Evaluating Current Authentication Methods: Prediction of a More Suitable Authentication Approach for Public Interaction

[a] Jimoh R. G., [b] Norshuhada Shiratuddin

Graduate Department of Information Technology,
Applied Science Office,
College of Arts and Sciences
Universiti Utara Malaysia
06010, Sintok, Kedah, Malaysia
[a] Tel : +60172425289 e-mail : jimoh_rasheed@yahoo.com
[b] *Tel: +04 929284700/4701/4846 e-mail : shuhada@uum.edu.my*

Abstract

The trend in information technology is towards achieving ubiquitous service rendering where barriers (geographical, time) in getting information related services will be eliminated. A good example of this is the ATM machines used by banks for public banking services, the likes in other sectors are currently on the way. This paper explores the user's perception on the current identity authentication (Token-based and Knowledge-based) with a view to predict a more secured authentication for authentication in public places. A survey study is conducted so as to justify the claims of the previous authors on the need to migrate from the conventional knowledge-based and token-based authentication methods to a more secured biometric authentication approach which makes impossible user's impersonation, and thus minimizing fraud, particularly in business transactions. Also, biometrical identification was also reviewed with respect to the all known biometric identifiers where human iris data was revealed to be the best human trait that can be used for identification/authentication purposes in public zones.

Keywords: *ubiquitous, biometric, authentication, iris and public zone.*

1.0 INTRODUCTION

The world has turned to a global village via information technology. The fast growing and dynamic world of information technology has called for fast responding and reliable security devices. The singular fact that almost all business data are now being converted into an electronic form requires us to protect such information from some unethical persons who are always exploring possibilities of gaining illegal access to the information. It has become practically impossible for any organization to succeed without information technology. This has brought the need to migrate from the traditional ways of doing things to an information technology compliant way so as to improve efficiency. The need for information technology in almost all organizations cannot be over emphasized. Some estimates indicated that since 1980s, about 50 percent of all new capital investment in organization has been in information technology (Alexander & Peter, 2008).

Searchsecurity.com (2007) reported that Privacy Rights Clearing House revealed that since 2005, over 93 million data records of U.S residents have been exposed as a result of data security breaches. Such profile cases within corporate America and the U.S government have exposed a glaring vulnerability within organizations; such difficulty in keeping sensitive data secured called for stronger user authentication. Similarly, Anil, Hartthick and Abhishek (2008) observed that there is an urgent need to come out with a reliable identity management system so as to reduce the epidemic growth in identity theft for meeting the emerging security demands in a variety of applications. This among others security problem associated with using information technology approach for public service delivery has proved the need for a more secured approach of interaction with public terminals. Several researchers have proposed biometric identification as the alternative to the inherent problems of both token-based and knowledge-based authentication. It was found out that security threat is a known fact in the prevailing information technology world, still the main problem is how to get the problem solved as described in a quotation by Nataliya (2004) as follow:

"We find that people are generally aware of the danger out there, but not aware of what they should do to keep their systems secure".

This calls for the need to embrace a more secured means of authenticating identity while interacting with public zone's service rendering system (Nataliya, 2004; Alexander et al., 2008). This article first discusses the authentication approaches viz-a-viz token-based, knowledge-based and biometric-based for the purpose of comparing the three approaches. Iris-based biometric authentication was identified as the best biometric authentication methods based on the findings from the content analysis. The article finally discussed the findings from the survey study.

2.0 IDENTIFICATION /AUTHENTICATION AND ACCESS CONTROL

Personal Identification is defined by several authors as the means by which a particular individual is associated with or attached to an identity (Anil et al., 2000; Manu et al., 2007). Mostly identification and authentication are used

interchangeably, notwithstanding, for personal access to an automated system authentication is the most appropriate word. Authentication can also be defined as a process of establishing or confirming someone (or something) as being authentic, this means validating the claim made by someone or something (Manu et al., 2007).

