Smart Card Security; Technology and Adoption

Hamed Taherdoost hamed.taherdoost@gmail.com
Department of Computer Science
Islamic Azad University, Semnan Branch
Semnan, Iran

Shamsul Sahibuddin shamsul@utm.my
Advanced Informatics School
Universiti Teknologi Malaysia
Kuala Lumpur, Malaysia

Neda Jalaliyoon neda.jalaliyoon@yahoo.com
Department of Management
Islamic Azad University, Semnan Branch
Semnan, Iran

Abstract

Newly, smart card technology are being used in a number of ways around the world, on the other hand, security has become significant in information technology, especially in those application involving data sharing and transactions through the internet. Furthermore, researches in information technology acceptance have identified the security as one of the factor that can influence on smart card adoption. This research is chiefly to study the security principals of smart card and assess the security aspects' affect on smart card technology adoption. In order to achieve this purpose, a survey was conducted among the 640 university students to measure the acceptance of smart card technology from security aspects.

Keywords: Smart Card, Security, Adoption/Acceptance, Satisfaction, Privacy, Non-repudiation, Authentication, Integrity, Verification, Information Technology

1. INTRODUCTION

Smart card is called 'smart' because it contains a computer chip. Indeed, smart card is often referred to as 'chip card' or 'integrated circuit card'. The smart card looks like a credit card but acts like a computer [19]. Without realizing it, smart cards have become a very important part of human's life. Smart cards are secure devices that enable positive user identification and they are multi-functional, cost effective devices that can be easily adapted for both physical and logical access. Logical access control concerns such familiar principles as password checking or the more sophisticated cryptographic mechanisms for authentication such as windows logon, virtual private network (VPN) access, network authentication, biometric storage and others. Physical access control relates to ID badges and building access control. Importantly, smart cards technology includes a wide range of applications and additional physical forms, than just plastic cards.

However smart card are currently used in many other applications such as health and services cards, banking (such as auto-teller machine cards), network authentication, telephone (calling) cards, identification (including government identity cards, employee ID badges and membership cards), telecommunication (mobile phone subscriber identification and administration), transport ticketing and tolling, electronic passports, and physical access control if having a look at the Iranian wallet, you will find; notes, coins, driving license, library card, paper identity card and other cards. As a result of accepting smart card technology, all these documents could be replaced by one card and it can be used for all.

It is important to note that consumer acceptance and confidence are crucial for any further development of smart card technology as the underlying issues [15][4]. Several researches developed theories and models to describe and analyze user acceptance and each of these models determines different factors to explain user acceptance. According to [20][11], security can effect on user satisfaction and consequently on user acceptance of smart card technology. In other words, in order to increase the level of smart card usage and user adoption, the emphasis on factors that can influence on user acceptance should be raised. Therefore, the smart card security principals were studied and additionally, a survey was broadcasted to measure the importance of security in smart card adoption.

2. SECURITY OF SMART CARDS

Smart cards are mostly used in security applications. Smart cards offer much higher security compared to basic printed cards, and even magnetic stripe cards. Smart cards are often used to prove identity, control access to protected areas, or guarantee payments. The reason for high security in smart cards is due to the fact that the users of the system are given access to the smart card. The security element is put into the hands of the users, and is therefore open to attacks from hackers, clever outsiders, malicious insiders, or even dedicated and well funded enemies. The memory technology used in smart cards has an influence on security, both in the card and in the overall system. Some memory technologies have characteristics that make them particularly secure or insecure. Smart cards also include other security measures such as holograms, security overlays, guilloche printing, micro-printing, optically variable printing.

2.1 Smart Card Security Features

Some components that play a role in smart card security:

- Human-readable security features
- Security features of the smart card chip
- Security features of the operating system
- Security features of the network

Human Readable Security Features of Smart Cards

Smart card includes human readable security identifiers. Smartcard falsification is prevented by features. The data in the card do not protected by this features, but abuse of the card as badge identification are prevented by features [8]. See Table 1.

