Association for Information Systems
AIS Electronic Library (AISeL)

ACIS 2004 Proceedings | Australasian (ACIS)

December 2004

Biometrics Acceptance - Perceptions of Use of Biometrics

Angela Chau
University of New South Wales

Greg Stephens
University of New South Wales

Rodger Jamieson
University of New South Wales

Follow this and additional works at: http://aisel.aisnet.org/acis2004

Recommended Citation
Chau, Angela; Stephens, Greg; and Jamieson, Rodger, "Biometrics Acceptance - Perceptions of Use of Biometrics" (2004). *ACIS 2004 Proceedings*. 28.
http://aisel.aisnet.org/acis2004/28

This material is brought to you by the Australasian (ACIS) at AIS Electronic Library (AISeL). It has been accepted for inclusion in ACIS 2004 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.

Biometrics Acceptance – Perceptions of Use of Biometrics

Angela Chau
Greg Stephens
Rodger Jamieson - Director[1]

SEAR: Security, E-Business, Assurance Research Group
School of Information Systems Technology and Management
University of New South Wales Sydney NSW 2052 Australia
Ph: 61 2 9385 4414 Fax: 61 2 9662 4061
Email: angela.chau@optusnet.com.au
g.stephens@unsw.edu.au
r.jamieson@unsw.edu.au

Abstract

With the exception of Deane et al. (1995), Furnell et al. (2000), Clarke et al. (2002), Giesing (2003) and Ho et al. (2003), much of the research conducted in Biometrics has only examined the technical aspects of biometrics. Given the importance of user issues and the gap in existing literature, this exploratory study will attempt to understand the 'people' side of biometrics. To examine the issues behind user acceptance and biometrics, the Biometrics User Acceptance Model (Ho et al. 2003) will be explored. This will be used as a framework within which to answer the research questions: (1) What are the perceptions of user acceptance issues surrounding the use of a biometric authentication system?, and (2) What are the perceived enablers and inhibitors of biometric adoption? This model will be used as a basis for a survey instrument and will be tested on post graduate students at the University of New South Wales.

Keywords

Biometrics, Technology Acceptance Model (TAM), user acceptance issues, biometrics user acceptance model.

INTRODUCTION

'Biometrics' refers to the "automatic identification or identity verification of living, human individuals based on physiological and behavioural characteristics" (Wayman 2002, p.1). Physiological systems measure an individual's physiology and include techniques such as fingerprinting, face recognition, hand geometry, palm print, and iris scanning biometrics. Behavioural systems measure the way people perform tasks such as speaking, signing (signature) and using a mouse.

There has been extensive research conducted to investigate the technical issues of biometric systems, such as the performance and accuracy of different algorithms (Gutkowski 2004) and biometric extraction techniques (Kong et al., 2003). Julian Ashbourn, a founder of the International Biometric Foundation, notes that there has been very little research done surrounding user psychological issues and human factors that are associated with the use of biometrics (Ashbourn 2004, p.9). With the exception of Deane et al. (1995), Furnell et al. (2000), Clarke et al. (2002) Giesing (2003) and Ho et al. (2003), much of the research conducted in this field has only examined the technical aspects of biometrics. Given the importance of user issues and the gap in existing literature, this study will attempt to understand the 'people' side of biometrics.

This research dissertation will be using the Biometrics User Acceptance Model developed by Ho et al. (2003) in order to examine the user acceptance issues associated with biometrics use. Based on this model, a survey instrument will be developed and tested with post graduate students enrolled at the University of New South Wales.

RESEARCH PROPOSAL

Significance of this research

This research thesis seeks to test the Biometrics Acceptance Model that was developed in an earlier study by Ho et al. (2003). This model addresses the user acceptance issues surrounding the use of biometrics authentication systems. The research questions that will be explored in this study include:

[1] SAFE: Security, Assurance, Fraud-prevention for E-business Research Program at the Securities Industries Research Centre of Asia-Pacific.

1. What are the perceptions of user acceptance issues surrounding the use of a biometric authentication system?
2. What are the perceived enablers and inhibitors of biometric adoption?

By identifying the user acceptance issues from questions 1 & 2, this study will then consider how such issues may be addressed in order to raise the user acceptance of a biometric authentication system.

The findings of this research will have real practical applications for the community by highlighting the user acceptance issues that practitioners should take into account when implementing a biometric system. This research will also provide suggestions to overcome some of the user acceptance issues that governments, organisations and industries face in adopting biometric technology. Through this, practitioners will have a greater understanding of how to implement a more effective biometric system. This will lead to greater acceptance of the technology, or increased satisfaction for users in a mandated environment. Finally, by discovering what the drivers and inhibitors are of biometric technology, vendors and manufacturers of biometric technology may use this information to develop better marketing campaigns to educate consumers as to the benefits of biometric technology from a potential users' perspective.

