March - April 2020
ISSN: 0193-4120 Page No. 8746 - 8750

Multi-Model Biometrics in Secure Transactions

Dr. S. Angel Latha Mary[1], Mukilan N[2]
[1,2] Department of Computer Science and Engineering, Karpagam College of Engineering, Coimbatore.
[1]xavierangellatha@gmail.com,[2]mukilannarayanamoorthy@gmail.com.

Article Info
Volume 83
Page Number: 8746 - 8750
Publication Issue:
March - April 2020

Article History
Article Received*: 24 July 2019*
Revised*: 12 September 2019*
Accepted*: 15 February 2020*
Publication*: 09April 2020*

Abstract

In the present world, the process of making payments and buying products online has become inseperable.People tend to find to is easy to make online payments either through credit and debit cards or through internet banking facility provided by the merchant. Though it is making the works easier, there are multiple threats to this as well. For example, the attackers or the spoofers can use the man-in-the-middle attack, listen to the transaction and steal the credentials. There are much more ways to do them. Thus, a secure method is required to complete the transactions, that is where the proposed multi-model biometric system can be used.In this method, the user completes the transactions with either the help of fingerprint or facial recognition or both. If the users wishes to be secure and protect themselves from the attackers, they can used the proposed method and make secured transactions.

I. INTRODUCTION

In the modern world dominated by technology, mobile phones and internet transactions, their day-to-day usage is increasing rapidly not only for basic communication, but also for processing information and dealing with worldwidestuffs. By statistics, it is concluded that, there are over 6 billion mobile phone users and it is increasing day by day. It is also predicted that about 86% of the world population will have atleast one mobile phone by the end of 2020.Sometimes, mobile phones are considered a symbol of status and it has become ainseparable gadget from our life. The main reason for such a drastic increase in the number and usage of smartphone is the amount the functionality they offer regardless of price. Thus, these mobile phones with hands-free and wire-free facilities proves to be an integral part of everyone'slife. Biometric models used in the mobile phones also proves to be ainseparable part of the internet transactions for a secure method. Thus, this paper discusses the main problems that arises with internet transactions, mainly the credit card transactions and suggests a multi-model biometric transaction system, that integrates fingerprint and facial recognition system for a secured transaction method.

II. BIOMETRICS

The word biometric has its origin from Greek words "Bio" which means life and "Metric" meaning measure. Automatic biometric systems has come into existence only for the past few years due to the advancements in technology that has took place in the last few decades. Many of these biometric techniques used today are only applying new technological improvements over the conventionally used methods to identify people like fingerprints.The term biometric means the method of identifying a human based on their biological and hierarchical characteristics.Biometric is used in the computer technology for the purpose of identification and authentication.It is used to point out an individual from a group of people under control. Biometric system is a personal identification system that uses certain physiological characteristics to identify the individual and authenticate them. This method has its own advantages over the conventional password and pin methods for various reasons:

Physical presence of the person to be authenticated is required to remove impersonation.

The need and requirements to remember the

passwords and pins are removed.

Depending on the way of usage or the functionality, the biometric systems can be classified as identification system or verification system. Identification system involves the identification of person to gather information about them whereas as verification system is used to authenticate the user who claims to have that particular identity. Token-based access control is the most conventional method for access control, example: passport, and there are knowledge based identification system that requires the user to remember their passwords and PIN(Personnel identification number). Since every individual has their own biometric information, the biometric systems are more reliable than the conventional methods. However, since they have more sensitive information than the conventional method, more security measures has to be taken in order to protect those information. Conventional methods of authentication are of two types. They are, Knowledge based and possession based. In Knowledge based system, the user has to remember their own passwords, PIN and sometimes answers to security questions. In possession based methos, the users are authenticated using RFID,access cards, rolling keys etc. The main problems with those methods are as follows. In the knowledge based method, the user might share information with their trusted ones, but it removes the importance of authenticity in that case. In possession based method, the user might lose their material of authentication or forget them in home etc.

