IOSR Journal of Business and Management (IOSR-JBM)
e-ISSN: 2278-487X, p-ISSN: 2319-7668. Volume 19, Issue 7. Ver. III (July 2017), PP 49-56
www.iosrjournals.org

A Study on the Opinion of Engineering Students on Significance of Biometric System for Authenticationofinternet Bankingsystem in India- A Review

*Prof. Ramola Premalatha
Associate Professor (Dept. Of Commerce)
Corresponding Author: Prof. Ramola Premalatha

***Abstract**: As a result of the need for cashless economy, the banking sector has come up as electronic banking popularly known as the e-banking system. It encourages the utilization of electronic (computer platform) to perform payment through bank transfers in terms of biometrics although their growth has not been as fast as some have predicted. This kind of system has been said to be very useful in stirring any economy from cash-based economy to a cashless economy with numerous advantage.There is a stigma attached to biometrics in which people have concerns over their usage. It may be that they fear what banks may do with their personal biometric data or it may be that they do not like the disturbing nature of the devices. A user-trial was suggested to investigate the awareness of biometrics, in order to conclude what the general public think about biometrics and their use. There were seven biometric devices chosen for the study and they are Fingerprint recognition, Iris recognition, Facial recognition, Signature recognition, Voice/Speech recognition, hand print and palm geometry with regards to its availability and cost. Hence, this paper has presented the usage of multiple human physiological cum physical features in securing this platform from the opinion of the technology students as they are the future of the country. Fifty student participants had taken part in the survey to answer questions to gain an opinion about the technology. It was found that fingerprint recognition was the most favoured of the technology, whereas Voice/Speech and Signature were the least liked.*

***Keywords**: Multiple Modal, Biometrics, Biometrics, Iris, Fingerprint, voice/speech*

Date of Submission: 27-06-2017 Date of acceptance: 15-07-2017

I. Introduction

Banking system is the backbone of the economy and information technology,in turn has become the backbone of the banking activities. The banks cannot think of introducing financial product without information technology support. Introduction to newer technologies allowed banks to offer new channels of banking through technology. Internet banking is the facilitation of banking transactions through internet. It is gaining popularity in India and Indian customers have started adopting this technology. The increase in accessing information along with the increasing use of information susceptible applications such as e-commerce, e-learning, e-banking and e-healthcare generate a valid requirement of reliable, easy to use and generally acceptable control methods for secret and essential information. Simultaneously, there must be a balance between privacy and security to safeguard the interest of the user. Hence, the banks should use effective methods to protect the identity of the customers who use their products and services. Traditional systems like use of personal identification methods (e.g., passwords, PIN) suffer from a number of drawbacks and are not able to satisfy the security obligation of the highly inter-connected information society.

Advantages and risks associated in internet banking

Internet banking is one of the services that the banks can offer to their customers. Many customers are relying on Internet-only banking as their only way of transacting their banking business. Before agreeing to online account access or before starting an account with an Internet-based bank, the customers should become familiar with the risks and advantages of online banking.

With internet banking the customers can access their account 24 hours a day, seven days a week and 365 days a year and can pay bills online by using online checking account. They can transfer funds, change their personal account preferences and can view up-to-date account statements whenever they want. They can access online services with internet banking account that they may not be able to access any other way, according to Financial Web. They can apply for loans online with the bank, request an increase in their credit limit and review the information for all of the different investment products the bank offers without leaving home.

Internet banking is thus changing the way people shop and how retailers operate. There is a steep decline in traditional payment methods such as cash and cheque and people are choosing the emerging digital

payment technologies as they render convenient and flexible methods for conducting cashless financial transactions. Retailers are also keen on investing in e-commerce platforms as compared to traditional in-store IT system upgrades because they anticipate rise in sales from mobile and online shoppers. Therefore online banking is reshaping the financial services ecosystem and more consumers are using their mobile devices for payment-related transactions as well as for accessing sensitive personal information.

