JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue

JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)

An International Scholarly Open Access, Peer-reviewed, Refereed Journal

BIOMETRICS TECHNOLOGY AND ITS SCOPE IN THE FUTURE

Vinod K T

Guide: Asst. Prof. Gauri Ansurkar

Keraleeya Samajam's Model College, Dombivli East, Mumbai, Maharashtra, India

vinodbhaskar1994@gmail.com

Abstract: Biometric recognition is the process of digitally recognizing a person based on their physiological or behavioral traits. The biometric system will reduce transaction security issues in e-business. Most systems such as e-business transactions require a reliable recognition system to provide services to authentic and legitimate users. Customers do not need to have a smartphone to make UPI transactions. Users do not need to have a Debit card to make an ATM transaction. This paper proposes Biometric Technology and its Future Scope. Experimental results are provided to illustrate the effectiveness of Biometric Technology. This paper presents an overview of the main topics related to biometric security technology.

Keywords: Security, Smart Phones, E-platforms, Biometrics, Fingerprint scanning. Cardless ATM Transaction.

I. Introduction

The term Biometrics is a combination of two words- bio i.e. life and metrics i.e. measurement. It refers to the metrics related to human characteristics, particularly the physical and behavioral aspects. The technology is implemented to measure and statistically analyze people's biological information mainly for their identification, access control, or surveillance. Every individual is unique and carries a separate identity in the form of traits like fingerprints, hand geometry, iris recognition, voice, etc. Biometric verification is gaining a lot of popularity among public security systems as well as in the commercial market. In our daily life, we witness the use of biometrics

in so many places such as the digital attendance system at offices, security checkpoints at airports, wearable and tech gadgets retrieving our biological information, and even our national ID cards Aadhaar cards are created using biometrics technology. In fact, this national ID program holds the largest biometric database in the world.

II. Literature Review

Biometrics technology has been extensively studied within the past few years. With the central purpose to provide a primer on this subject. Biometrics can offer greater security and convenience than traditional methods for people recognition. Even if we do not want to replace a classic method (password or handheld token) with a biometric one, we are potential users of these systems, which will even be mandatory for new passport models.

III. History of ATM

The first automated teller machine was introduced by the City Bank of New York in 1960. It was designed to allow customers to pay utility bills and receive receipts without having to visit a teller. Throughout the past three decades, consumers have increasingly relied on and trusted Automatic Teller Machines, known as ATMs, to conveniently meet their banking needs. Using an ATM, customers can access their bank accounts to make cash withdrawals, debit card cash advances, and check their account balances. In addition, they can purchase prepaid cell phone credit. Due to the convenience of banknotes, trading is very common. Many criminals have been tampering with ATM terminals and stealing credit cards and passwords in recent years, leading to an increase in financial crime cases. The criminal will withdraw all cash in the shortest time possible after stealing the user's bank card and password. This will cause the customer huge financial losses. ATM cards have largely remained the same since they were introduced in the 1960s in terms of authentication methods. A trusted hardware device is typically involved in the authentication process (such as ATM

cards or tokens). Usually, only the cardholder's Personal Identification Number (PIN) can be used to verify their identity. ATM security is threatened by a number of security pitfalls with magnetic media. I'm trying to create a prototype model where a user can verify themselves with their fingerprint and OTP for more security before accessing their account and making transactions.

IV. Automatic Teller Machine(ATM)

The term "ATM" refers to an automated teller machine. The machine allows the account holder to make transactions with their own accounts without accessing the entire bank's database. In June 1967, John Shepphardbaren invented the ATM machine at Barclays Bank in Enfield, United Kingdom. In 1987, Hong Kong and Shanghai Banking Corporation (HSBC) installed India's first ATM. Asynchronous Transfer Mode transfers data in fixed-size packets or cells. A cell used in ATM is relatively small when compared to a cell in older technologies. ATM equipment transmits video, audio, and computer data over the same network, and assures that no single type of data hogs the line. Some believe ATMs hold the solution to the Internet bandwidth crisis, but others are less sure. Data transfer between two points is initiated by an ATM by creating a fixed channel, or route. Different from TCP/IP, where messages are divided into packets and each packet can take a different route. Despite this advantage, ATM networks are less adaptable to sudden surges in network traffic because of this difference.