Within the context of computer networks including internet, authentication is mostly achieved via the use of logon passwords, where the knowledge of the password is assumed to confirm the authenticity of the user. The major weakness of this approach most especially for security-critical system such as exchange of money is that the password can be stolen, accidentally revealed or forgotten. This among other factors called for the need to provide a more stringent and secured authentication approach for the emerging sensitive transactions (Information Security Magazine, 2007).

Access control constitutes proper identification, authentication, authorization and accountability in enforcing security. In controlling access to a system, users are first identified, then the identity is verified through authentication, having confirmed the user to be authentic, authorization specify the authority/ access level of the user and lastly, the record of users' activities are accounted for. Access control is mainly to protect the confidentiality, integrity and availability of data. Access control can be achieved by knowledge-based authentication, token-based authentication and biometric authentication. A multi-factors access control can be implemented by combining multiple of the method (Nataliya, 2004).

Sometimes, identification can be referred to as verification or authentication that involves authenticating a claimed identity. It can as well be viewed as recognition (identification) which has to do with the determination of the identity of a given person from a database of persons contained in the system. Traditionally there are two main identification methods namely: the knowledge-based and the token-base/ possession-based approach (Anil, Lin, & Sharath, 2000).

The knowledge-based method: - this has to do with something you have knowledge of to be used for personal identification purpose. Examples of this category are: passwords or Personal Identification Number (PIN).

Token-based/ possession-based method: - this approach is concerned with the use of something that you can show to identify you such as driver's license, ID card, credit card, identification tag and passport among others.

According to Information Security magazine (2007), Forester researcher has identified biometric authentication as one of the top ten identity management trends in 2006 and predict that it will go mainstream- extending beyond the market of early adopters. Authentication of the identity of individual has been a great concern to all sectors in order to be sure that people with forged identities do not get undue services or benefits. As a result of this, more organizations tend to adopt an automated identity authentication system to improve efficiency, customer satisfaction and more importantly to save critical resources by determining "who gets what" at any point in time. Previous researches have proved that biometric identification is the only secured means of authenticating individual identity since knowledge-based or token-based are unable to differentiate between an authorized person and an impostor since the basis of confirmation is acquiring the token and the knowledge (Anil et al., 2000).

Asides security issues, previous research has shown that not all users tend to remember their Personal Identification Number (PIN) at the point of using it. A survey conducted revealed that more that 55.7% of participants had already forgotten a PIN with the consequence that they were denied access to a specific service by the service provider (Alexander et al., 2008). As a result of this, several researchers have come out with their submission that only a biometric-based authentication approach is the novel authentication method to guarantee both security and usability (Manu et al., 2007; Alexander, Roman & Heirich, 2007; Desney et al., 2005; Alexander et al., 2008).

2.1 Authentication with Public Terminals

With the world becoming a global village via interconnectivity, various services are made readily available at public places using public terminals. Such services include: cash withdrawal, recharging mobile phone prepaid cards, buying bus or train ticket and so on. Services of this nature are no longer location-based but rather made available to people at public places for more convenience. No doubt this innovation has bridged the usual geographical barrier of service delivery, that notwithstanding, a lot of challenges accompanied such opportunities since interaction with the machines will take place in public places. Authentication of identity becomes highly necessary so that users can validate their claimed identity before having access to the services offered by the machine. The need for such authentication cannot be over emphasized since they are dealing with highly sensitive user data which are prone to security threats.

A good example of such security problem is the manipulation of ATMs to get in possession of users' PIN and therefore getting access to their bank accounts. The most common attack now is called shoulder surfing, most often than not, the threats come from one of the companions of the authentic user who can easily have access to the card when required (Alexander et al. 2008). The issue of uniqueness of biometric identifier is more crucial when technology is to be applied for both identification and authentication in large-scale public applications (Akhilesh & Thomas, 2005).

Shoulder surfing has been a very serious attack on password authentication most especially at public places; it is very hard to defeat, this can be achieved even from a remote location by using binoculars and cameras, keyboard acoustics or electromagnetic emanations from displays physiological or behavioural characteristics that can be employed to solve this problem since such characteristic will be unique to one and only one individual and they are difficult to replicate (Akhilesh & Thomas, 2005). Information resources are protected by unambiguously identifies and authenticates users. Such unique

way of authentication is achieved via biometrics. Introduction of biometrics has resolved some issues arising from identification and authentication in information system, this has resultantly paved way for the suitability of biometric authentication techniques in a wide range of application domain such as computer access control, physical security and customs and immigration among others (Matysa & Stapleton, 2000).

