SMART CARDS AND THE FINGERPRINT: A FRAMEWORK FOR USER IDENTIFICATION AND AUTHENTICATION

M. H. Omar, R. Din, and H. M. Tahir

Faculty of Information Technology,
Universiti Utara Malaysia, 06010 UUM Sintok, Kedah

Tel: 04-928 4662, Fax: 04-928 4753, E-mail: hasbullah@uum.edu.my
Tel: 04-928 4617, Fax: 04-928 4753 , E-mail: roshidi@uum.edu.my
Tel: 04-928 4659, Fax: 04-928 4753 , E-mail: hatim@uum.edu.my

ABSTRACT

Access control has been a great concern in this Information and Communication Technology (ICT) era. The need to control access to certain information and resources has been taken seriously by the ICT community. This research believes that no single security method, algorithm, key or procedure is entirely secure. Hence, a combination of multiple security components is mandatory to provide a high level of protection against fraud and other threats. This research combines two security components, which are the smart card and fingerprint recognition. It looks into the vulnerabilities of magnetic-stripe cards and Personal Identification Numbers (PIN) or passwords widely used in systems today. As a result, the research proposes a framework for user identification and authentication in automatic-teller-machine (ATM) systems using fingerprints and smart cards as opposed to the PIN and magnetic-stripe cards.

Key words: Smart Cards, The Fingerprint, Automatic-Teller-Machine (ATM), Identification and Authentication (I&A).

1.0 INTRODUCTION

To date, most information systems authenticate their users by the use of passwords or Personal Identification Numbers (PIN) (Gaskell, 2000). This use of the password or PIN schemes was introduced in the early days of multi-user (time-sharing) machines and its use has continued into today's highly networked and distributed systems (Omar, 2002). The system does not further identify users if the

password or PIN is correctly entered because the password or PIN is meant to be known only to the authorized user. This allows anybody related or unrelated to the user who knows the user's password or PIN to make illegal access or withdrawal.

In a password or PIN based system, it is assumed that all parts of the system are trustworthy (Gaskell, 2000). It is assumed that the end user device (e.g., a terminal or personal computer) is free from any untrustworthy activities such as password sniffing or system tapping.

In order to achieve a greater level of security along with greater flexibility, smart cards are being pushed as a replacement for magnetic-stripe cards. Some large corporations and governments have mandated the use of token based authentication for their new and existing applications. Therefore, smart cards and biometrics are seen as a good combination for enhancing user identification and authentication in computer security.

This research concentrates on the security features of the smart card for user identification and authentication compared to the conventional magnetic-stripe card. It also suggests the PIN replacement by user unique biometrics feature, i.e., the fingerprint. The prototype system developed potrays a potentially high security token-based system for accessing ATMs in the future.

1.1 Identification and Authentication (I&A)

The I&A is defined by the United States National Institute of Science and Technology (NIST) as a process for verifying a user identity (NIST, 1995). Identification is concerned with how the user provides his/her unique identity to the system. The identity must be unique so that the system can distinguish one user from another. Authentication, on the other hand, is the process of associating an individual with his/her unique identity, which is the manner he/she establishes the validity of his/her claimed identity. Authentication consists of three methods (Corcoran et al., 2000):

- Something you are (e.g., biological characteristics)
- Something you possess (e.g., a token or a card)
- Something you know (e.g., password or PIN)

This research believes that 'something you are' (i.e., the fingerprint) would be a better identification method rather than 'something you know'.

1.2 The Personal Identification Number (PIN)

Automatic-teller-machines (ATM) use magnetic-stripe cards to identify and authorize the person accessing them. The card contains details of the user's bank account and is protected by a Personal Identification Number (PIN). Users must enter the PIN associated with their card before they are allowed to perform any transaction with their account. The scheme is flawed in that the only items needed to authorize the ATM transaction are the card and the PIN.

The PIN, like the password, is a piece of information that falls into the category of 'something the individual knows', which is easy to forget. Cards are easily stolen or misplaced and PINs are also vulnerable. Passwords and PINs can easily be cracked by hackers since there are a finite number of alphabets and alphanumericals to choose from. A password uses 52 choices of alphabets (lower and upper case letter) and 10 choices of numbers in its combinations while the PIN has only 10 numerical choices. This makes the PIN more vulnerable than the password (Omar, 2002).