V. ATM Attacks

Because ATMs are such attractive targets, they are subject to a variety of attacks.

1. Physical attack: Attacking ATM machines with the intent of gaining access to cash.
2. ATM Fraud: Bank card information was stolen.
3. Software and network attack: Controlling ATMs to automatically disburse cash and steal sensitive information

VI. ATM Authentication

To continue the ATM operation, we authenticate ourselves using what we have, ie an ATM card, and what we know, ie PIN or Password. Despite this, we still do not use biometrics, such as fingerprints, retinas, etc. We usually authenticate the user with a combination of what we have and what we know. However, a password can be easily guessed or compromised, and a debit card can be lost or misplaced. Instead of using ATM cards and passwords to secure our transactions, we can use fingerprints and OTP as a more convenient way to do so.

VII. What is Biometrics

Biometrics is a method of describing a person based on quantifiable factors (or metrics) about their characteristics or traits. In computer science, this type of identification or authentication is used to identify users and control access to resources. Groups that are under surveillance can also be identified with the help of this method. Biometric identifiers are distinctive, measurable characteristics used to label and describe individuals. Because biometric identifiers are unique to each individual, they are more reliable at verifying identity than tokens and knowledge-based methods; however, the collection of biometric identifiers raises privacy concerns regarding their ultimate use.

VIII. Various Biometrics Technologies

1. Fingerprint verification

Verification of fingerprints is also known as 1:1 (one-to-one) fingerprint matching or Fingerprint Authentication and it involves verifying that an individual is who they claim to be. Typically, users provide some form of identification before placing their finger on the fingerprint scanner, such as their user ID or username. It compares the newly created fingerprint to the fingerprints associated with the user ID. Access is granted if a fingerprint match is found. When verifying fingerprints, biometric software only needs to search through one record.

2. Hand geometry

It is a form of biometrics that reads the hand or fingers of a person. In this technique, the finger and hand characteristics of the user are measured.

3. Voice verification

The technique used some types of words, keys, or numbers sought by customers at the front of ATM machines, and biometric ATM machines recognize the voice and identify the customer's voice next.

4. Retinal scanning

The retinal scanning device is one of the most accurate physical biometrics available today since there is no known way to duplicate a retina.

5. Iris scanning

The iris scan is a biometric system that analyzes the features in the colored tissue surrounding the pupil of an eye, using a conventional camera element with no intimate contract between the user and reader.

6. Facial recognition

Analyzing a person's face is known as facial recognition. A match must be found for access to be granted. Digital video cameras record the user's overall facial structure, including the distances between their eyes, noses, mouths, and jaw edges, standing about two feet from the camera.

7. Signature verification
This technology examines the dynamic of writing speed, ballpoint writing pressure, and direction of writing.

8. Vascular patterns
In vascular patterns, veins in the hand and face are portrayed in detail. Individual vein thickness and location are thought to be unique enough to verify a person's identity based on their thickness and location.

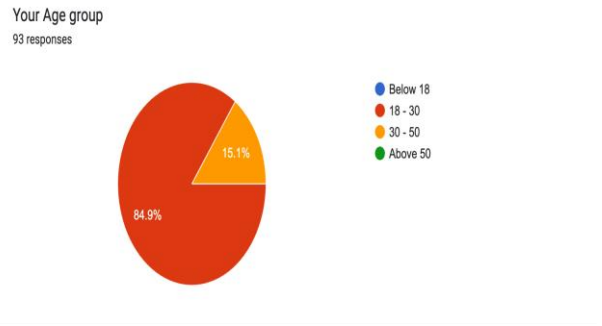
9. Palm print
Biometrics of the palm is a method that uses the physical characteristics of a person's palm to identify them.