2.2 Biometric Authentication

Biometric Authentication Process

The process of biometric authentication is generally divided into two main phases as follow (Anil et al. 2000; Anil et al. 2008):

The enrollment phase: At this stage, the biometric sample obtained through a sensor, from the person also referred to as the identifier will be stored in a special database called template database. The stored sample (the template) represents the best obtainable sample after undergoing a lot of screening and assessment by the quality assessment module and the feature extractor.

The Authentication (matching) phase: This is the real authentication stage during authentication. Failure to establish such match results into denial of access. The verification is done by a matcher controlled by decision module.

Generally, five major components are identified within the authentication process. These include the sensor, the feature extractor, the template database, the matcher and the decision module (Anil et al. 2008).

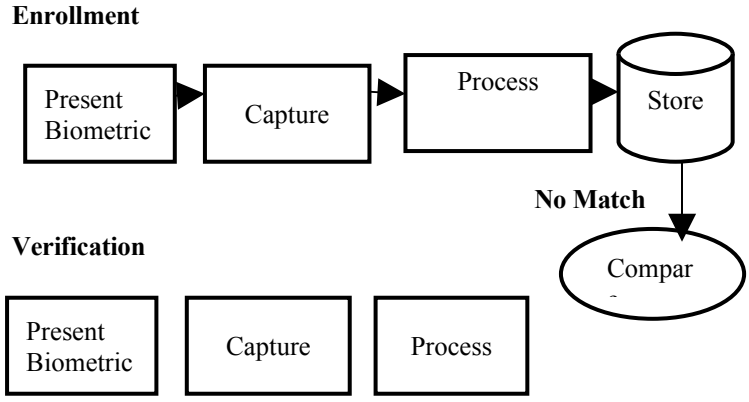
The Sensor: This is an interface positioned between the user and the authentication system to capture (scan) the biometric trait from the user.

The Feature Extractor: is a module responsible for processing the scanned biometric data so as to extract the salient information that is unique enough to differentiate users.

The Quality Assessment Module: This is used to determine how quality the scanned biometric image is so as to decide whether to forward it or not. Most often, this is normally integrated in the feature extractor.

The Template Database: is a special database where the extracted biometric feature to be used for identification is stored. This is properly indexed on user's basis.

The Matcher: conducts the actual authentication with the use of appropriate **Decision Module.** Figure 1 below describes the real biometric authentication process.



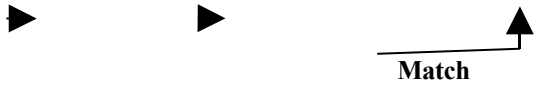


Figure 1: Biometric Authentication process

According to Jain et al. (1999), questions that have to do with identity of individuals are asked million of times every day by different organizations ranging from financial, health care, e-commerce, government and telecommunication. Identity of individuals has being a major concern to virtually all aspects of livelihood. This accounted for the rampant identity fraud in virtually all sectors amounting to over $6 billion each year. Having noticed the level of identity fraud, more organizations are now trying to pave way for automated identity authentication system to improve customer satisfaction and efficiency. The International Biometrics Industry Association (IBIA) defined Biometric Identification as those technologies used in establishing person's identity by measuring some unique physical characteristics of human being which guarantee accuracy, reliability, safety and privacy (www.ibia.org).

Biometric identification has gained more popularity in the area of user authentication most especially, for a security-critical system. This can be can be traced to its flexibility nature as a result of being able to use a number of human characteristics as identifiers.

"When it comes to working with biometric identification technologies, it is not only our fingerprints that do the thinking. Now, our eyes, hands, signature, speech, and even facial temperature can ID us" - (Anil et al. 2000).