People tend to choose passwords or PINs that can be easily guessed compared to well-chosen passwords or PINs which are difficult to remember (Gong et al., 1993). These poorly chosen passwords or PINs are vulnerable to attacks based upon copying information (e.g., the result of applying a one-way hash function to a password or of encrypting a message using the password as the encryption key) and experimenting on it off-line. Although long passwords are hard to crack, they are inconvenient to memorize which lead users to write the password or PIN down.

1.3 Magnetic-stripe Cards

The magnetic-stripe card has been used widely in the banking sector. Unfortunately, it is facing a threat since it has been discovered that it can be cloned and is therefore prone to fraud. Ever since these cards were introduced, attempts have been made to alter or counterfeit them in order to obtain funds illegally.

The most common method for magnetic stripe theft and fraud is by card withholding. Card withholding is done by installing a special programmed machine or device to record the card information, collecting the PIN from the unsuspecting customers and letting the system inform them that the transaction they requested could not be processed. Days later, the criminal collects the information and makes bogus ATM cards and then uses them to withdraw money from the victim's accounts via ATMs (Omar, 2002).

A more sophisticated method is the skimming technique. It uses a skimmer, which is a black box the size of a palm pilot with a slit down the front and bits of Velcro tape on the back. The device can read and store data embedded within a charge card's magnetic-stripe—not only the name, number and expiration date that appears on the card's face, but also an invisible, encrypted verification code that is transmitted electronically from merchant to card issuer to confirm a card's validity at the point of sale. With the data retrieved, the counterfeiter has enough information to create a perfect clone of the charge card.

Furthermore, on April 8, 2000, Tan Sri Dato' Seri Ali Abul Hassan bin Sulaiman, the Governor of Bank Negara Malaysia, announced that they have investigated the recent reports on incidents of unauthorized ATM withdrawals, and found that virtually all of the unauthorized ATM withdrawals were due to cloning by syndicates of the ATM cards issued by two commercial banks and one non-bank financial institution (Bank Negara Malaysia, 2000).

The flaws in password or PIN and the vulnerabilities of magnetic-stripe cards have given significant motivation to substitute them with fingerprint recognition and smart cards respectively.

2.0 METHODOLOGY

The basic methods may be employed individually, but many user login systems employ various combinations of the basic authentication methods. Traditional automatic personal identification technologies, which use 'something you know', such as PIN or 'something you posses' such as ID card, key or both, to verify the identity of a person, are no longer considered reliable enough to satisfy the security requirements of electronic transactions (Jain et al., 1997). Therefore, this paper combines two methods which are 'something you are' and 'something you possess'.

The 'Something you are' provides a very sophisticated method for identifying users called biometrics. It uses the unique characteristics (or attributes) of an individual to authenticate the user's identity. These include physiological attributes (such as fingerprints, hand geometry, or retina patterns) or behavioral attributes (such as voice patterns and hand-written signatures). Biometric authentication technologies based upon these attributes have been developed for computer log-in applications (NIST, 1995).

The 'Something you possess' is mostly combined with the 'something you know' method. The obvious example is the ATM which combines the magnetic-stripe card and the PIN. The magnetic-stripe card is given by the bank in order to make

transactions with their ATM and the PIN is used to identify them. The objects that a user possesses for the purpose of identification and authentication are called tokens. In this prototype, in order to obtain or be granted access to certain accounts, users need to fulfill two conditions. They should have the authorized card or token from the bank and also their fingerprint.

2.1 Fingerprint Identification

The easiest 'something you are' characteristic to capture and process is a fingerprint. It is also very easy for a user to supply and is neither invasive nor inconvenient since the user would use their finger for pressing buttons to initiate transactions anyway and touching a fingerprint reader momentarily is no extra effort. In fact, among all the biometric techniques, fingerprint-based identification is the oldest method which has been successfully used in numerous applications (Jain et al., 2001). There are three main methods to capture fingerprint images, which are optical, capacitive and thermo-conductive. The optical method is implemented with a small camera and light source to capture an image of a fingerprint. The capacitive method makes full use of the human body's natural electrical charge to measure the differences in capacitance value between ridges and valleys in a fingerprint and certain algorithms are used to construct an image from the capacitance values. The last method, which is the thermo-conductive method, is done by measuring the human tissue's thermal conductivity characteristics differences between the ridges and valleys of a fingerprint. In other words, the ridges and valleys conduct heat at different rates and these minute differences can be registered. The last two methods are reliable for differentiating a living finger and a dead finger (Omar et al., 2001). The research uses the capacitive method provided by the Gemplus GemPC-Touch430 reader.