IX. How Fingerprints are forming
Your fingerprint consists of tiny ridges and patterns on every finger. Friction ridges are present on your fingertips, palm, toes, and soles! Also known as 'dermal ridges'. The fingerprints of every individual are completely unique. The most widely accepted theory states that the middle skin layer, called the ***basal layer***, is scrunched between the inner layer (the ***dermis***) and the outer layer (the ***epidermis***). The basal layer grows faster than the other two, causing it to strain against its neighbors.This straining pressure causes the skin to buckle, resulting in the folding of the epidermis into the dermis. This shows itself in the complex ridge patterns we see on our fingers today. Ridges are the faint lines on the fingertips that create the foundation of a fingerprint.

X. Why are fingerprints unique for even identical twins?
Fingerprints are set in stone by the time a fetus reaches 17 weeks. Fingerprint pattern formation consists of two components: developmental and genetic. The ridge pattern development not only depends on genetic factors but also on unique physical conditions. So even if identical twins are genetically similar, the pressure faced by the fetus in the womb can affect their fingerprints. Even the difference in the length of the umbilical cord can make changes to the fingerprints. So ya, identical twins could fool everybody with their looks, but they ain't fooling the fingerprint test!
Innumerable environmental factors are thought to influence the formation of fingerprints, including blood pressure, oxygen levels in the blood, nutrition of the mother, hormone levels, the exact position of the fetus in the womb at particular times, the exact composition and density of the amniotic fluid that's swirling around the fingers of the fetus as they touch surrounding structures, and the pressure with which they touch their surroundings. These myriad variables decide how each individual ridge is formed.
The level of activity of a fetus and the general chaos of the conditions of the womb prevent fingerprints from developing exactly the same way in any two fetuses. The entire development process is so chaotic that, over the entire course of human history, there is virtually no chance that the exact same pattern formed twice. What this means, though, is that fingerprints are different on every finger of your hand, they're different on the same fingers of opposite hands, and even the fingerprints of identical twins are different from each other.

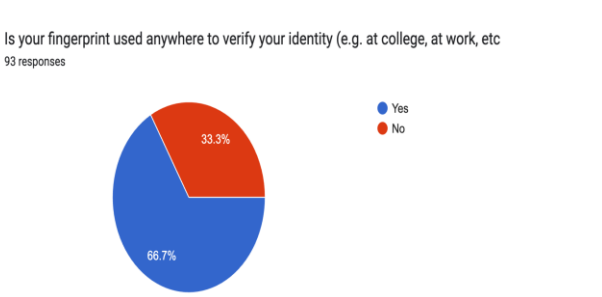
XI. Public Survey:
A. Questionnaire:
1. Is your fingerprint used anywhere to verify your identity (e.g. at college, at work, etc?
2. Does your mobile phone have a fingerprint sensor for unlocking the device?
3. If your mobile phone is equipped with a fingerprint scanner, will you use it, or will use a password to unlock it?
4. How much do you believe that fingerprint scanning is secure on a scale of 1 to 5?
5. Will you use your fingerprint to make an ATM transaction instead of a debit card, and an OTP in your mobile device for two-factor authentication?
6. Instead of using a smartphone, a fingerprint scanner at the shop, and an OTP on your mobile device for two-factor authentication, will you use your fingerprint to make a UPI payment?
7. Internet is everywhere, everything is digitalized in the 5G era. This research aims to link everything to our fingerprint in order to eliminate the need for us to carry any physical form of identification to prove ourselves at any time, such as driving licenses, and voter IDs,
8. ATM cards, passports, etc. When you lose your identity card or forget to bring it to a place where proof of identity is required, you know what it's like, In the event that you forgot to bring your passport to the airport, as you were waiting for your flight, you will miss the flight; however, your fingertips won't be far behind you. What is your opinion of the concept on a scale of 1 - 5?