According to Electronic Frontier Foundation, biometric identification refers to identity verification of living persons using their physical or behavioural characteristics. In similar view, Patrick, (2005) defined biometrics as the application of identification via iris scanners, facial analyzers, handprint authentication, as well as voice recognition. The use of biometric technology has now gained considerable acceptance in sensitive organizations like governments and financial institutions. It is most likely to witness an increase in the number of new proposals of biometric technology applications (Alexander & Peter, 2008). Similarly, biometric system simply means a computerized system that uses measurable physiological features or behavioural characteristics of an individual to either determine or authenticate the identity of such individual (Jennifa, 2005; Schonberg & Kirovski, 2008).

Due to the distinctive nature of physiological and behavioural characteristics of every human being, biometric identifiers are considered to be more reliable and capable compared to either knowledge-based or token/possession-based methods while differentiating between an authorized person and a fraudulent impostor (Jain et al., 1999).

Akhilesh and Thomas (2005) observed that, the resultant challenges and constraints that accompanied biometric identification/authentication technique in information system applications led to the development of a generalized conceptual

model that can be applied by future researches on empirical model work related to the diffusion of biometrics in information security. Thus researches on acceptance of biometric authentication technology are more encouraged.

Alexander and Peter (2008) also identified degradation or deformation of biometric identifier over time, variance in the stored template and the actual biometric identifier and threshold values for authentication as the technical concerns presently facing biometric technology which ought to be overcome as the technology gets more matured. Such is not applicable to iris-based authentication approach since the iris image remains the same throughout once life span once developed (Anil, 2000;Raviraj, 2007).

A biometric system can be classified depending on the characteristics or traits involved. These traits can also be seen from two different perspectives i.e physiological and behavioural as described in the Table 1 below.

Table 1: The architecture of a typical biometric system

Physiological characteristics	Behavioural characteristics
Face	Key stroke
Finger print	Signature
Hand	Voice
Iris	
DNA	

2.3 The Physiological Biometric Identifiers

These are derived from the physiological characteristics of human being and examples include the face, the fingerprint, the hand, the iris and DNA. Below are some reviews exposing the shortcomings of the identifiers.

The Face to start with is considered the most traditional trait of human being used for personal identification. Facial recognition has opened ways for many research opportunities (Chellapa, Wilson & Sirohey, 1995). Though, the facial recognition is unique to some extent (Anil et al., 2000), it has very few features for identification and also difficult to collect.

The Fingerprint is one of the oldest ways of authenticating person's identity, it has been used for century having establish its validity (Anil et al. 2000; Nataliya, 2004). A fingerprint can be defined as a natural pattern consisting ridges and furrows on the surface of a fingertip (Jain et al. 1999). Despite the popularity of the forensic fingerprinting, it is still found unreliable in some cases (Barry & Peter, 2002). Automated fingerprint identification requires large amount of computational resource which serves as a disadvantage from organizational perspective (Jain et al. 1997).

The Hand is a biometric technology that uses the shape of human hands for identification purposes. The user's hands are measured by hand geometry readers along a number of dimensions which are going to be compared with the stored templates before authentication can take place. The problem with this is that it cannot be used alone as (David, 2004).

The Iris image is used for personal identification purposes as early as the late 19th century (Kaushik & Prabir, 2008).The human iris has some distinguished features that make it suitable as a biometric identifier. The image can be captured from relatively fair distance (2 – 24 inches) and verification is faster compared to other (Michelle & Xin, 2007; Raviraj, 2007). The iris image has 266 unique spots unlike other biometric identifiers with just13 to 60 distinct characteristics (Kaushik & Pabir, 2008). The summary of the outstanding feature of iris is in section 2.5.

The DNA according Anil et al (2000), (deoxyribonucleic acid) can be defined as a double helix structure that is present in every human cell. The DNA sample is used to provide a DNA profile for a particular individual. Its identification techniques are not generally considered suitable for biometric recognition technology mainly because, its process is yet to be automated. The major drawback towards its successful implementation as a biometric identifier is that, it includes sensitive information about the genetic and medical aspects of individuals (Anil et al., 2000; Shannon & Hamed, nd).