BIOMETRIC USER ACCEPTANCE ISSUES

In terms of using biometrics for the purpose of identification and verification, Jain et al. (2004, p.4) identifies the following issues that need to be considered in the adoption of biometric technologies:

- performance – this refers to the achievable recognition accuracy and speed, the resources required to achieve the desired recognition accuracy and speed, as well as the operational and environmental factors that affect the accuracy and speed;
- acceptability – this indicates the extent to which people are willing to accept the use of a particular biometric identifier (characteristic) in their daily lives;
- circumvention – this reflects how easily the system can be fooled using fraudulent methods.

Other user acceptance issues were identified in a qualitative study conducted by Ho et al., (2003). These included:

- Security – the confidentiality, integrity, and availability of information used;
- Visibility – the level of direct interaction required during system usage;
- Perceived invasiveness – the apparent degree one's self is impinged upon;
- Privacy invasiveness – the disruption to one's ability to control personal information;
- Perceived safety – the beliefs of a person regarding the impacts that the system may have on his or her health or well-being;
- Information sensitivity –the perceived sensitivity of work material being protected by the biometric system;
- Identity assurance – the assurance that only authorised individuals are given access;
- Reliability – the probability that the system remains successful (does not fail) in achieving its intended objectives; and
- Convenience – this refers to a reduction of effort through using the system, thereby increasing the systems ease of use.

A study conducted by Giesing (2003) also identifies issues that influence user perceptions associated with biometrics use, but was limited by the context of Electronic Business. Giesing (2003) identified social factors including trust, privacy and fraud as factors that influence the adoption of biometrics. Also, similar to Ho et al.'s (2003) study, user perceptions including perceived ease of use and perceived usefulness were found to influence the adoption of biometrics.

BIOMETRIC ACCEPTANCE

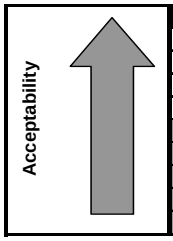
Of the few papers that have explored the acceptance of biometric technology, only Ho et al. (2003) and Giesing (2003) conducted empirical research on the user acceptance issues associated with biometric use. Earlier papers, Deane et al. (1995), Furnell et al. (2000), and Clarke et al. (2002) all examined the acceptability of different biometric techniques but did not consider the reasons behind such acceptability. Superficial conclusions were made based on conjecture but not as a result of empirical study.

Deane et al. (1995) conducted a survey comparing the acceptance of behavioural and physiological biometric techniques. The study found that in general, biometric techniques had a low acceptability rating with the exception of fingerprinting, voice and hand geometry. Retina scanning, signature analysis, keystroke analysis and pointing (mouse) had the lowest acceptability ratings. Furnell et al. (2000) also conducted a similar survey to assess the public attitudes to alternative forms of user authentication as compared to passwords. This study

found a high level of user acceptance for all the initial login authentication techniques suggested, including voice, fingerprint, signature, face, iris, signature, keystroke and mouse dynamics.

Clarke et al. (2002) conducted a survey of current mobile subscribers towards authentication on their phones. It presented different biometric techniques (fingerprint recognition, ear geometry, facial recognition, iris scanning, and typing style) as alternative authentication measures to protect their mobile phones, and found that respondents considered all techniques favourably.

The table below was adapted from Ho et al. (2003) to include the results from Clarke et al's. (2002) and Giesing's (2003) study. It shows the rankings of different biometric techniques from most acceptable to least acceptable across the different studies.



Deane et al., 1995	Furnell et al., 2000	Clarke et al., 2002	Giesing 2003
Fingerprint	Password	Fingerprint	Fingerprint verification
Password	Voice	Voice print	Voice recognition
Handgeometry	Face	Iris scanning	Face recognition
Voice	Fingerprint	Facial recognition	Retinal scanning
Signature Less than	Iris	Typing Style	Iris scanning
Retina acceptable	Hand geometry	Ear Geometry	None
Pointing (mouse)	Signature		
Keystroke	Keystroke		
	Mouse Dynamics		

Table 1: Ranked user preferences of security methods – a comparison between three studies (Source: Ho et al., 2003, p.36)

However, the limitation of the research conducted by Deane et al. (1995), Furnell et al. (2000) and Clarke et al. (2002) was that their was no attempt to understand the level of experience that the respondents had in regards to biometrics. Participants may have based their responses on actual use or on the limited knowledge they had in regards to the system, but no analysis was conducted to discover whether biometrics experience affect user perceptions. Also, these surveys only looked at comparing the acceptability of different biometric techniques. The research conducted did not go into depths to understand the reasons why one biometric system was more acceptable than another. There was no attempt to understand what the reasons and determinants of biometric acceptance were, with conclusions drawn from speculation and conjecture rather than from empirical evidence.