However, this technology and digital convergence has also attracted the threat of cyber-attacks and made banks and financial institutions more vulnerable to fraud. It has led to a new breed of fraud perpetrators that use sophisticated technologies to hack into personal devices and corporate networks. Traditional techniques such as password or tokens are no match to their attacks. Research studies estimate the total fraud revenue loss in e-commerce sales in North America to be more than $3.4 billion.Biometrics refers to automatic identification of an individual based on his or her physiological or behavioural traits.

Fingerprints are the maximum used biometric traits, but with improvements in technology, numerous sources of biometric data have emerged. These contain data associated to facial features, iris, voice, hand geometry and DNA. Each trait is collected using different technologies and can be used for different purposes separately or incombination, to support and improve the accuracy and reliability of the identification process. The proposed purpose of biometric technology is to confirm the identity of individuals through a "one to one" check. This system equates a source of biometric data along with existing data for that specific person. This system is used at airport passport controls, and in targeted public service delivery systems (health care, pension schemes, etc.).

Whilst biometrics is not an identification solution, it is a start to offer very powerful tools for the difficulties which require a positive identification. Biometrics system Authentication is a process that validates the identity of a user who wishes to sign into a system by measuring some indispensablefeature of that user. The traditional methods involving passwords and PIN numbers don't require the person to be present there at the time of authentication, while biometrics techniques do not require password, PINnumbers. It stopsmal usage of ATMs, mobiles, PCs, smart cards etc. The characteristics are quantifiable and unique. Identity verification occurs when the user claims to be already enrolled in the system (presents an ID card or login name); in this case the confirmation biometric data got from the user is equated to the user's data already kept in the database.

Recognition occurs when the identity of the user isprior unknown. In this case the user's biometric data is coordinated against all the records in the database as the user can be anywhere in the database or the person actually does not have to be there at all. In biometric authentication, a genuine user doesn't have to remember or carry anything and it is known to be more consistent than traditional authentication schemes. Biometric authentication offers a convenient, accurate, unique and supreme security alternative for an individual, which makes it as an advantage over traditional cryptography-based authentication schemes.

Types of preferred biometrics

1. Eye feature recognition: - eye recognition is further categorized into two.

A- Retinal recognition- The first is based on the retinal recognition. The particular user has to look into a device that performs a laser-scanning of the retina. The device analyzes the blood vessels configuration of the acquired retinal picture. This blood vessels configuration is unique for each eye. This device is not friendly, because you have to stay fixed to a point while the inbuilt laser analyses your eye.

B- Iris recognition: - The scan is done by a camera. Unlike the retinal method, you don't have to be close to the device for authentication. The acquired picture is analyzed by the device, and contains 266 different spots. Moreover iris is stable through the whole life. Those 266 spots are actually based on the characteristics of iris, such as furrows and rings.

2. Fingerprint recognition: - This is the oldest biometric authentication approach. It analysesyour fingerprint characteristics. The first is by scanning the finger optically. The other method is by using electrical charges that determines which part of your finger is directly in contact with the sensor. Each fingerprint has its own unique characteristics, such as curves, bifurcations etc. One set of these characteristics is distinctive for each person.

3. Facial recognition: - A simple camera or a web cam with proper resolution used in facial recognition, after capturing the image the device computes a digital representation based on the facial structure's. The representation is compared with one which is stored in a database, and if there is a match, then the user will be authenticated. It is easy to implement and is said to be a convenient authentication method with exclusive recognition.

4. Voice command recognition: - A simple camera or a web cam with a proper resolution isused in facial recognition, after capturing the image the device automatically computes a digital illustration based on the facial structures. The representation is compared with one which is stored in a database, and if there is a match, then the user will be authenticated. It is easy to implement and is said to be a convenient authentication method with exclusive recognition.

Speaker verification focuses on the vocal characteristics that produce speech and not on the sound or the pronunciation of the speech itself. The vocal characteristic'snormallydepends upon the dimensions of the vocal tract, mouth, nasal cavities and other speech processing mechanisms of the human body. The system naturally asks the user to pronounce a phrase during the enrolment;the voice is then processed and will be stored in a template (voiceprint). Later the system asks for the similar phrase and compares the voiceprints. Currently there are three major international projects in the field of voice technology: PICASSO, CASCADE and Cost 250.