B. Results
1. Your Age group?



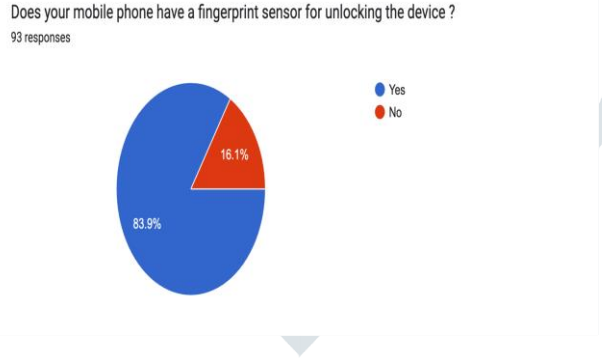
The graph above shows that 84.5% of participants were young adults (18-30), while 15.1% were older.

2. Is your fingerprint used anywhere to verify your identity (e.g. at college, at work, etc?



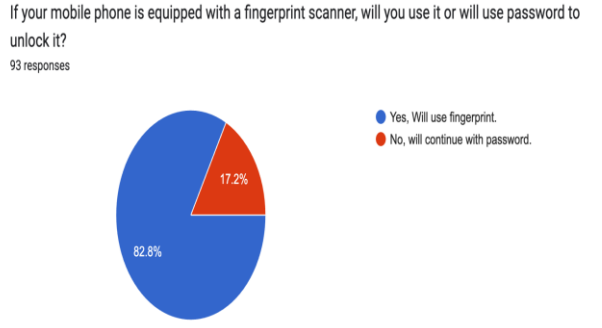
The graph above shows that 66.7% of participants already used fingerprints to identify themselves somewhere, and 33.3% were not used anywhere apart from mobiles.

3. Does your mobile phone have a fingerprint sensor for unlocking the device?



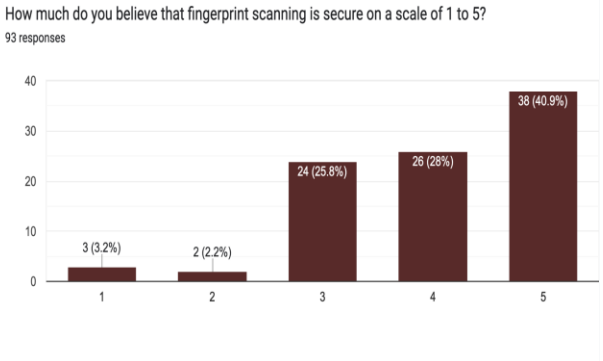
The graph above shows that 83.9% of participants having a mobile device with a fingerprint scanner built-in, and 16.1% do not have the feature.

4. If your mobile phone is equipped with a fingerprint scanner, will you use it, or will use a password to unlock it?



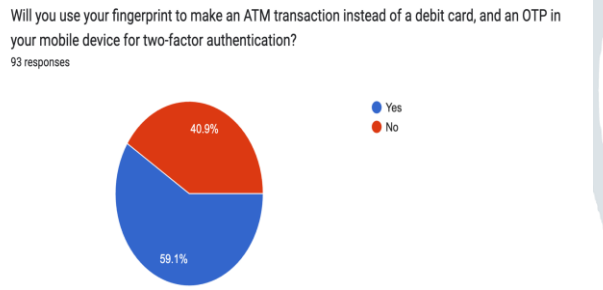
The graph above shows that 82.8% of participants were willing to use fingerprints for securing devices over passwords, and 17.2% will use passwords for the purpose.

5. How much do you believe that scanning is secure on a scale of 1 to 5?



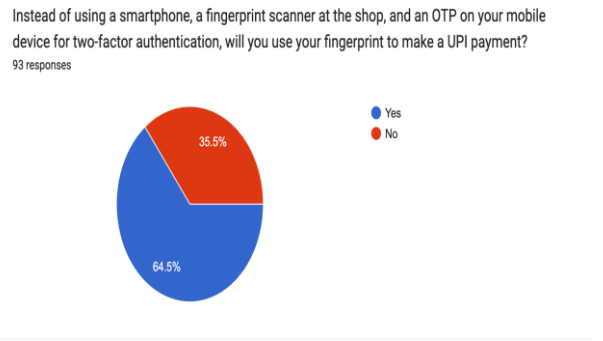
The graph above shows that 40.9% of participants believed in fingerprints as high security, and 3.2% were not believing in fingerprints.