Giesing (2003) however, had examined what were some of the factors that influenced biometric acceptance, and concluded that user perceptions and social factors were issues behind the adoption of biometric technology. This study resulted in a development of a Technology Adoption Model, which was derived from the Technology Acceptance Model created by Davis (1989). However, all the issues identified by Giesing's (2003) study were also captured by Ho et al's. (2003) study within their Biometric Acceptance Model which was derived from the modified Technology Acceptance Model (Venkatesh & Davis 2000). The difference between these two models is that Ho et al. (2003) includes the driving and inhibiting external forces that lay behind the user and social factors identified by Giesing (2003). It is for this reason that this research will be examining the Biometric User Acceptance Model (Ho et al 2003) in more detail.

The study conducted by Ho et al. (2003) examined user acceptance issues surrounding biometric authentication systems by conducting interviews and surveys with managers and users of biometric authentication systems. Through this, Ho et al. (2003) identified drivers and inhibitors of biometric acceptance, and developed the Biometrics User Acceptance Model.

THEORY AND METHODOLOGY

There has been extensive research conducted on technology acceptance and adoption. To examine the issues behind user acceptance and biometrics, the Biometrics Acceptance Model (Ho et al. 2003) which is derived from Venkatesh & Davis's (2000) extended Technology Acceptance Model (TAM2) will be explored. This will be used as a framework within which to answer the research questions surrounding the user acceptance issues for biometrics. The TAM has been used extensively to explain why a technology or system has been unsuccessfully or successfully accepted by its users. In a biometric context, the ease and comfort in interaction with a biometric system contribute to its acceptance (Jain et al., 2004), therefore TAM is a useful model in examining biometric user acceptance.

Biometric Acceptance Model

The Biometric Acceptance Model (Figure 1) developed by Ho et al. (2003), is derived from the extended TAM2 (Venkatesh & Davis 2000). Ho et al. (2003) used TAM2 as a framework to explain biometric authentication acceptance issues and modified it to include determinants that were specific to biometric authentication systems.

Their research, unlike Furnell et al. (2000), Clarke et al. (2002) and Deane et al. (1995), was conducted with organisations that had actually implemented a biometric authentication system. Their study involved semi-structured interviews conducted with managers. Surveys were also completed by users and managers of the biometric authentication system.

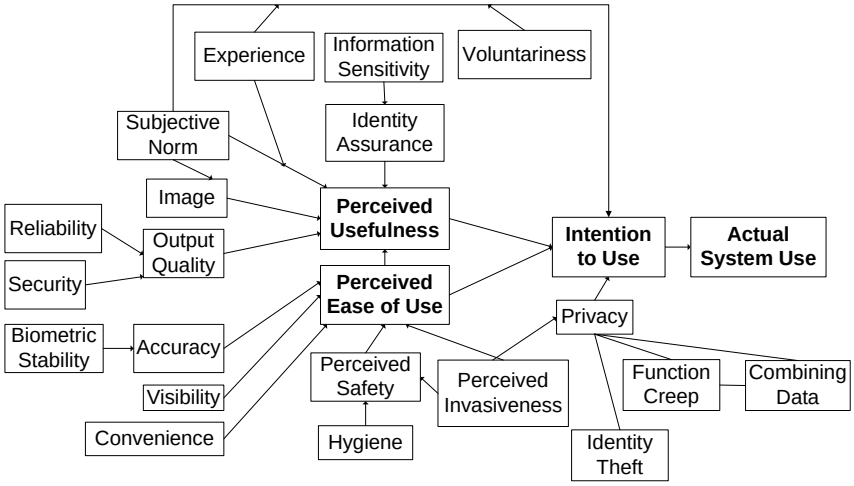


Figure 1: Biometrics Acceptance Model (Source: Ho et al., 2003)

Perceived Usefulness

For a biometric authentication context, Ho et al. (2003, p.41) redefine perceived usefulness as "the degree to which a person believes that using a particular biometric system would fulfil the organisation's security access requirements in a particular domain". As a biometric authentication system is not directly related to job performance, job relevance was removed as a determinant. Result demonstrability was also removed from the model. Ho et al. (2003, p.97) argue that this is not relevant to biometrics since it is a "preventive innovation" and as such, the benefits of a biometric authentication system are intangible.