5. Signature analysis: - The signature analysis is a biometric authentication solution. The device is a compact tactile screen. The parameters that are computed for the authentication are the shape of the signatures, the time consumed, and the stroke order and last the pen pressure. With the computation of these parameters, the system delivers a unique authentication method. It is virtually impossible to replicate in the same way of somebody else's signature. It is easy to implement and quite cheap.

6. Handprint recognition: - This method is actually based on the recognition of the handprints. The device is a scanner that extracts a pure picture of a particular user's hand. Some characteristics like length of the fingers distance between them or their relative position everything is being computed. These characteristics are compared with the saved database and the result will be delivered. This method is not much complicated as the IRIS or signature analysis type methods. An optical hand geometry scanner capturesthe image of the hand and using theadvanced image edge detection algorithm computes the hand's characteristics.

7. Palm geometry recognition: - Palm print is the inner part of hand. A palm print acquiresthe features such as principal lines, orientation, finer points, singular points etc. Also palm print structure is unique. Palm print recognition is being used in civil applications, law enforcement and many such applications where access control is very essential. Palm has geometrical like features, delta point's, principal lines features, minutiae, ridges and creases. Principal lines are heart line, head line and life line.

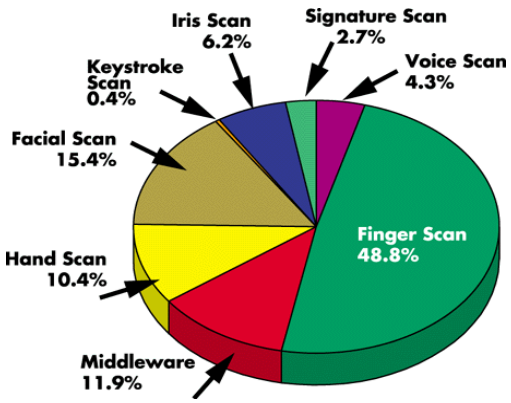


Fig 1. Graph for Biometric Technologies occupied in market *(Source: Thermal imager FLIR infrared camera resources)*

It can be seen from the figures below that fingerprint is the most common Biometric, occupying 48.8% of the market.

Applicability of Biometrics in internet banking for Authentication

Utilizing biometrics for internet banking is becoming convenient and considerably more accurate than current methods (such as the utilization of passwords or PINs). This is because biometrics links the event to a particular individual (a password or token may be used by someone other than the authorized user), is convenient (nothing to carry or remember), accurate (it provides for positive authentication), can provide an audit trail and is becoming socially acceptable and inexpensive.

Advantages of Using Biometric system

Biometric technology is now becoming very important that no banks can ignore. It provides security benefits across the spectrum, from IT vendors to customers, and from system developers to users. All these industry sectors must evaluate the costs and benefits of implementing such security measures. Different technologies may be appropriate for different applications, depending on perceived user profiles, the need to interface with other systems or databases, environmental conditions, and a host of other application-specific parameters.

Its benefits can be summarized in the following points:

• Greater security—biometrics can help to link a person to an action.

• Convenience—No need to remember identification number or password

• Local verification—customers' account is linked with Aadhar card (e.g., on a Smart Card), so there is no need to verify again.
• Verification is instant and does not require any banking staff.
• Customer identity is safe and trouble-free.

The goal of any access control system is to let authorized people into specific places. Only with the use of a biometric device can this goal be achieved. A card-based access system can control the access of authorized pieces of plastic, but not who is in possession of the card. Systems using PINs (personal identification numbers) require that an individual only know a specific number to gain entry. Who actually enters the code cannot be determined. Biometric devices verify who a person is by what they are, whether it is their hand, eye, fingerprint or voice. Biometrics also can eliminate the need for cards. While dramatic price reductions have lowered the initial cost of the cards in recent years, the true benefit of eliminating them is realized through a reduced administrative effort. A lost card must be replaced and reissued by someone. There is a cost associated with the time spent to complete the task. Eyes and hands are seldom lost, stolen or forgotten. They also don't wear out and need to be replaced.