The fingerprint is processed by comparing the captured image and the present image provided by the user. Before the comparing process can occurr, the images need to be reduced to their key features called minutiae points. Users are identified by using the one-to-one method where the key feature of the original fingerprint is being compared to the template stored on the smart card. Additional characteristics include the core, which approximates the centre of the pattern, and the axis, which represents the vertical orientation of the finger as shown on fig 1.

Each individual possesses one unique arrangement of minutiae. This can be described by the probabilistic model as (Omar, 2002): $P(C) = P(N).P(M).P(A)$

where:

$P(N)$ = f(Poisson's Law)
$P(M)$ = f(frequency of appearance of minutiae type)

P(A) = f(number of possible permutations of minutiae)

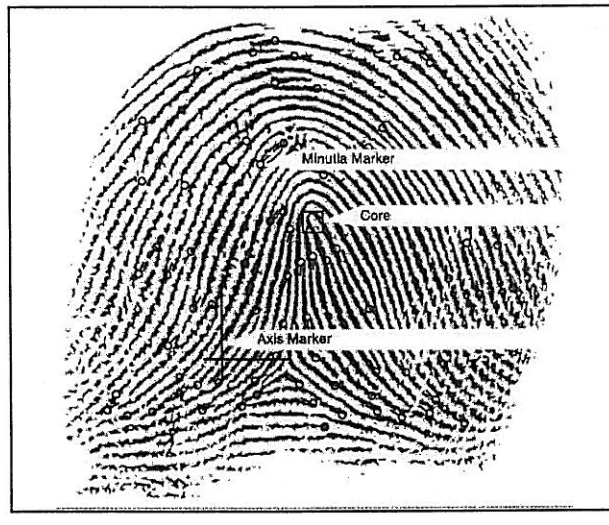

Fig 1: A Fingerprint Image Showing Core, Axis Marker, and Marked Minutiae.

From the probabilistic model, to find two identical fingerprint is 1 over 8 billion fingerprints. Therefore the fingerprint is most suitable for identification purposes. Fingerprint identifications need a closeness-of-match threshold for comparing the measured features of the user to the pre-recorded values, allowing access if there is a match (Ganger, 2001). This closeness-of-match threshold is due to the changes in the fingerprint itself because of the change in the measurement environment. Fig 2 below illustrates the closeness-of-match thresholds for biometric-based authentication and the corresponding trade-off between false acceptance rate and false rejection rate.

Fig 2(a) shows possible distributions of closeness value for a user and an impostor. Each cut-off threshold would sometimes reject the real user and sometimes accept the impostor. Specifically, at a given cut-off threshold, false accepts are to the right of the dashed line and false rejects are to the left of the solid line. As fingerprint accuracy improves, the area beneath the user's distribution would increase and that beneath the imposter's curve would decrease. Fig 2(b) illustrates the trade-off between false acceptance rate and false rejection rate more directly with the common "Receiver Operating Characteristic" curve. A biometric accuracy would be good if the space beneath the curve is reduced.