TABLE 1: Smart card human readable security features

Feature	Description
Photo lamination	The smart card is issued with passport sized photograph. This photo is laminated on the smartcard.
Signature strip	Credit card have very familiar feature. For singing smart card indelible ink is used.
Hologram	During production of card the hologram is bonded to card. Hologram can be separated from card only with destroying the substrate.
Micro Printing	It is ultra-fine printing that the naked eyes see it as a line. This print completely appears under the magnification.
Embossing	The number that is pressed on the card. For increasing the security some companies presses the card number over the hologram.
Security Patterns	They are expensive process and known as a guilloche. This print is very fine interwoven line onto the card substrate.
Laser Graver	With using laser, company burn images into the card substrate only when the smart card is issued to the cardholder the burning can be done then the burning is personal.

Security Features of the Smart Card Chip

Testing the microcircuit, during the production, is the necessary act for the smart card chip. After testing the chip, it is converted to a mode. Accessing the internal chip circuit is impossible for this mode. For example outside can't access the memory directly. To prevent attacks execution of some project is necessary. For example with interchange the conductor; deduce the function is impossible for firms. The connections between on-chip elements are encrypted. There are circuits in smart card which can detect external tampering. The circuit detects too high and too low supply, too high or too low external clock frequency and too low an operation temperature.

Security Features of the Card Operating System

Access to smart card files can be protected with a Personal Identification Number (PIN) or with cryptographic keys. PIN protected card access, with fine-grained access controls to data objects so that different areas of memory can be subject to different security rules. Likewise, functions in the card – including those realized using card applications downloaded into multi-programmable smartcards can also be PIN enabled, to help safeguard lost and stolen smartcards against potential abuse.

When a pin isn't entered correctly then after number of attempts, which is setting by issuer of smartcard, the smart card is deactivated. Some issuer of card can reset the smartcard when it is inactive. It depends on designing of smart card [6].

Security Features of the Network

The system design should take into account the accessibility of data in transit and protect it accordingly or design the transport protocol such that tampering will not affect the overall system security. Some actions can physically secure the card terminal. For example, building card terminal into a wall then some equipment such as motorized smart card reader with shutter guaranties the security of card. Placing the smart card reader and communications link in a secured environment can physically protect them.

2.2 Security Principles

There are several reasons one requires security in a smart card system. The principles being enforced are namely; Privacy, Non-repudiation, Authentication, Integrity, Verification.

Smart cards use different encryption algorithms to implement these principles. In some cases a single mechanism can provide a number of security services. For example, a digital signature can provide data integrity with source authentication and non - repudiation. Most of this security needs require key management, which provides the policies and procedures required for establishing secured information exchange, and public key infrastructure (PKI) plays a big role. PKI includes data encryption to ensure confidentiality, digital certificates to provide authentication, and digital signatures to prove the transaction was completed by the originator without intervention or error [7]. In the following sections, we will describe the mechanisms use in smart cards to enforce these principles:

Privacy

The act of ensuring the nondisclosure of data between two parties from third party is privacy. More research on privacy and security is needed before such a card comes into being, since the more personal and varied the information stored on an individual's smart card, the greater the potential for privacy loss when that card is accessed. But even in their current incarnation, smart cards support an impressive variety of applications, and are expected to support more as they become smaller, cheaper and more powerful [18].

Symmetrical cryptography and asymmetrical cryptography are used to assure privacy. Depend on the application of cards, different processes are needed. In spite of many physical resources, implement of multiple algorithms is impossible. Single, standard, algorithm will be used. For symmetric key cryptography this will almost certainly mean DES (FIPS 46-3, [13]) or maybe triple-DES (ANSI X9.17 [3]) and for asymmetric cryptography the typical algorithm of choice will be RSA [17]. In the future there might be moves towards using the AES (FIPS 196, [14]) as a replacement for DES, but this is not likely any time soon.