2.4 The Behavioural Biometric Identifiers

The Key Stroke is a behavioural biometric technology that measures both the dwell time (how long a key is pressed) and flight time (how long does it take to move from one key to another) (Thomas, 2006). The keystroke dynamics as a behavioural biometric technology uses the manner and rhythm a character is typed on either a keyboard or keypad. The rhythms are measured and captured as the unique representation of the user's biometric template for future authentication purposes. The dwell time and flight time are recorded as the keystroke timing data. This data is then processed using unique neural algorithm to determine the pattern for future comparism (Checco, 2003). Bergadano, Gunetti, and Picardi (2002) revealed that keystroke biometric technology is yet to come with any technique with acceptable level of accuracy.

The Signature is generally believed to be unique for each individual. This notwithstanding, two signatures produced by only one person cannot be absolutely identical, such variation can be attributed to changes in emotional and environmental conditions (Anil et al. 2000).

The Voice recognition was defined by Nataliya (2004) as a process of validating a pass phrase via the telephone which requires user to produce sound both at low and high frequencies. Voice biometric identifiers are derived from the components of human voice. Voice biometric image, unlike other biometric identifiers, voice varies based on some varying conditions such as illness (running nose), emotions, aging (such as puberty, old age etc.) and one's environment. For this reason among others, voice biometrics is considered inappropriate for measuring biometric security (Michelle & Xin, 2007). Also, the features are not unique enough to be used for authentication in a security-critical environment (Anil et al., 2000; Anil et al., 2008).

2.5 Human Iris as the best biometric identifier

The algorithm used in Iris recognition is so accurate and universal that it can accommodate people in the whole world to be enrolled in an iris database without making false acceptance and false rejection error (Fakhry & Cardozo, 2006). The human iris is a colored oval-to round-shaped ring surrounding the pupil of the eye. The iris is the only internal organ that is visible externally. The stability nature of iris has distinguished it from all other forms of biometric identification. It acquires the stability from when a person is two year of age and retains such stability in one's life time except if damaged either by accident or disease (www.biometricgroup.com; Anil et al. 2000).

Human Iris, with its complex biometric structure is made up of many distinctive features such as arching, ligaments, furrows, ridges, crypts, rings, corona, freckles and zigzag collate (Daugman, 2006). One of the major glaring features of the iris is the trabecular meshwork tissue which makes it appear as if the iris has radial divisions. There is no genetic influence during the development of iris; this makes it to be free of genetic similarity of its features (Fakhry & Cardozo, 2006). According to RaviRajtech (2007), with iris-scan technology, false matching and fraud is practically impossible because patterns easy to capture.

The following is the summary of the iris outstanding features (Anil, et al. 2000; Nataliya, 2004; RaviRajtech 2007):

(a) Not prone to modification and alteration due to its complex nature.
(b) Iris is unique to one and only one individual, the chance of two irises producing the same numerical code is almost zero.
(c) The iris gets stable from age of two and does not degrade either with time or environment.
(d) Highly protected against accidental damage.
(e) It has a minimal false acceptance and false rejection rate of 1/1.2 million and 0 respectively.
(f) Iris patterns are easy to capture and encode.
(g) Eyeglasses and contact lenses do not present any problem to iris-scan system.
(h) Iris recognition does not use infrared light beams, this makes it safer for the eye damage as one of the factors hindering the successful implementation of any eye-based authentication.

Table 2; adapted from RaviRajtech (2007), shows how the iris-based biometric authentication outperformed all other biometric system, while Table 3 compares token-based, knowledge-based and biometric-based authentication approaches.

Table 2. Comparing biometric identifiers.