Using biometrics for identifying human beings in internet banking offers some unique advantages given as follows:

• Biometrics can be used to identify you as you.
• Tokens, such as smart cards, magnetic stripe cards, photo ID cards, physical keys and so forth, can be lost, stolen, duplicated, or left at home.
• Passwords can be forgotten, shared, or observed. Moreover, today's fast-paced electronic world means people are asked to remember a multitude of passwords and personal identification numbers (PINs) for computer accounts, bank ATMs, e-mail accounts, wireless phones, web sites and so forth.
• Biometrics holds the promise of fast, easy-to-use, accurate, reliable, and less expensive authentication for a variety of applications.
• Another key aspect is how "user-friendly" a system is. The process should be quick and easy, such as having a picture taken by a video camera, speaking into a microphone, or touching a fingerprint scanner.
• As biometric technologies mature and come into wide-scale commercial use, dealing with multiple levels of authentication or multiple instances of authentication will become less of a burden for users.

Factors attributing to the rise of biometrics in the online banking sector

More than half of the global population has access to mobile devices. Brick and mortar banking has been revolutionized by online services and customers now have several options to access their bank accounts – either through a web browser or through mobile apps. However, this trend has also increased the vulnerability of customer accounts. Criminals are targeting the online and mobile banking platforms to commit transaction frauds and identity theft. Moreover, security measures that rely heavily on passwords and PINs not only make online banking inconvenient but are also not foolproof and easy to hack.

Banks and financial institutions are continuously looking to improve their security beyond the traditional username and password protocols. The traditional security methods have failed to decrease the vulnerability of customer accounts. Furthermore, it has created trust issues and distress for customers who have been victims of security breaches and identity theft. The success of online banking now lies on robust measures that can detect fraud and prevent cyber-criminals from hacking into customer's accounts.

Cyber criminals are a threat to e-commerce and the online banking sector hampering growth opportunities in this industry. Fraud and payment card theft continue to be the top data breaches committed by hackers. The root cause behind this issue is that the actual identity of customers making the purchase is unknown as that individual is making the payment on a remote computer. As passwords and PINs can be stolen and used without the permission of the owner, it is not an effective way to stop data breaches thus resulting in loss of customers and increased expenses for the banking and financial services industry.

The need for a high-tech and reliable authentication technique that can combat savvy hackers has given rise to biometric security in the online banking arena. Unlike passwords or tokens, biometric technology authenticates transactions based on something inherent to the user. It is an approach to positively identify users based on their unique physiological or behavioural characteristics like fingerprints, retina, gait, face, voice etc. These biometric identifiers are virtually impossible to replicate nor can be shared.

Hence biometric solutions are gaining momentum in the financial services sector due to their exclusive features and the ability to provide greater security in comparison to other traditional user authentication methods. The deployment of fast and efficient online services that will allow users to make mobile payments across all channels is an important pre-requisite to enhancing the customer experience. And biometrics can enable financial institutions to achieve this goal by providing a secure, hassle-free and easy to use payment approach for the next-generation online shoppers.

How is biometrics adding value to online banking?

Banking has become more digitized nowadays and biometrics can help banks to provide customers with enhanced security and cutting-edge technology while performing online transactions. As biometrics is based on identifying an individual as opposed to simply identifying a device or a piece of information, the biometric identifier can never be forgotten or shared. Moreover, it is very difficult to steal biometric data as long as the biometric vendor uses appropriate architecture and security methods.

Most smart phones now come with built-in biometrics support that helps to verify the buyer's identity and prevent payment fraud. This simplifies the process of making payments with fingerprint or facial recognition technology. Major financial organizations are starting to leverage biometric technologies and have introduced biometrics-enabled smart cards. These cards are compliant with various standards such as MasterCard, Visa etc. and are being increasingly used to make online payments. These smart cards are embedded with sensors that get activated at the time of purchase by using the owner's fingerprints. Leading smartphone manufactures have also equipped their phone with fingerprint sensors that can be used not only for unlocking the phone but for authenticating online purchases.

