A SOPHISTICATED BIOMETRIC BASED DIGITAL TRANSACTION SYSTEM WITH SECOND-LEVEL AUTHENTICATION

M.Sreelatha[1], Dr. M.V. Lakshmaiah[2], B.Bilvika[3], Dr. Harish Kalla[4]
Research Scholar[1], Head Department of Physics and Electronics[2], Research Scholar[3], GF[4]
Department of electronics
Sri Krishnadevaraya University, Anantapuramu-515003, India.

Abstract

In this project we propose a design, to add more security to the current digital transaction systems by using biometric and Random finger generation technology. In conventional method, identification is basing on ID cards and static 4 digit password. Whereas in our purposed system, Bankers will collect the customer fingerprints and mobile number at the time of opening the accounts then only customer will be able to acc.ess digital transaction machine. The primary step of this project is to verify current scanned fingerprint with the fingerprint which is registered in the bank at the time of account opening. If the two fingerprints get matched, then a proposed system generate random finger (out of 10 hand fingers) to access the account. For every transaction new random finger will be generate display on the user's screen thus there will not be fixed finger for every transaction. Thus, finger number will vary during each transaction.

Keywords: Biometric, Raspberry pi3, Digital Transactions, Credit cards, Touch Screen

INTRODUCTION:

Electronic Point of Sale (POS) equipment which includes products used in the electronic processing of financial transactions in the retail, hospitality and banking segments. Different products in the POS space are card payment terminals, electronic cash registers, self-service kiosks, vending machines and accessories like card readers, pin entry devices and printers.

The main feature of a POS terminal revolves around the reading of contact and contactless cards while securely transmitting the information – including the transaction - to a server for authentication and approval. Today, most of the POS systems transmit transactions to their network over a tethered connection but there is a growing demand for a portable / mobile solution.

In the fingerprint, verifications play vital role in forensic application, criminal's investigation, terrorist identification, or any other security purpose. So in fingerprint verification is roved that it is one of the most reliable personal identification.

Biometric system is able to identifying accurately an individual based on his/her distinctive physiological (e.g. Fingerprint, face retina, iris) or behavioural (e.g. gait, signature, ATM) characteristics. Fingerprint verification methods include minutiae-based and image-based methods. The system is undoubtedly improves the fingerprint verification is based on these method so in addition to hybridization it also useful to fingerprint verification because fingerprint recognition which refers to the automated method for verifying a match between two human fingerprint. Suppose the twins are uses same account though they use same account but their fingerprint (thumb impression) different. We know about that when we use the biometric, same like that ATM.Using the ATM when provide customer with the convenient banknote trading is very common. However, the financial crime tamper with the ATM terminal, steal user's credit cards and password by illegal means. Suppose by mistake one user's card is lost and the password stolen, then the criminal draw all the cash in the shortest time [9. It is very difficult to carry the ID cards or ATMs at ATM Machines. Thus it is very much important that the biometric thumb impression gives the main identification proof of any unknown person. Until today, ATM security using the hybridizing method with biometric fingerprint verification. Fingerprint has

unique features for which they do not change for whole life and are personally different. They are easy to use, cheap and the most suitable for miniaturization. Therefore fingerprint verification is an efficient personal verification method that has been the most widely used in comparison with other biometric information. But all most here these two methods used.

WORKING OF BIOMETRIC SYSTEM

Biometric data and Biometric Identification combine to form Biometric System. It involves two phase. First is the enrolment Phase which is defined as the interval when the individual encounters the biometric system initially, here the subject gets their biometric information stored in the database. Since it is a single-time work it is conducted slowly and multiple times to make an accurate entry in the system. Second is the Verification Phase which involves several steps:

a) Data Collection: The very first, time consuming step where the user presents its characteristics to sensing device. In case of fingerprint or palm geometry scan requires a physical contact each time with the sensor. In schemes such as retina scan requires no physical contact.

b) Transmission: It is only carried out in open system where the sensor is located at one location and processor at the other. It involves compression of data.

c) Signal Processing or Pre-Processing: Having acquired the biometric characteristics need to prepare it for matching. It involves removal of noise and distortion.

d) Feature Extraction: The pre-processed data is re-processed once again to obtain more precise feature with reduced size.

e) Template Creation: Template defines a model or standard for making comparison. Thus, a template is created and relayed to comparison algorithm.

f) Matching: The last step involves implementation of comparison algorithms to compare the stored template of the individual with the collected sample. On the basis of this comparison the decision to grant or deny access is made.