Ho et al. (2003) extended TAM2 to include security, reliability and identity assurance as determinants of perceived usefulness of biometric systems. Ho et al's (2003) results show that identity assurance and information sensitivity, security, reliability and subjective norm were influential determinants of perceived usefulness, with identity assurance being the main reason why biometrics is adopted Security and reliability were highly ranked in their importance however interestingly, security and reliability were not a concern to users and managers as they assumed that a biometric system deployed by their organisation was reliable (Ho et al., 2003, p.93).

From TAM2, the effects of subjective norm will only occur in a mandatory or non-voluntary system usage setting where a referent will have the power to reward or punish non-behaviour (Venkatesh & Davis 2000, p.188). Biometric authentication systems are usually subject to mandatory usage, and one may argue the relevance of the TAM in such a situation. However, a mandated environment may still result in users having negative attitudes towards the system. Brown et al. (2002, p.291) contend that if perceptions of usefulness are low, negative attitudes can arise which may result in negative repercussions. This may lead to sabotage or users misusing the system, for example, allowing tailgaters into the building and thus bypassing the authentication system. Therefore it is important to understand users' perceptions to be able to educate and promote positive attitudes towards the technology and its use (Brown et al., 2002, p.291).

Perceived Ease of Use

Ho et al. (2003) do not modify the definition for perceived ease of use as the original definition, "the degree to which a person believes that using a particular system would be free of effort" (Davis 1989) is applicable to the biometrics domain. However, Ho et al. (2003) add accuracy, visibility, convenience, perceived safety, hygiene and perceived invasiveness as determinants of perceived ease of use.

The results of this study found that convenience, perceived safety and hygiene were the most influential determinants of perceived ease of use. Convenience was seen as an important acceptance factor with many users mentioning some type of convenience as a reason why they chose to use the system. However, the study also highlighted that security is a priority over convenience, as there is no advantage of simplifying the security process if it compromises security (Ho et al., 2003, p.92).

Perceived safety reflects the beliefs that people have regarding safety that may or may not be true, for example, iris scanners are only taking a photo of a person's eye yet users may be concerned about damage to their eyes. Hygiene was a dominant factor in user acceptance for those users that require direct contact with the biometric

system, eg, fingerprint scanning devices. Users of iris-based systems do not require any contact with the system and hence raised no hygiene problems (Ho et al., 2003, p.91).

Intention to Use

Ho et al. (2003) add privacy as a determinant of intentions to use. Ho et al's. (2003) study into the issue of privacy discovered that the concerns relating to privacy include Function Creep, Combining Data and Identity Theft. However, Ho et al's (2003, p.96) research found that privacy was not a deep-rooted concern, as "users seemed to place considerable trust in the organisation, where simple assurance regarding the privacy of their biometric data seemed to appease them."

Limitations

The limitation of Ho et al's (2003) research was that the causal relationships developed in the Biometrics Acceptance Model were not determined statistically due to the limited number of participants (Ho et al., 2003, p.116). However, it provides a helpful framework for understanding the biometric acceptance issues. The main objective of this research is to understand what the user acceptance issues are for biometric authentication systems. The Biometrics Acceptance Model (Ho et al., 2003), provides a simple yet strong framework to be used as a basis for this research as it carries with it the foundations of the extensively tested TAM (Davis 1989) and TAM2 (Venkatesh & Davis 2000), see Henderson et al., (2003) and Chen et al., (2002).

Research Methodology

This exploratory study will be conducted using a quantitative methodology with a questionnaire developed as the research instrument. The questionnaire will be created based on the research framework developed by Ho et al., (2003), the Biometrics User Acceptance Model. The questionnaire will contain three sections:

- Background information: Including questions related to demographics, information technology experience, internet use and knowledge of/experience with internet scams.
- Biometric Experience: this section will be used to determine the level of exposure a participant has had to actual use of biometric technology.
- Perception of Use of Biometrics: this section aims to measure the perceptions that participants had towards the use of biometrics. The questions relate to:
  - the Technology Acceptance Model (TAM) by Davis (1989), including Ease of Use, Usefulness and Actual Use;
  - the user acceptance issues identified in the Biometrics User Acceptance Model (Ho et al., 2003), which was adapted from Ho et al.'s (2003) user questionnaire;
  - the ranking of preferences for a given set of biometric techniques;
  - what participants considered as the drivers and inhibitors of biometric use. The issues listed were derived from Ho et al.'s (2003) study, which identified the influential acceptance issues from a user's perspective.