Thus biometrics is revolutionizing the online payment system by using the customer's inherent traits to verify his or her identity. It is like an individual's personal password that cannot be lost, forgotten or stolen. The speed and agility of transactions are significantly enhanced as users do not need to remember answers to security questions nor do they need to carry a separate hardware-token. Thus it provides ease of use and helps to enhance customer trust in the bank.

Examples of how biometrics can be used to make a positive impact in banking

Fingerprints and biometrics

In addition to fingerprints and facial recognition, keystroke biometrics i.e. a person's typing pattern can be deployed to automate the process of verifying online banking customers. For example, the keystroke rhythms of an individual lead to a unique biometric template. This keystroke timing data can be recorded, stored and matched for future comparisons. As keystroke biometric authentication is not capital intensive it can be readily deployed and used for authenticating internet banking customers. This is an example of second generation biometric authentication.

Voice biometrics

There may be a percentage of the population who are not educated enough to sign and transact on their own or those who do not meet the identification requirements of financial institutions. In such cases, voice biometrics can play an important role by simplifying the authentication process. A voice or speech recognition system can be used to perform bank transactions and customer service where customers verify their identity using the microphone in their phones.

Indian banking sector and biometrics

Biometrics is not a new phenomenon in the country, but Indian banks are going to great lengths to use biometrics to its full potential. Fingerprints, voice pattern, iris scans and facial geometry are widely used for biometric recognition. According to a TechSci report, the biometrics market in India will grow at a CAGR of 31 percent from 2016 to 2021 and will surpass $3 billion by 2021.

Biometrics is not only highly secure but also cost effective for banks. It lifts the burden of remembering passwords, PINs and card numbers. Biometric, either it fingerprint, iris, face or voice recognition, all getting explored by Indian Banking Sector for providing safe and secure banking for its customers. With this new age where we are talking technology for the ease of process, Indian Banks are not leaving any single stone unturned for making their customer experience fabulous with new age banking with these technologies.According to a TechSci report, the biometric for Indian Banking Sector market will grow at a CAGR of 31 percent from 2016 to 2021 and will surpass $3 billion by 2021.Biometrics is not only highly secure but also cost effective for banks. It lifts the burden of remembering passwords, PINs and card numbers. It also helps curbing the fraud and makes it safer. Banks attracting customer with their new slogan of safe banking based on Biometric Technology. IDG takes a look at how biometrics is driving banking system in India:

DCB Bank: DCB Bank has set up ATMs that require your fingerprints to withdraw money. The ATM operates using Aadhaar card data and links a customer's fingerprint data with his Aadhaar biometric details. These biometric ATMs are available in Bengaluru, Mumbai and Chennai. However, this service can only be availed by DCB Bank customers.

Federal Bank: Federal Bank has introduced a zero balance selfie account. A person can now download the Feed book app from the Play Store or App Store, scan their PAN card and Aadhaar card and click a selfie to open an account instantly. Once the account is opened, the app will turn into a passbook.

HDFC Bank: HDFC Bank is reaching out to rural areas which don't have ATMs through a hand-held device or a micro ATM with biometric verification. It uses Aadhaar card and fingerprints for biometric verification for instant KYC (know your customer) check. HDFC has tied up with Gramin Banking Officers (GBO) to provide this facility in Punjab.

ICICI Bank: ICICI Bank introduced voice recognition for its customers to transact smoothly through the bank's call centre. Customers are no longer required to enter their PIN and card number as their voice will act as the password now. The voice recognition technology authenticates based on speed, accent and pronunciation, which are unique to every individual.

State Bank of India: SBI uses a biometrics authentication application that incorporates fingerprints and biometric matching software to verify bank employee credentials before they access its core banking system. The bank will install this system across 21,000 locations.