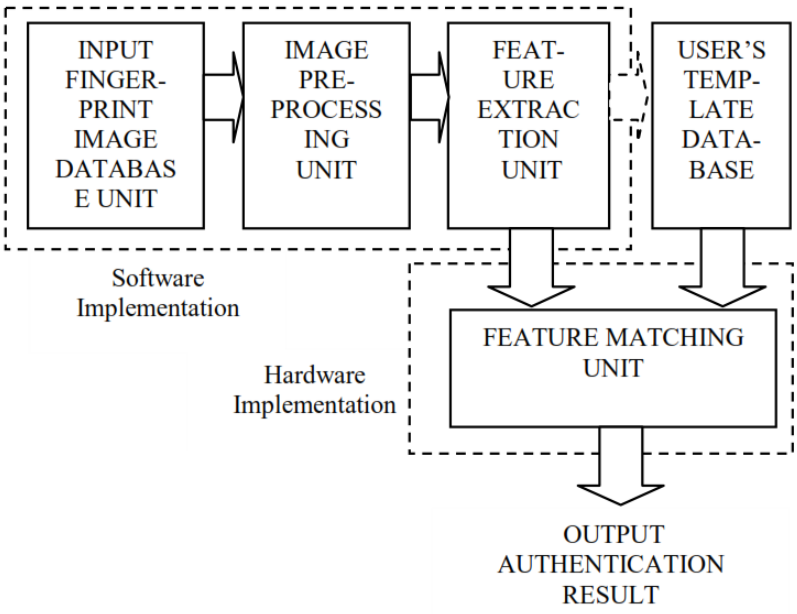

Figure-1: Biometric Extraction System.

BLOCK DIAGRAM:

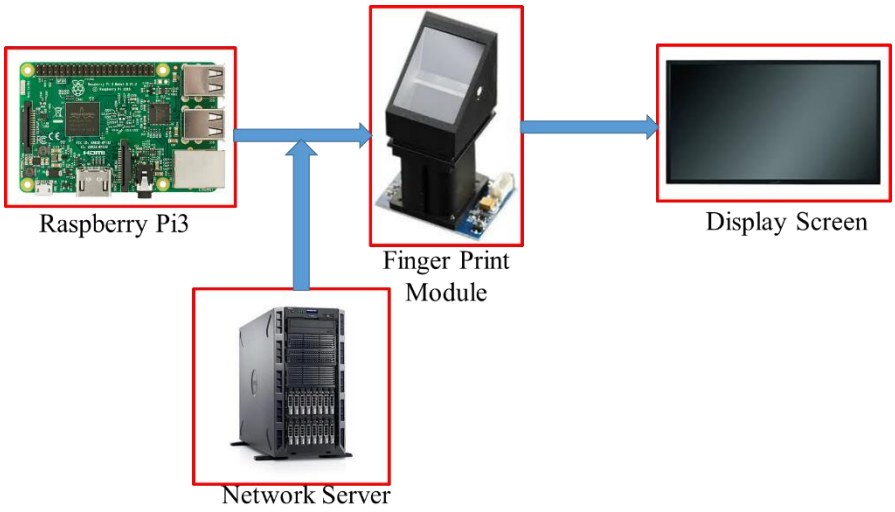

Figure-2: Block diagram of proposed biometric digital transaction system

DESIGN OF THE PROPOSED ATM AUTHENTICATION PROTOCOL:

The current ATM authentication protocol has a couple of security challenges and issues. An attacker may install a card swipe device "skimmer" that has the capabilities to read the information stored on an ATM card. Then, it sends PIN numbers to the attacker within a closed area (e.g., wireless coverage). He could possibly place a spy camera (a small CCD camera) to analyze videos to obtain a user's PIN number while a user enters it into an ATM terminal.

Furthermore, he may produce a fake or cloned ATM card to gain unauthorized access to a user's account; and consequently steal money. In some cases, an attacker may figure out the encryption mechanism of the PIN number especially if the same bank issued it. Then, he could determine the target PIN number. Lastly, he may install a fake ATM's keyboard in the top of a real ATM's keyboard; and this fake keyboard stores all entered keys (including PIN numbers) with their associated time.

