Chapter 7
Towards an Understanding of User Acceptance to Use Biometrics Authentication Systems in E-Commerce: Using an Extension of the Technology Acceptance Model

Fahad AL Harby
University of Bradford, UK

Rami Qahwajim
University of Bradford, UK

Mumtaz Kamala
University of Bradford, UK

ABSTRACT

Security is an increasingly important issue for business, and with it, the need for authentication. The use of biometric systems for personal authentication is a response to the rising issue of authentication and security. As with any new technology, user acceptance is often hard to measure, thus, in this work, a study of user acceptance of a biometrics authentication system in e-commerce, such as online banking within the Saudi society, was conducted. The study examined whether Saudis are practically willing to accept this technology by involving 306 participants in a large scale laboratory experiment that actively tested a biometric authentication system in combination of a survey. The Technology Acceptance Model (TAM) was adopted as the theoretical basis to develop the research framework in which the model has proven its efficiency as a good predictor for the study’s application.

DOI: 10.4018/978-1-61350-462-8.ch007
INTRODUCTION

Due to the rapid development of e-commerce during the last decade, e-commerce activities such as online banking have become widely accepted in industrialised countries such as UK and partially accepted in less industrialised countries such as Saudi Arabia. The following table shows a comparison of the levels of online banking use in the two countries (Alsajjan, 2008) (Table 1).

<table>
<thead>
<tr>
<th>Country</th>
<th>Population¹</th>
<th>Number of Internet Users</th>
<th>Registered banks²</th>
<th>The percentage of online banking users of total banks users</th>
<th>Industry Net Income (£ mil)</th>
</tr>
</thead>
</table>

Securing online banking log in access is becoming increasingly important. Identity theft, hacking, and viruses are growing threats to online banking users. As more people use the internet, more identity theft cases are being reported. This could harm not only the users but also the reputation of the organisations whose names were used in these illegal acts. Over 8.4 million Americans had their personal information compromised during 2007. For the same year, the loss caused by referred complaints was $239.09 million. In 2007, the latest UK statistics have estimated losses due to online banking fraud at £22.6 m³.

The use of biometric authentication is a response to the rising issue of security. Biometrics devices have the obvious benefit of not falling prey to many of the well known vulnerabilities of traditional methods (James et al., 2006). While a biometric device uses a unique biological trait to distinguish an individual, it is very difficult and often impossible for the identifier to be lost, stolen, duplicated, or given away (Liu & Silverman, 2001; James et al., 2006). This advantage makes biometric authentication an attractive opportunity for individuals and organisations that wish to adopt a new security technology. The most widely used method of biometric authentication is fingerprint recognition. Fingerprints are well known to be unique for each person, and, for this reason, they are considered a secure method of authentication (Jain, 2004). The choice of fingerprints over other biometric technologies was due to their low cost, ease of use, reliability and high accuracy (Jain, 2004). Choosing fingerprints could also make it easier to overcome cultural issues that may arise if other features such as speech or faces are used.

Online banking is among to which biometrics may be applied (Liu & Silverman, 2001). Several companies look forward to using biometric technologies for authentication as it could reduce losses because of fraud (James et al., 2006). Biometrics technology can help prevent illegal financial transactions and identity theft (Jain et al., 2000; Herman, 2002).

Many benefits can be gained from using a fingerprint biometrics authentication within online banking applications, such as ease of use (since no data input (user ID and password) are required from the user), and reducing data vulnerability. Another benefit is increased security and decreased risk of viruses, as the browser is built in such a way that there is no need to type the Uniform Resource Locator (URL). As a result, phishing would be reduced due the lack of data input by user. Moreover, the benefits of investigating biometric authentication systems in online banking will secure the log in process to the system and removes password vulnerabilities; enhanced convenience such as employees quickly log in using their finger; reduced help desk costs by eliminates calls for password resets.
Related Content

Drivers and Inhibitors to XBRL adoption: A Qualitative Approach to Build a Theory in Under-Researched Areas
[www.igi-global.com/article/drivers-inhibitors-xbrl-adoption/1895?camid=4v1a](www.igi-global.com/article/drivers-inhibitors-xbrl-adoption/1895?camid=4v1a)

Patterns for Designing Agent-Based E-Business Systems
[www.igi-global.com/chapter/patterns-designing-agent-based-business/9416?camid=4v1a](www.igi-global.com/chapter/patterns-designing-agent-based-business/9416?camid=4v1a)

The Emerging Application Ecosystems: An Introductory Analysis of Android Ecosystem
[www.igi-global.com/article/the-emerging-application-ecosystems/114184?camid=4v1a](www.igi-global.com/article/the-emerging-application-ecosystems/114184?camid=4v1a)

Real Time Decision Making and Mobile Technologies
[www.igi-global.com/chapter/real-time-decision-making-mobile/19541?camid=4v1a](www.igi-global.com/chapter/real-time-decision-making-mobile/19541?camid=4v1a)