III. MULTIBIOMETRICS

A Multi-model system is obtained by the combination of multiple unimodal systems. Many models using multiple recordings of hand-strokes, iris data etc. is flooding the market over the past few years. Here we are proposing a multi-model system that uses a combination of fingerprint and facial recognition system to ensure authentication.It removes the problems of high false rejections and false positives that occurs in the case of conventional finger print method and facial recognition. It uses simple sensors to overcome the problems faced in the conventional unimodal systems. For example, in facial recognition system, there might arise some problems with aging and in fingerprint scanners , there may arise some problems with cut fingers and bruises. Broadly, the information fusion is divided into three parts, pre-mapping fusion, midst-mapping fusion, and post-mapping fusion/late fusion.Pre-mapping fusion is further classified into sensor-level or feature level fusion. Sensor-level fusion can be mainly organized in three classes:

(1) Single sensor-multiple instances,

(2) intra-class multiple sensors, (having multiple sensors within same class)

(3) Inter-class multiple sensors. (Having multiple sensors across multiple class)

Feature-level fusion can be mainly organized in two categories:

(1) intra-class (Within the same class)

(2) Inter-class. (Between multiple classes)

Intra-class is again classified into four subcategories:

(a) Same sensor-same features,

(b)Different sensors-same features,

(c)Same sensor different features, and

(d) Different sensors-different features

IV. NEED FOR BIOMETRICS IN MOBILE PHONES

Nowadays, people tend to find it easy to make internet transactions for every purchase they make online. For example, the most popular method for ordering food online is to use the food ordering online services and they provide options to order food online. Credit/Debit cards proves to be the promising method of online transactions. On the

March - April 2020
ISSN: 0193-4120 Page No. 8746 - 8750

other hand, credit card numbers are stolen in the middle of the transactions and are used by the hackers to their advantage. Thus, this makes the card transactions insecure. In addition to this,a report says that anti-fraud softwares, which promises to protect against the credit card fraudulent. But they are reported to have some backdoors that sends the credit/debit card numbers to the attackers to user them for their own advantage. Moreover, due to some unpatched bugs in the softwares and payment gateway, the attackers are able to install some Trojans and malwares to steal the card details. As the problems faced due the internet transactions increased day by day, the service providers have decided to include the biometric systems to facilitate secure eTransactionmethod.Biometric systems can be associated with the mobile phones as either a biometric data collector or a authenticator that restricts access to the unwanted users.In the first case, the data is collected and is sent to a processing place over the internet or any other communication network and is processed to find the match.This proves to be promising for remote transaction to protect the authenticity of the users. For example, the user may call a bank and recite their name. The bank system captures that voice, process the information using a combination of natural language processing and machine learning .It is then processed along with the voice data captured during the registration and further processes are done. Facial data, fingerprint and digital signatures are capable of being transferred to a remote place for processing of information.The other important biometric system which is being popularly used in the biometric systems in the mobile phones. They are of various types and have multiple functionalities like authentication of the user, protecting privacy of the user and ensuring the protection of sensitive data as well.As mentioned before, there are multiple implementations of biometric systems and they include, fingerprint recognition, facial recognition, 3D face scanning, ultrasonic authentication and iris scanner.

The advanced sensors that are being used today can be used to our advantage because of their capacity to detect physiological and hierarchical data.This provides a wide range of application which includes authentication of the user, protecting privacy of the user and ensuring the protection of sensitive data that can be used to provide a secured transaction method .

V. POTENTIAL THREATS

From the above two sections, we can say that multi-model biometrics system implementing fingerprint and facial recognition system are secure. However, we have to know what are the problems we are already facing in the existing systems and how much damage could they potentially cause.

1. POS machines: They are nothing but the Point of Sale terminals or the machines available in the shops where we can use our debit or credit card to complete the payment. This looks simple, because we just swipe the card, the magnetic reader reads the information from the magnetic strip, process it and asks for the pin number. The user then enters the pin number in the prompt and completes the transaction. However, there are potential ways to steal the user's information. They are as follows

1. There could be a small skimmer, which records the information from the magnetic strip when swiped in the POS machine.

2. There could be a logger recording the pin number

Thus, POS machines are not as safe as they seem to be.

2. Card Payments: This is another payment method wherein the user enters the Card Number, the Date of Expiry and the CVV number. After that is entered, the payment gateway processes the details with the merchant bank, the bank in turn sends an OTP to the registered mobile number. The user enters that OTP and completes the transaction. This is also simple as the previous POS method. The problem with this method is that, Man-in-the-middle

March - April 2020
ISSN: 0193-4120 Page No. 8746 - 8750

attack or sim hijacking can sniff the OTP. This may occur without the knowledge of the user and potentially cause a lot of damage.

3. RFID/NFC Payment: This is also called as tap and pay. In this method what user does is that, he can make the payment even without entering the pin and the transactions can occur up to certain limit depending on the bank. The card must have RFID/NFC enabled and the POS machine must have the same options. The main problem with this method is that, the attacker might shoulder surf the victim and complete the transaction without the knowledge of the victim

VI. PROPOSED SYSTEM

In order to overcome the above-mentioned problems we go for a multi-model biometric system. This system is classified or divided into two parts. The former being the fingerprint system and the latter being the facial recognition system. Both can operate together as an integrated process or as a separate system.