Security related researchers have started thinking about employing a mobile phone device to develop approaches that may increase the level of assurance in accessing critical information by users such as accessing an ATM terminal. Enhancing the security level of the ATM authentication mechanism by using biometrics on a mobile phone device is attracting attention due to the increasing number of users adopting mobile technologies.

The primary goal of our proposed protocol is not to replace the current ATM authentication protocol rather it proposes a model for more secure ATM authentication using biometrics on a mobile phone device under the restriction that no changes can be made to the existing physical infrastructure (i.e., a mobile network, an ATM terminal and a bank network).

The proposed authentication protocol provides an additional security layer by using a combination of two authentication methods (a multifactor):

- Something you know (a PIN number).
- Something you are (a biometrics feature "fingerprint ").

The proposed ATM authentication protocol offers more features over the existing one. It requires no modification or change in the current infrastructure setup. Thus, it utilizes the current communication channel between the ATM terminaland the banking system. Additionally, it does require adding only one new hardware to the existing ATM components.

It just needs to update the current software of the ATM terminal with a new feature that encodes fingerprint codes and displays them in the screen. It uses a biometric feature as a second level of authentication. Furthermore, the matching process between the captured biometric feature and the stored template is not applied as the biometric data is used only for reserving the secret key at the mobile phone device side.

A. Assumptions

As part of the registration and enrolment process, a user has to subscribe for a biometric service at his bank. Then, thebank activates and creates a user's profile based on his ATMcard, PIN number and a biometrics feature (fingerprint).

During the authentication process, a user's biometrics feature (fingerprint) needs to be captured. From security perspective, we assume that a use ccesses his fingers in a secure way. Also, the connection between an ATM terminal and a bank network is secured (in most cases leased line, satellite or fast dial-up link).

B. System Architectural Components and Design

The architecture of the proposed authentication consists of a genuine bank's customer, an attended terminal hardware with an added finger code image display feature, a banking system that has transactional database for money withdraw aland stores user bank information, an ATM card information(PIN number, card number…) and user's biometrics feature(fingerprint), a valid fingerprint with a valid PIN number, and lastly a random finger images from the ATM terminal screen as well as acts a sensor that captures biometric feature (fingerprint or face). Our proposed authentication process is accomplished through three main phases (sub-protocols): registration and enrolment protocol, authentication protocol and transaction authorization protocol respectively.

CONCLUSION:

The use of the biometric as a password has made the digital transaction system more reliable and secured. The random generation concept added to the system further enhances the security and avoids the need for us to remember passwords. Moreover the system is built on embedded technology which makes it user friendly and non-invasive. Using this system the ATM terminal is secured from fire and thief attacks.

References

[1] Anil K. Jain, Karthik Nandakumar, and Abhishek Nagar, Review Article: Biometric Template Security, Journal on Advances in Signal Processing Volume 2008, Article ID 579416.

[2] Debnath Bhattacharyya, Rahul Ranjan1, Farkhod Alisherov A., and Minkyu Choi, Biometric Authentication: A Review, International Journal of u- and e- Service, Science and Technology, Vol. 2, No. 3, September, 2009.

[3] http://biometrics.gov/Documents/Glossary.pdf, National Science and Technology Council's (NSTC) Subcommittee on Biometrics, Biometrics Glossary, 2006.

[4] "BCM2835 Media Processor; Broadcom". Broadcom.com. 1 September 2011. Archived from the original on 13 May 2012. Retrieved 6 May 2012.

[5] Brose, Moses (30 January 2012). "Broadcom BCM2835 SoC has the most powerful mobile GPU in the world?". Grand MAX. Archived from the original on 18 February 2012. Retrieved 13 April 2012.

[6] Shimpi, Anand Lal. "The iPhone 3GS Hardware Exposed & Analyzed". Retrieved 2018-10-11.

[7] "Raspberry Pi 2 on sale now at $35". Raspberry Pi Foundation. Retrieved 5 August 2015.

[8] "Raspberry Pi 2, Model B V1.2 Technical Specifications" (PDF). RS Components. Retrieved 20 September 2017.

[9] Upton, Eben (14 March 2018). "Raspberry Pi 3 Model B+ on Sale at $35". Raspberry Pi Blog. Raspberry Pi Foundation. Retrieved 2018-05-04.

[10] "Performance – measures of the Raspberry Pi's performance". RPi Performance. eLinux.org. Retrieved 30 March 2014.