines. Credit cards are not only accepted at major retail stores but also at grocery stores. Consumer demand for this type of payment decreases the cost of the transaction required for acceptance. The forth method of payment is through a debit card which is widely used by consumers, the infrastructure required for debit card and or ATM transactions is similar to that required for credit cards. Debit or ATM cards are widely accepted in Bahrain. Debit/ATM cards are used overall POS machines outlets using online PIN authentication. As mentioned earlier that the surcharge of 3% on all transactions applied on POS machines is paid by the merchant.

2 Gulf Daily News – kingdom of Bahrain, (2006), *Fraud Incident*, available http://www.gulf-daily-news.com [Accessed in January 2006].

6. RESEARCH METHOD

Bahrain has one of the highest levels of shopping using plastic cards within the gulf region and has a constantly growing part of its population using POS technology. Therefore, a customer always needs confidence and trust towards shopping using plastic cards. A qualitative study was selected in this paper to obtain customer perception related to improvement of the security mechanics. A judgmental sampling was used in this study by interviewing key people in the I.T sector and frequent users of POS outlets of both major banks. The interviews took place with e-commerce department heads, I.T heads of the two major banks, legal advisor, sales people, clerks and academic staff. All the said were selected to obtain a comprehensive overview of the perceptions of implementing a biometric technology.

7. FINDINGS

As previously mentioned, one of the key objectives of this study is to gain customer and professional insight into consumer acceptance of biometric technology and whether it will be convenient and easy to replace the PIN code with a fingerprint. The outcome was almost in agreement with a causation of their privacy and data disclosure. The findings took almost a month and half in order to complete all the interviews. For the last three years e-commerce has grown in Bahrain and is frequently an independent division or department in both government and private sector. The first interview was with a major bank e-commerce division head who had transparently answered the questions related to replacing the PIN code with fingerprint authentication mechanism. He was fully agreed with a biometric technology in terms of security, authentication enhancement and customer convenience but said that the implementation and customer acceptance will require quite a time to be accepted as there are a lot of concerns from the customers such as trust, ease of use, privacy etc. I.T heads in general noted that new technology will be able to be cost-beneficial at first, secondly that biometric technology will eliminate humans from the process and thirdly they emphasized on security enhancement in protecting the customer and the bank. The legal advisor interview was done in order to obtain a legal point of view in terms of legal issues related to fraud and privacy misuse. The legal advisor opinion was that as a technology biometrics will improve and enhance security and this will build a confident bridge between the bank and the customer. The legal advisor had no clear evidence that the Kingdom has issued such legal support toward misusing or fraudulent related plastic cards or captured fingerprint in Bahrain. Other interviewees were the clerks; sales representatives and academic staff, their main concerns were customer training, awareness, privacy and disclosure of a person's fingerprint. The academics

indicated that the bank should train and educate the customer before implementing such enhanced technology, otherwise this will lead to customer frustration.

CONCLUSION

The deployment of POS terminals using biometric fingerprints will require further development of stronger criteria for cost and benefit assessment, security assurance, and privacy protection. The challenges in implementing such technology need a holistic solution that satisfies the customer, bearing in mind the main key factors such as trust, privacy and legal issues in the Kingdom of Bahrain. Private and government sectors have recently used a wide array of initiatives to increase public safety and confidence such as staff attendance, police evidence etc. The accuracy and reliability of the identification is an important issue in crime and cyber security today's issues. The biometric recognition is emerging as a sound scientific justifiable tool in investigative procedure as well. It holds future potential to solve the criminal activities. However, replacing the PIN code with a fingerprint will be a future use.

REFERENCES

Bhosale, S., & Sawant, B. (2012). Security in e-banking via card less biometric ATMs. *International Journal of Advanced Technology & Engineering Research* (IJATER). ISSN No: 2250-3536.

Bouchaffraa, D., & Amira, A. (2008). Structural hidden Markov models for biometrics: Fusion of face and fingerprint. *Pattern Recognition, 41*, 852- 867.

Chandra, A., & Calderon, T. (2005). *Diffusion of biometrics in information systems, 48*(12).

Gulf Daily News – kingdom of Bahrain. (2006). *Fraud incident*. Available http://www.gulf-daily-news.com [Accessed in January 2006].

Intell Manuf, J. (2014). Construction of a secure two-factor user authentication system using fingerprint information and password. doi: 10.1007/s10845-012-0669-y.

Jain, J., & Pankanti, S. (2006). Fingerprint classification and matching. Available http://citeseer.ist.psu.edu/jain00fingerprint.html [accessed in March 2006].

Maltoni, D., Maio, D., Jain, A., & Prabhaker, S. (2005). *Handbook of library of fingerprint recognition.* Congress Cataloging-in-Publication Data.

Nuger, K., & Wayman, J. (2005). Biometric and the US Constitution, Biometric Systems – Technology, Design and Performance Evaluation, 311-333.

O'Gorman, L. (2000). Practical systems for personal fingerprint authentication. *IEEE Computer, 21*(2), February 2000, 58-60.

Saini, M., & Kapoor, A. K. (2016). Biometric in Forensic Identification: Application and Challenges. doi: 10.4172/2472-1026.1000108.

Sanchez-Reillo, R., Heredia-da-Costa, P., & Mangold, K. (2018). *Developing standardised network-based biometric services.* ISSN 2047-4938.

Sandstorm, M. (2004). *Liveness detection in fingerprint recognition systems Linloping.*

Wayman, J., Jain, A., Maltoni, D., & Maio, D. (2005). *Introduction to biometric authentication systems, technology, design and performance evaluation.* ISBN: 1-85233-566-3.