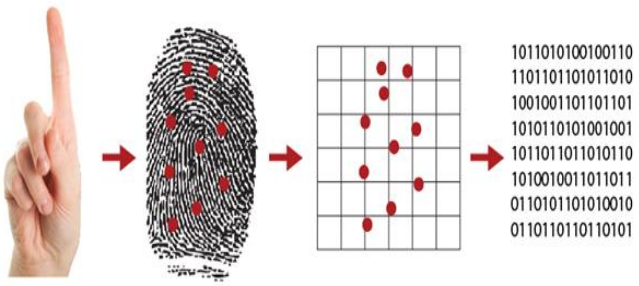
Fingerprint System:

The working of fingerprint is not complex, as it seem. There are multiple types of fingerprint scanners. They are as follows.

Physical finger scanner

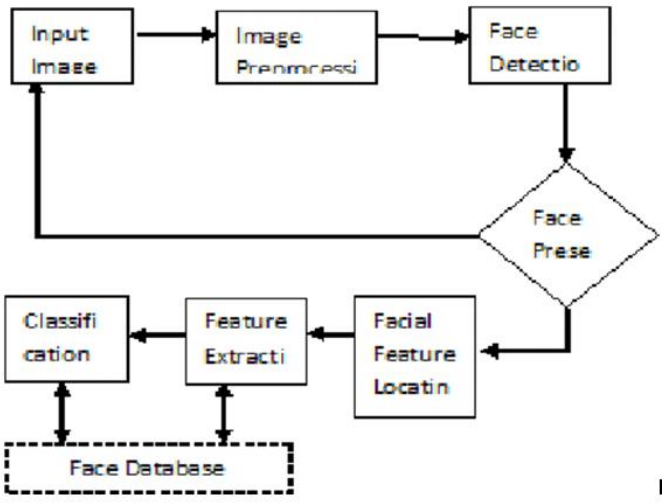
Optical scanner

The general procedure that happens in fingerprint scanners is that, when the finger is scanned, the scanners takes a stream of fingerprint data. Then it processes that information, and hashes it with the original algorithm. That hash is compared with the original hash in the database. If the data matches, the transaction can be completed else, the system must take appropriate action.



Facial System:

In facial recognition system, the user uses the camera to scan the face, Once the face data is detected , it is extracted and processes. Then the processed image is hashed. After hashing the hash is compared with the hash present in the database. If the hash matches, the transaction is processed and completed.



From the above-mentioned system, we can say that, both facial and fingerprint system can be used to complete a secured transaction.We can use either fingerprint or facial system or both at the same time as a factor of additional security.

VII. CONCLUSION:

Biometric is a newer technology to most of the people because it is implemented only for the past few years .There are various applications and functionalities of the biometric systems that used as a factor of security.It has many advantages that has made our lives a bit more secure like authentication

of the user, protecting privacy of the user and ensuring the protection of sensitive data,easy usage making our lives hazelfree.Though the conventional methods of passwords and PINs provide a good security, they have their own security concerns that make them unreliable.Thus the multi-model biometric system proposed has most of the security measures and proves to be the most promising method for secured eTransactionsand also protects the user's credit/debit card information

REFERENCES

[1]. Shuo Wang and Jing Liu , Department of Biomedical Engineering, School of Medicine, Tsinghua University, P. R.China " Biometrics on Mobile Phone "

[2]. InformaticaEconomică vol. 13, no.1 "Biometric Security for Cell Phones"

[3]. NimalanSolayappan and ShahramLatifi, Department of Electrical engineering, University of Nevada at Las Vegas, USA, " A Survey of Unimodal Biometric Methods"

[4]. International Conference on Telecommunication Technology and Applications, Kounoudes et al.,Voice Biometric Authentication for Enhancing Internet Service Security, pp. 1020- 1025, with permission from IEEE.

[5]. Bao, X.; Wang, J. & Hu, J. Method of Individual Identification based on Electroencephalogram Analysis. Proceedings of 2009 International Conference on New Trends in Information and Service Science, pp. 390- 393, ISBN 978-0-7695-3687-3, Beijing, P.R.China.

[6]. Snapshots of fingerprint security - Pro (retrieved from company release news [http://itunes.apple.com/us/app/fingerprint-securitypro/id312912865?mt=8)

[7]. Reprinted from Proceedings, 2nd International Conference on Telecommunication Technology and Applications, Kounoudes et al., Voice Biometric Authentication for Enhancing Internet Service Security, pp. 1020-1025, with permission from IEEE

[8]. (OKI introduces Japan's first iris recognition for camera-equipped mobile phones and PDAs, In: OKI Press Releases.