Method	Coded Pattern	Mis-identification Rate	Security	Application
Iris Recognition	Iris Pattern	1/1,200,000	High	High-security facilities
Fingerprint	Fingerprints	1/1,000	Medium	Universal
Hand Shape	Size, Length and Thickness	1/700	Low	Low-security facilities
Facial recognition	Outline, shape and distribution of eyes and nose	1/100	Low	Low-security facilities
Signature	Shapes of letters, writing order and pen pressure	1/100	Low	Low-security facilities
Voice printing	Voice Characteristics	1/30	Low	Telephone service

Table 3: Comparing token-based, knowledge-based and biometric-based authentication approaches

Token-Based	Knowledge-Based	Biometric-Based
Based on Possession of something	Based on knowledge of something	Based on human biological trait
Impersonation is possible	Impersonation is possible	Impersonation is impossible
Insecure	Not fully-secured	Fully-secured
Not suitable for public authentication	Not suitable for public authentication	Appropriate for public authentication

3.0 SURVEY STUDY

3.1 Basis of the Study

Previous studies have identified insecurity and inability to remember the knowledge associated with the authentication medium as the major problems of both token-based and knowledge-based authentication approaches (Anil et al., 2000; Nataliya, 2004; Alexander et al., 2008). This forms the basis for the two variables used in this study; i.e security and memorability, to evaluate the current evaluation methods so as to determine its suitability for public interaction. The following research questions and hypotheses were then formulated:

1. Do ATM users feel fully secured while authenticating their identity in public places using PIN?
2. Do all ATM users remember their PIN easily without inscription?

H1: Majority of ATM users are not fully secured while authenticating their identity in public places using PIN.

H2: Only few ATM users remember their PIN easily without inscription

3.2 Descriptions of Study

A quantitative study is conducted to describe the current perception of ATM users (ATM, being the most widely used public terminal that require authentication) on the use of personal identification number (PIN) in terms of security and memorability based on the findings of the previous study. A sample of 104 ATM users was taken using convenience non-probability sampling method. ATM users are chosen as our respondents being the most widely used public terminals that requires authentication. The study was conducted between January and February, 2009 and the response rate was encouraging.

Quantitative approach is considered the most applicable research method while describing human behaviour (Sekaran, 2000; Olakunle, 2003). A survey questionnaire is designed to collect data which was made up of two related constructs: security and memorability since the problems associated with the current authentication methods fall in to the two categories. ,the security variable is made up of eight items while the memorability consists six items (formulated from the assertion of previous authors like Anil et al., 2000; Nataliya, 2004; Alexander et al., 2008). The content of the instrument was validated using pilot testing while the construct validation was done through a computational method using SPSS 14.0. For the two constructs the reliability levels are 0.682 and 0.714 respectively (i.e. Cronbach's α for security = 0.682 and Cronbach's α for memorability = 0.714) as shown in tables 4 and 5 respectively.

4.0 RESULTS AND DISCUSSION

The two variables (security and memorability) are considered reliable with Cronbach's α of 0.682 and 0.714 respectively which is greater than the required average reliability of 0.50 as shown in tables 4 and 5. Similarly, only 7 respondents, representing (6.7%) of the sampled population, feel highly secured while authenticating their identities using the current knowledge-based PIN-entry method for transactions on ATM machines in public places while 81 respondents, representing (77.9%) are fairly secured and 16 respondents, representing (15.4%) are completely insecure as shown in Table 6 and Figure 2 below. At the same time, 29 respondents, representing (29%) of the sampled population find it very easy to remember their PIN during authentication, 62 respondents, representing (59.5%) of the sampled population find it fairly easy to remember their Pin during authentication while 13 respondents, representing (12.5%) of the sampled population do not find it easy to remember the PIN as can be seen from Table 7 and Figure 3 below meaning that the two hypotheses (**H1 & H2**) will be accepted These results are in line with the claims of the previous researchers like Manu et al. (2007); Alexander, Roman & Heirich, (2007); Desney et al., (2005) and Alexander et al., (2008). This shows that there are a lot of problems facing both the token-based and knowledge-based authentication method for interacting with public terminals for service rendering purposes.