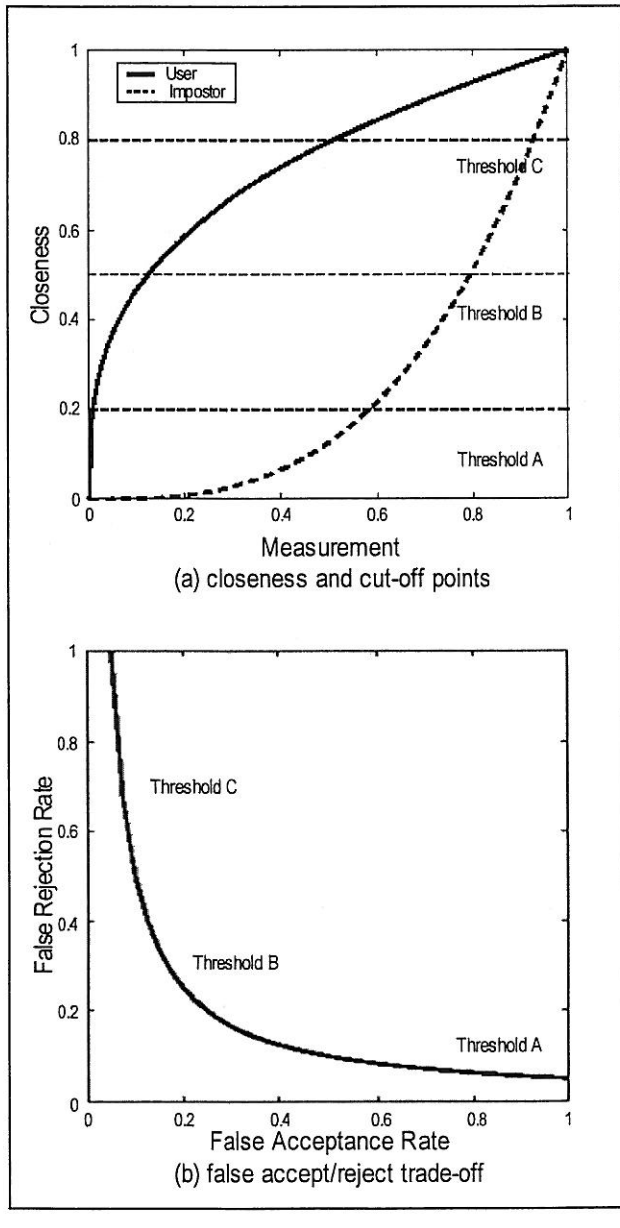

Fig 2: The Closeness-of-Match Thresholds and False Acceptance/Rejection Trade-Off (Ganger, 2001)

2.2 Smart Card

The fingerprint offers a viable alternative to PIN; however, there is also a need to have a reliable storage of the authenticated fingerprint key features that falls into the category of 'something you possess'. Smart card is a device typically having the size and shape of a credit card. It contains one or more integrated chips that can perform functions of a computer, consisting of a microprocessor, memory and input/output (NIST, 1995). Smart cards are more secure than magnetic-stripe cards. The data stored is not easily accessible because it contains a processor. Smart card security could be enhanced by encryption algorithms implemented on the card so that the data is safe from system tapping. In fact, the maximum storage capacity of a smart card is many times greater than that of a magnetic-stripe card (Rankl and Effing, 2000).

ATM users are used to the magnetic-stripe card dimension and the smart card works in the same way. Hence, it is not difficult to implement the scheme to the user. Smart card is a mature technology which currently enjoys widespread use in many applications. The technology is constantly progressing and getting easier to develop. Furthermore, the flexibility of the smart card allows many different applications to be integrated onto one card. Its proponents see all of one person's identification, authentication, access control and even purchasing revolving around their single personal smart card. Whether this happens or not, smart cards offer an excellent identification and authentication tool for ATM users and providers.

3.0 THE FRAMEWORK

This research adapts the framework outlined by the American Biometric Company (1999). The ABC model relies on a two-factor level of security, which are the smart card and the fingerprint for logon to the workstation beyond the password, which it claims provides incremental access control to secure their IT environment. In addition, the model also allows the use of Public Key Infrastructure (PKI) which consists of Certificate Authority (CA), secure backup, Certificate Revocation Server and also virtual private networks (VPNs). The model also supports current industry standards for interfacing with cryptographic tokens, such as smart cards, known as PKCS#11.