The questionnaire will be completed by post graduate students studying in the school of Information Systems at the University of New South Wales. The results gathered from this survey will then be analysed using Structured Equation Modelling (SEM).

CONCLUSION

This paper has presented a review of some of the literature relating to user acceptance issues of biometric authentication systems. It is clear that there has been little research conducted in this area with the exception of Deane et al. (1995), Furnell et al. (2000), Clarke et al. (2002) and most recently, Giesing (2003) and Ho et al. (2003). The identified gap in literature therefore gives leverage for this research to explore the little known area of user acceptance issues in biometrics. The Biometrics User Acceptance Model developed by Ho et al. (2003) establishes a strong framework for this research to discover what the user acceptance issues are in biometric authentication. This exploratory study will be particularly useful in understanding the drivers and inhibitors of biometric adoption and will also attempt to discover how such issues can be addressed in order to raise the user acceptance of biometric authentication systems.

REFERENCES

Ashbourn, J., 2004, 'Where We Really Are With Biometrics', *Biometric Technology Today*, vol. 12, issue 4, April 2004, pp. 7-9

Brown, S. A., Massey, A. P., Montoya-Weiss, M. M., & Burkman, J. R., 2002, 'Do I Really Have To?' User Acceptance of Mandated Technology', *European Journal of Information Systems*, 11, 283-295.

Chen, L., Gillenson, M.L., & Sherrell, D.L., 2002, 'Enticing online consumers: an extended technology acceptance perspective', *Information and Management*, vol. 39, issue 8, pp 705-719

Clarke, N. L., Furnell, S., Rodwell, P. M. & Reynolds, P. L., 2002 'Acceptance of Subscriber Authentication Methods for Mobile Telephony Devices' *Computers & Security*, vol. 21, issue 3, pp. 220-228

Davis, F.D., 1989, 'Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology', *MIS Quarterly*, vol. 13, pp. 319-339.

Deane F., Barrelle, K., Henderson, R. & Mahar, D., 1995, 'Perceived acceptability of biometric security systems', *Computers & Security*, vol. 14, issue 3, pp. 225-231.

Furnell, S. M., Dowland, P. S., Illingworth, H. M. & Reynolds, P. L., 2000, 'Authentication and Supervision: A Survey of User Attitudes', *Computers & Security*, vol. 19, issue 6, 1 October 2000, pp. 529-539.

Giesing, I., 2003, 'User Perceptions Related to Identification Through Biometrics within Electronic Business' University of Pretoria, 21 November 2003, URL http://upetd.up.ac.za/thesis/available/etd-01092004-141637/, Accessed 2 October 2004.

Gutkowski, P., 2004, 'Algorithm for Retrieval and Verification of Personal Identity Using Bimodal Biometrics', *Information Fusion*, vol. 5, issue 1, March 2004, pp. 65-71.

Henderson R., & Divett, M.J., 2003, 'Perceived usefulness, ease of use and electronic supermarket use', *Internation Journal of Human-Computer Studies*, vol. 59, issue 3, pp. 383-395.

Ho, G., Stephens, G., & Jamieson, R., 2003, 'Biometric Authentication Adoption Issues'. *Proceedings of the 14th Australasian Conference on Information Systems*, 26-28th November 2003, Perth, Western Australia ISBN: 0-7298-0544-1.

Jain, A. K., Ross, A., & Prabhakar, S. 2004, 'An Introduction to Biometric Recognition', *IEE Transactions on Circuits and Systems for Video Technology*, vol. 14, no. 1, January 2004, pp.4-20.

Kong, W.K., Zhang, D. & Li, W., 2003, 'Palmprint Feature Extraction Using 2-D Gabor Filters', *Pattern Recognition*, vol. 36, issue 10, October 2003, pp.2339-2347.

Venkatesh, V. & Davis, F., 2000, 'A Theoretical Extension of the Technology Acceptance Model: Four Longitudinal Field Studies' *Management Science*, vol. 46, no. 2, February 2000, pp. 186-204

Wayman, J. L (2002) Digital signal processing in biometric identification: a review, 2002 International *Conference on Image Processing* (Proceedings), vol. 1, pp. I-37 –I-40.

COPYRIGHT

Angela Chau, Greg Stephens, Rodger Jamieson © 2004. The authors assign to ACIS and educational and non-profit institutions a non-exclusive licence to use this document for personal use and in courses of instruction provided that the article is used in full and this copyright statement is reproduced. The authors also grant a non-exclusive licence to ACIS to publish this document in full in the Conference Papers and Proceedings. Those documents may be published on the World Wide Web, CD-ROM, in printed form, and on mirror sites on the World Wide Web. Any other usage is prohibited without the express permission of the authors.