Table 4: Reliability Statistics for Security

Cronbach's Alpha	N of Items
.682	8

Table 5: Reliability Statistics for memorability

Cronbach's Alpha	N of Items
.714	6

Table 6: Security categorization

		Frequency	%	Valid %
Valid	Highly secured	7	6.7	6.7
	Fairly secured	81	77.9	77.9
	Non secured	16	15.4	15.4
	Total	104	100.0	100.0

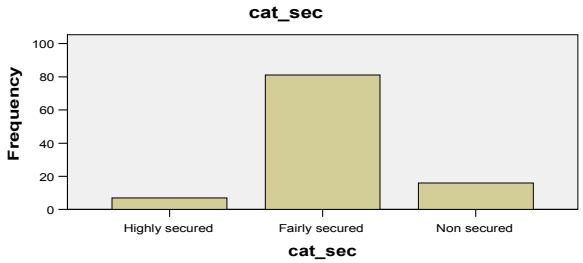


Figure 2: Security categorization

Figure 3: Memorability Categorization

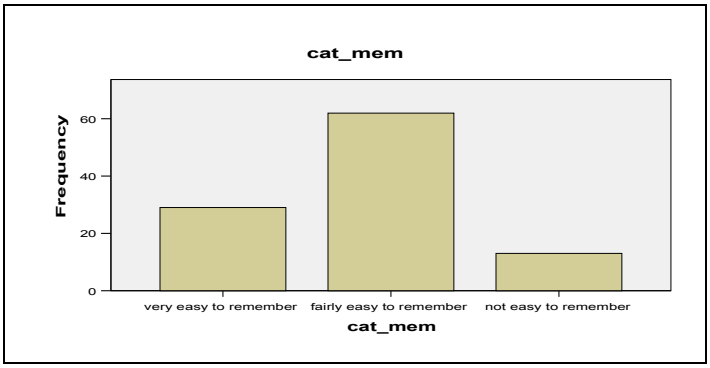


Table 7: Memorability categorization

		Frequency	%	Valid %
Valid	very easy to remember	29	27.9	27.9
	fairly easy to remember	62	59.6	59.6
	not easy to remember	13	12.5	12.5
	Total	104	100.0	100.0

5.0 CONCLUSION

Our conclusion is based on both the findings from the content analysis and the results from the survey study. From the result of the survey study, majority of users of ATM have both **security** and **memorability** problems, one can then arrive at the conclusion that there is need to migrate to biometric-based authentication due to the recorded deficiency of the existing authentication method in terms of security and memorability. With the aforementioned findings resulting from related publications, it can be seen that, gaze-based (iris-based) authentication approach off all biometric methods, is considered the most promising way of reducing shoulder surfing and other authentication problems experienced by users of public zone terminals.

References

Alexander, D., Roman. W. & Heiko, D. (2007) Evaluation of Eye-Gazed Interaction Methods for Security Enhanced PIN-Entry. *CHI 2007 Proceeding, Australia*, pp 199 - 202

Alexander, D., Roman, W. & Heinrich, H. (2007) PassShape-Stroke based Shape password, *CHI Proceeding* ,pp. 239- 240.

Alexander De Luca, Roman Weiss, Heinrich Hussmann and Xueli An, (2008) Eyepass- EyeStroke Authentication for Public terminals. *CHI proceedings, Italy*, pp. 3003 – 3008.

Alexander, P. P.& Peter, P. (2008). Understanding User Perspectives on biometric technology. *Communication of the ACM*, Vol. 51, No. 9, pp. 115 – 118.

Akhilesh, C. & Thomas, C. (2005). Challenges and Constraints to the Diffusion of Biometrics in Information Systems. *Communication of the ACM*, Vol 48, No.12, pp. 101 – 106.

Anil, J., Lin, H. & Sharath, P. (2000). Biometric Identification. *Communication of the ACM,* Vol. 43, No. 2, pp. 91 -98.

Anil, K. J., Karthik, N. & Abhishek, N. (2008). Biometric Template Security. *EURASIP Journal of Advances in Signal Processing,* Vol. 2008, No. 579416, pp. 1 – 17.

Barry, S. & Peter, N. (2002) Will Fingerprinting stand up in Court? *A Publication of the New York Times*.

Bergadano, F., Gunetti, D., & Picardi, C. (2002) User Authentication Through Keystroke Dynamics. *ACM Transactions on Information and System Security (TISSEC)*, Vol.5, No. 4, pp.367-397.

Bruce, S. (1999). The Uses and Abuses of Biometrics. C*ommunications of the ACM*, Vol. 2, No. 8., p. 136.