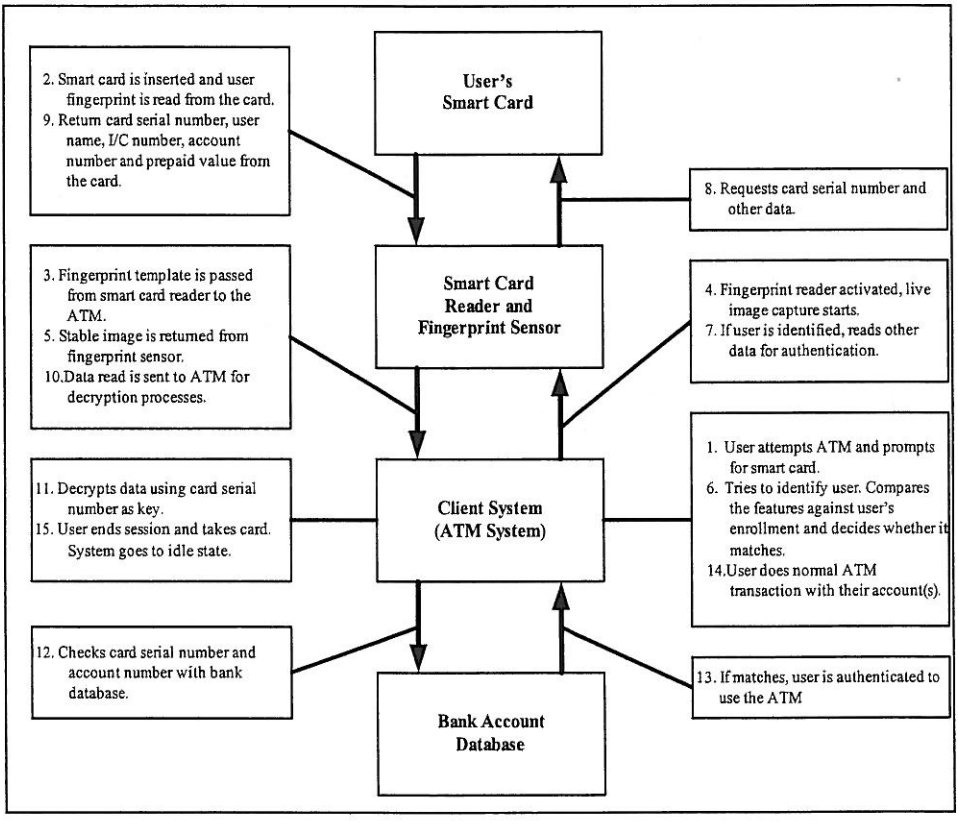

Fig 3: A Framework for Identification and Authentication for ATM system.

The system identifies and authenticates its user using the smart card, fingerprint recognition and PIN. The system still relies on PIN which is the component that the research wants to replace. Moreover, the system uses the authentication server for comparing the fingerprint against user enrollments. Keeping user fingerprints in a server will result in privacy concerns since the fingerprint templates are exposed to fraud either from a hacker or an inside person (i.e., the person in charge of the system). As a result, the research has modified and come up with the framework for identification and authentication for ATM systems as shown in Fig 3. To prove the framework's integrity, two prototype systems have been built and further discussed in the next section.

4.0 THE PROTOTYPE SYSTEMS

Basically the prototype systems consist of two components which are administrator component and client component. The administrator component is used to store user's specific data such as name, identity card number, account number and the fingerprint template. In the process of enrolling the user, the administrator will key-in user's particulars, captures the fingerprint image and identify the key features, verify the fingerprint and stores it onto the smart card. Besides storing user's particulars onto the smart card, they will also be stored to a database for record and recovery purposes.

The client component is built based on the Hachez et al. (2000) model (Fig. 4). The model consists of four components which are measure device, feature extraction unit, comparison unit and reference database. The measure component is in charge of capturing the user's fingerprint when he or she tries to identify himself or herself.

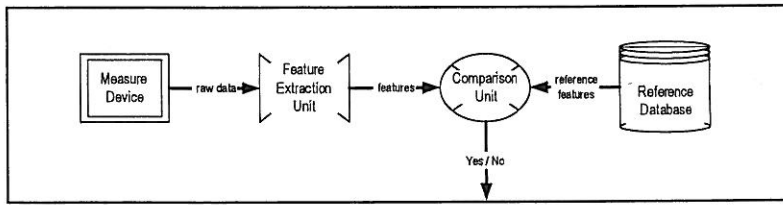

Fig 4: Components of The Model (Hachez et al., 2000)

Then the fingerprint image is passed to the feature extraction unit. Feature extraction unit takes the raw image and extract key features from it. Next, the key features are passed to the comparison unit which compares it with the key features stored in a reference database. A reference database is not always the centralized database. This study suggests that a smart card is more reliable for storing user's data and fingerprint template compared to a centralized database.

The client component acts exactly like the normal ATM except that it asks for the user to be scanned and authenticated. The flowchart of the client component is illustrated below in Fig 5.

The client starts by initializing the program, setting the hardware and making the ATM idle for smart card insertion. When the user inserts a smart card issued by the bank, the user would be asked to momentarily put his/her fingerprint on the scanner. Then, the image captured is reduced to the key feature and compared to

the stored template on the smart card. Hence, this eliminates the use of a central computer. This provides better security since the template does not have to travel through a network from fingerprint scanner to central computer. If the user identity is confirmed, then the user is allowed to make any transaction provided by the ATM.