6. Will you use your fingerprint to make an ATM transaction instead of a debit card, and an OTP in your mobile device for two-factor authentication?



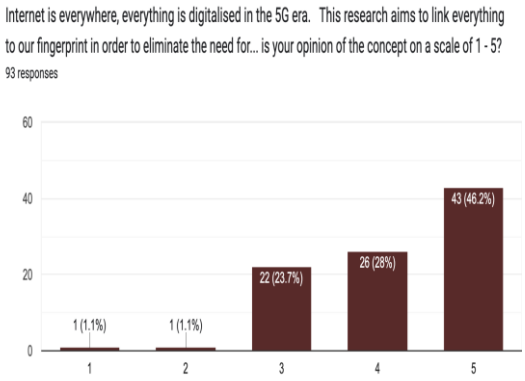
The graph above shows that 59.1% of participants were willing to make ATM transactions with fingerprints and OTP, and 40.9% were not willing to do the same.

7. Instead of using a smartphone, a fingerprint scanner at the shop, and an OTP on your mobile device for two-factor authentication, will you use your fingerprint to make a UPI payment?



The graph above shows that 54.5% of participants were willing to make UPI transactions with fingerprints and OTP instead of a smartphone, and 35.5% were not willing to do the same.

8. Internet is everywhere, everything is digitalized in the 5G era. This research aims to link everything to our fingerprint in order to eliminate the need for us to carry any physical form of identification to prove ourselves at any time, such as driving licenses, voter IDs, ATM cards, passports, etc. When you lose your identity card or forget to bring it to a place where proof of identity is required, you know what it's like, In the event that you forgot to bring your passport to the airport, as you were waiting for your flight, you will miss the flight; however, your fingertips won't be far behind you. What is your opinion of the concept on a scale of 1 - 5?



The graph above shows that 46.2% of participants agreed with the concept of storing all data with fingerprints and should retrieve using fingerprints instead of physical cards to carry for all purposes, and 1.1% were thinking it is a bad idea.

XII. Findings

Through the survey conducted we came to know that almost all of the respondents were aware of and using fingerprints for authentication in any manner, either at work, college, or on mobile, There is an inconvenience people are facing with the existing ATM systems with the limitations of Bank cards, even though having sufficient balance in the accounts people are unable to withdraw money without a Bank card. Not everyone carries Bank cards all the time, if there is any emergency, we are not able to access our own money without it. Also highly contours about the fraudulent activities related to ATMs, people are feeling very uncomfortable with online payments and transactions with Bank cards due to the security threats. Card details can be easily accessed and the password too, but if there are fingerprints and OTP to replace the cards then that is not the case.

XIII. Conclusion

With this research, I came to the conclusion that biometrics systems have a lot of popularity nowadays on top of traditional authentication methods. Regardless of age group and gender, all are somehow using some kind of biometrics system on a day-to-day basis. Among those fingerprint scanning is most popular due to its high-security rates and the convenience of its easy-to-use nature, people are well aware of atm fraudulent activities and are willing to adapt to cardless ATM transactions using fingerprint scanners and OTP to add an extra layer of the mode of security.
Considering all my findings I am concluding that biometrics will be the future in terms of authentication.

XIV. Reference

1. https://www.techtarget.com/searchsecurity/definition/biometrics
2. https://www.atmmarketplace.com/articles/what-are-the-biggest-atm-security-issues/
3. https://www.securityweek.com/latest-threats-atm-security
4. https://www.hypr.com/security-encyclopedia/fingerprint-authentication#:~:text=Fingerprint%20authentication%20or%20scanning%20is,%2C%20third%2Dparty%20biometric%20algorithms
5. https://www.sciencedirect.com/topics/computer-science/biometric-authentication