Checco, J. (2003) Keystroke Dynamics and Corporate Security. *WSTA Ticker Magazine.*

Chellapa, R., Wilson, C., & Sirohey, A. (1995). Human and machine Recognition of Faces: A survey. *Proceedings of IEEE,* Vol. 83, No. 5, pp 705 – 740.

Daugman, G. J. (2008) Anatomy, Physiology and Development of Iris. *www.cl.cam.ac.uk/HSB Electronic Identification Report (2008) Identification Solution and Biometric Enrolment.*

David, D. Z. (2004). Palmprint Authentication, *Kluwar Academic Publishers*.

Desney, S. T., Pedram, K. and Mary, C. (2005). Spy-Resistant Keyboard: More secured Password Entry on Public Touch Screen Displays. *ACM Digital Library, OZCHI 2005 Proceedings.* Page not indicated.

Fakhry, H. H. & Cardozo, B. B.(2006) Research and development of an Iris-Based Recognition System for Identification and Secure Authentication. *Information and Security International Journal*, Vol 19, pp. 39-57

Information Security Magazine. Search Security.com (2007), *http://www.searchsecurity.techtarget.com/sDefinition/* – Accessed October, 2008.

International biometric Industry Association reports (2008): Uses of Biometrics Identifiers; http:/www.ibia.org – Accessed October, 2008.

Jain, A. K., Hong, L. & Bolle, R. (1997) An identity authentication system using fingerprints. *Proceedings of the IEEE*, Vol. 85, No. 9. pp. 1365 – 1388.

Jain, A. K. Bolle, R.& Pakanti, S. (1999) Biometrics: personal identification in networked society. Kluwer, New York.

Jennifa, M. F. (2005) Privacy Made Public: will national security be the end of individualism? *Computers and Society,* ACM Digital Library, Vol. 35, No 1, pp. 1- 6.

Kaushik, R. & Prabir, B. (2008). Optimal Features Subset Selection and Classification for Iris Recognition. *EURASIP Journal on Image and Video Processing*, Vol. 2008, No. 743103, pp. 1 - 20.

Manu, K., Tal, G., Dan, B. and Terry, W.(2007) Reducing Shoulder Surfing by Using Gaze-based password Entry. *Symposium on Usable Privacy and Security (SOUPS), Pittsburg, USA.* pp. 13 – 19.

Mytas, S. M. & Stapleton, J. A. (2000). Biometric Standard for Information management and Security. *Computer Security*, Vol.19, pp. 428 – 441.

Michelle, B. & Xin, and L. (2007) What Do we know about Biometrics Authentication? *Information Security Curriculum Development Conference, ACM, Georgia, USA,* 978-1, page not indicated.

Nataliya, B. S. (2005). Access control and Biometrics. *Infosec Conference '04*, USA, pp. 124 – 127.

Olakunke, A. O. (2004). Research Methods in Social Sciences. (Second Edition), E-Book press, Norway.

Patrick, K. (2005). Biometrics: possible Safe Haven or lost Cause? *TheACM Digital library, Computer and Society,* Vol. 35, No.1, pp1 - 4.

Raviraj Technologies (2007) Iris recognition Biometric Authentication. *www.ravirajtech.com/iris-recognition*.

Sanchez-Avila, C., Sanchez-Keillo, K. and deMartin-Roche, D. (2002) Iris-based Biometrics recognition using dyadic wavelet transform. Aerospace Electronis System Magazine, IEEE, Vol. 17, No.10, pp. 3 – 6.

Sekaran, U.(2000). Research Methods for Business: a skill-building approach. NYC: John Willey Sons, Inc.

Schonberg, D. and Kirovski, D. (2008) Iris-based biometric identification. *Foreign Patent documents*.

Shanon, S. & Hamed, V. (nd) DNA as a Biometric Identifier; *http://www.findbiometris.com/article* – Accessed October, 2008.

Thomas, O. (2006) Keystroke Dynamics: Low Impact Biometric Verification.

[a] is a PhD candidate in the Faculty of Information Technology, UUM while [b] is his Supervisor.