Biometric ATMs to expand in India- Banknet India

Banks in India have started introducing biometric automatic teller machines (ATMs) as it seems to be an effective way of preventing PIN theft and is also a channel to expand a bank's reach to the rural & illiterate masses, according to Banknet India's Report on Indian ATMs. Union Bank of India installed a first such 'Kisan ATM' at Sivagangai branch Tamil Nadu. Dena Bank has launched the Bio-metric ATMs in Gujarat. Andhra Bank has launched two mobile biometric-access ATMs, one each for the Twin Cities of Hyderabad and Secunderabad. Corporation bank has also introduced 'talking' biometric ATMs. These ATMs 'talk' to the farmers in their local language. The biometric ATM replaces personal identity number (PIN) with thumb impression. The fingerprint scanner fitted in the machine only recognizes the customer's thumb impression. These Kisan ATMs are designed for the rural farmer and incorporate video & voice animation system coupled with single-touch application that makes things not only easier but also safer for farmers who no longer have to depend on others to withdraw money from the bank. Such ATMs from some providers also accept traditional PIN based cards.

Two of India's largest banks, ICICI Bank and State Bank of India, are partners in the Centre's national rural employment guarantee scheme (NREGS) in certain parts of rural Tamil Nadu. As many as 10 'Gramm tellers', or low-cost ATMs, will be rolled out in the test phase in the state.

In coming days, Banks will incorporate more Biometric Technology to make life easier for their customer. With mobile banking becoming popular, it will also boost the confidence of their customer for safe and secure banking. Online and telephone banking will have more customers now based on the introduction of different biometric recognition for these platforms. Biometric for Indian Banking Sector has become a boon for customers.

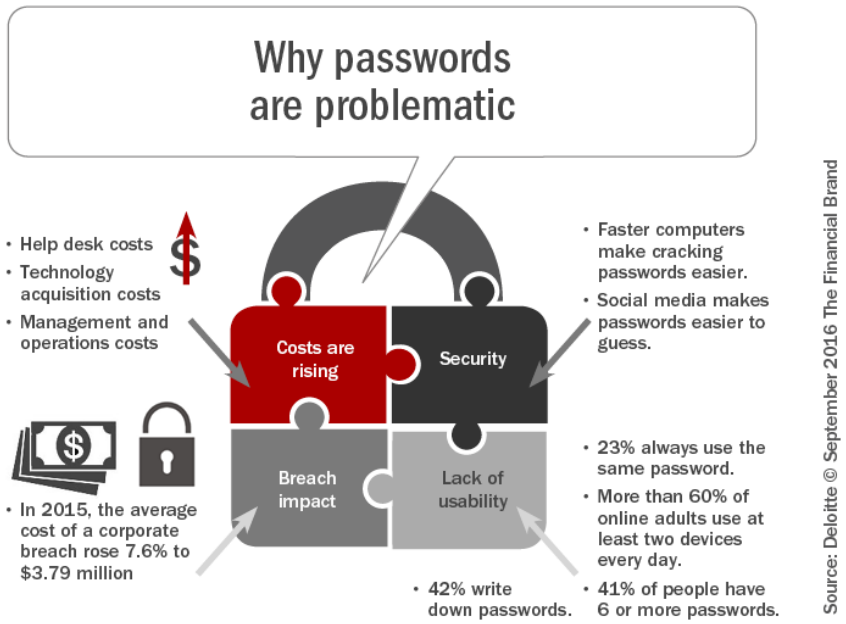
Comparison of various biometric technologies

It is necessary to compare the various biometric technologies in terms of their characteristics for the adoption in authentication process of internet banking. In this context we are highlighting the comparison of various types of Biometric Authentication techniques already given by some authors and research studies. This is presented below. Comparison of various biometric technologies based on the perception of the authors. High, Medium, and Low are denoted by H, M, and L, respectively.

Types of biometrics and its preferences.