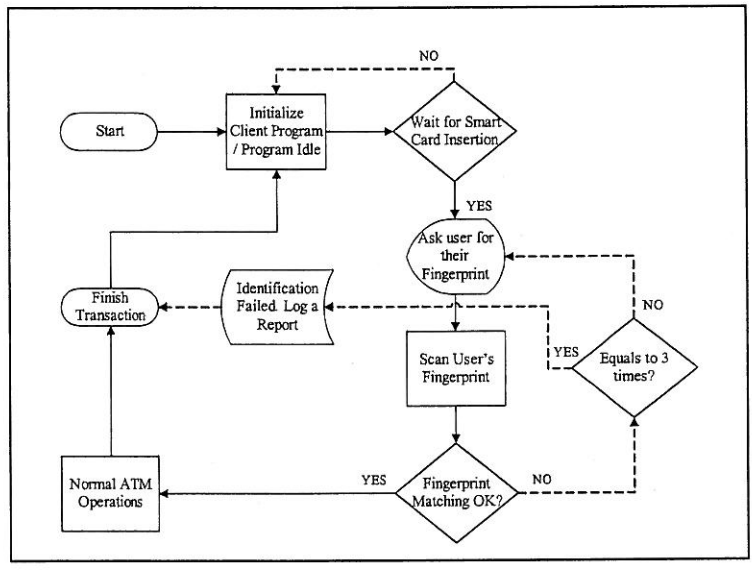

Fig 5: The Client Component Flowchart for User Identification

5.0 CONCLUSION

This study highlights the framework for identification and authentication using smart cards and the fingerprint for ATM system. It shows that the fingerprint is a feasible method for identifying user and smart cards as the reliable token for storing sensitive data. The system improves the vulnerabilities experienced in the PIN or password-based system. This paper suggests two alternatives for today's ATM systems. First, the fingerprint as an alternative for the PIN; secondly, smart card as an alternative for the magnetic-stripe card. Fingerprinting provides a more viable method of identifying users and smart card provides a reliable tamper-proof infrastructure for storing the fingerprint template. The two authorization methods have given a sufficient security level for the ATM systems. The use of human characteristics in our prototype development might tackle a lot of security implementation issues in identification and authentication for the ATM systems. Hence, the vulnerabilities of the ATM would dramatically be reduced in the future.

REFERENCES

American Biometric Company (1999). *Biometric and Smart Card User Authentication*. Discussion Paper.

Bank Negara Malaysia (2000). *Unauthorised ATM Withdrawals*. [On-Line] Available http://www.bnm.gov.my/en/News/releases.asp?yr=2000&sid=0408.

Corcoran, D., Sims, D., & Hillhouse, B., (2000). *Smart Cards and Biometrics: Your Key To PKI*, Retrieved [On-Line] http://noframes.linuxjournal.com/lj-issue49/3013.html.

Ganger, G. R. (2001). *Authentication Confidences*, Technical Report [On-Line] Available http://reports-archive.adm.cs.cmu.edu/anon/2001/abstracts/01-123.html.

Gong, L., Lomas, M. A., Needham, R. M. & Saltzer, J. H. (1993). Protecting Poorly Chosen Secrets From Guessing Attacks. *IEEE Journal on Selected Areas in Communications*, 11(5):648-656.

Gaskell, G. I. (2000). *Integrating Smart Cards into Kerberos*. Master Dissertation, Faculty of Information Technology, Queensland University of Technology.

Hachez, G., Koeune, F. & Quisquater, J.J. (2000). Biometrics, Access Control, Smart Cards: A Not So Simple Combination. In *Proceedings of the fourth working conference on smart card research and advanced applications*, Kluwer Academic Publisher, Norwell, MA, USA: 273-288.

Jain, A. K., Hong, L., Pankanti, S. & Bolle, R. (1997). An Identity Authentication System Using Fingerprints. In *Proceedings of IEEE*. 85(9):1365-1388.

Jain, A. K., Prabhakar, S. & Pankanti, S. (2001). Matching and Classification: A Case Study in Fingerprint Domain. In *Proceeding of Indian National Science Academy (INSA-A)*. 67(2): 67-85.

National Institute of Standards and Technology (NIST), U.S. Department of Commerce (1995). *An Introduction to Computer Security: The NIST Handbook*, Special Publication 800-12.

Rankl, W. & Effing, W. (2000). *Smart Card Handbook*, West Sussex, England: John Wiley and Sons, Ltd.

Omar, M. H., Din, R, & Mohamad Tahir, H. (2001). Smart Card and Fingerprint: An Alternative for User Identification and Authentication. In *Proceeding of National Conference on Research and Development of Public Higher Education Institution.* Pusat Pengurusan Penyelidikan, Universiti Kebangsaan Malaysia: 882 - 886.

Omar, M. H. (2002). *Smart Cards and the Fingerprint: A Proposed Framework for Automatic Teller Machine (ATM) System*, Master Thesis, School of Information Technology, Universiti Utara Malaysia.