Biometric identifier	Universality	Distinctiveness	Permanence	Collectability	Performance	Acceptability	Circumvention
Face	H	L	M	H	L	H	H
Fingerprint	M	H	H	M	H	M	M
Hand geometry	M	M	M	H	M	M	M
Iris	H	H	H	M	H	L	L
Keystroke	L	L	L	M	L	M	M
Signature	L	L	L	H	L	H	H
Voice	M	L	L	M	L	H	H

Source: http://www.basicofy.com/biometric-authentication/



The Move to Biometrics

Deloitte expressed that while fingerprints consumed a long time to gain traction, the technology had taken off during the past three years. The company interviewed 4,000 people and said that 31% of 18-24 year olds were using the fingerprint scanners on their phones, compared with 8% of those aged over 65. In future there will be one billion smartphones with fingerprint scanners in use by the end of 2017 and that the technology will spread to cheaper models. Big banks increasingly are offering customers the option of using fingerprints, voices, retina scans and other biometric technologies to access their accounts instead of passwords. Expediency for consumers and enhanced security in a time of extensive data breaches are fuelling the switch. Majority of the providers in the US and Australia have also integrated fingerprint authentication into their mobile banking apps, according to Maxpa Research. In Europe, several providers have gone further and rolled various forms of biometric authentication. It can be seen that the majority of people (70%) believe Iris recognition to be the most secure of the biometric technologies on test done by Network Research group. Fingerprint recognition also gained a good rating from participants this technology has been proven to be in theory very secure. It can be seen that signature and voice recognition scored the lowest. But the two most rarely used biometric technologies were Iris recognition and Facial recognition. This is due to the fact that both these technologies have a reputation for being expensive and are more specialised ssto an application. Thus they are not used so much in applications that the public would have access to. Most of the reason behind Iris recognition being expensive when compared to other biometric methods was due to a twenty-year patent covering the technology, thus not allowing other researchers to develop it and create better-priced versions (ZD Net, 2006).

View on Awareness

This paper has presented a wide-angled view of the way in which the students view biometrics. In that it hasshown how aware they are ofbiometrics andalso their reactions to differenttypes of biometric devices. Bylooking over at the usability and security factors, fingerprint recognition aims to achieve the best-rounded score. There are of course many reasons as to why the public may believe fingerprint recognition to be the best in these factors. Hence, the fingerprint recognition was one of the first biometrics to be developed, so it may simply be that the public are just more accustomed to the idea of having their fingerprint read. Another factor is that fingerprint recognition is one of the least intrusive biometric technologies. But again Iris recognition also scored very well in each of the three sections, which could be considered an intrusive technology as it requires a picture of the participant's eye and also involves a lot of aligning.

Future Work

In our study although we have seen that authentication is the only control mechanism insecurity concerned,but it is to be inadequate in the case of high risk transactions involvingaccess to customer information or the movement of the funds to other parties. In future a research can be conducted on various security aspects in terms of internet banking and will try toimplement an integrated authentication model by using new technological approach to dealwith security challenges of internet banking system.

II. Conclusion

Banks are embracing biometric technology to realize greater business benefits by improving their sales and services function. The practical and reliable authentication that biometric technology provides us, has helped to delight all the customers as well as offering a superior banking experience through personalized and need based engagement.

Reference

[1] Mr. Mule Sandip S and Mr.H.B.Mali (2015).Review on Biometric Authentication Methods.International Journal of Advanced Research in Computer and Communication Engineering.Vol. 4, No. 11, ISSN (Online) 2278-1021 ISSN (Print) 2319 -5940. pp. 252-255.

[2] GunajitSarma and Pranav Kumar Singh (2010). Internet Banking: Risk Analysis and Applicability of Biometric Technology for Authentication. International Journal of Pure and Applied Sciences andTechnology. Vol. 1, No. 2, ISSN 2229-6107,pp.67-78.

[3] Amtul Fatima (2011). E-Banking Security Issues – Is There A Solution in Biometrics? Journal of InternetBanking and Commerce. Vol. 16, No.2,pp.1-9.

IOSR Journal of Business and Management (IOSR-JBM) is UGC approved Journal with Sl. No. 4481, Journal no. 46879.

Prof. Ramola Premalatha. "A Study on the Opinion of Engineering Students on Significance of Biometric System for Authenticationofinternet Bankingsystem in India- A Review." IOSR Journal of Business and Management (IOSR-JBM) 19.7 (2017): 49-56.