- Symmetrical Cryptography: For encrypting plain text into enciphered text and decrypting enciphered text back into plain text the symmetrical cryptography uses single key. To encrypt and decrypt the message the same key is used by symmetrical therefore symmetrical cryptography is termed symmetrical. DES is utilizable on smart card software and it is fast algorithm (FIPS 46-3, [13]). The defect of Symmetrical encryption is the both partners need to recognize the key. For securely transferring keys to cardholders, writing a des key at card personalization time is the typical manner. If it is not possible the asymmetrical cryptography, that is explained blow, must be used.

- Asymmetrical Cryptography: In 1976, the idea of splitting the encryption/decryption key instead of sharing a common key was first proposed in an article by W. Diffie and M.E. Hellman entitled "New Directions in Cryptography". This idea has since become known as asymmetrical cryptography. Asymmetrical cryptography uses two keys: one to encrypt the plain text and another to decrypt the enciphered text. The keys are mathematically related. Only messages encrypted with one key can be decrypted with the other key. The best-known asymmetrical cryptographic algorithm is RSA [17].

The credit card companies use asymmetrical cryptography for authentication purpose. It uses rarely to perform the data encryption .also the symmetrical cryptography is used to this aim. For send the des key securely from one partner to another the asymmetrical encryptions is often used. If the Des key is known by both partners transmission of data is symmetrically encrypted. This act improves the performance.

Integrity

Errors and tampering in electronic communications are too many. Cryptographic techniques confirm the correctness of message that transmitted from the original to the recipient this is known as data integrity. In fact Integrity assures that only those authorized can access or modify the information. A data integrity service guarantees the correctness of content of message which we sent [21].

Message Authentication Code: For generate the value one-way cryptographic algorithm is used therefore Mac is unique to that message because it is an 8_byte value generated for a message. A one way cryptographic algorithm cannot be reversed and guaranty the enciphered text always unique then we can say it is special. DES using a key calculates the Mac in smart cards. Both the smartcard and smart card reader share it.

Before the message being sent, the Mac is attached to the end of plain text message. When message is received, the Mac value is calculated and compared by recipient. The Mac changed in an unforeseen way if even one character in the message is changed. The Mac is the assurance for recipient that massage hasn't been tampered. This is necessary that Mac or one of these examples protect the messages which transmitted between smartcard and smart card reader.

Non-Repudiation

Non-repudiation confirms that the origin of data is exchanged in transaction. Certain transaction, that is performed, never could be denied by party. A certain message that sent form a sender could never be denied by receiver. And receiver never can deny this message. Non-repudiation of the transaction is ensured by cryptography.

Digital Signature: For understanding better of this feature we need to plan one example: Bob sent message, which is encrypted, to Alice. For encrypting message, Bob uses Alice's public key, and Alice uses her private key to decrypt the message. With this property Alice can check that bob actually send the message. This is basis for digital signatures [8].

Authentication

Authentication is the process which specifying identity of person. In fact it specifies that someone or something is who or what it is claims to be. For example, before Bob accepts a message from Alice, he wants to be assured that Alice is the owner of key. This needs a process by the name of authentication.

Certificates: Authority issuing the certificate guaranty certificates that the holder of certificate is who she/he pretends to be. If digitally signed message, that include copy of the holders public key and information about certificate holder, is a certificate. Then a person who receiving message assure that key is reliable because the issuing authority signed it.

Verification

Confirming the identity of cardholder is the useful act before using a card. If two parties want to start business they must be assured of identify of another party. For recognizing other parties visual and verbal clues can help us. Encryption technology is used to verify that another person is who to pretend to be.

- PIN Codes: PIN consists of four or five digit numbers this number attaches to smart card. Cardholder memorizes this number. PIN is saved safely. Until accessing from the external world is allowed, data and functions on the smartcard can be protected. This time will took only after the correct pin code is available because of the applications of smart card are too many therefore People are needed to remember more and more pin numbers remember 15_20 different pin codes are difficult for all people and it could causes that somebody write the pin number on the card. It eliminated the benefit of having PIN in the first place that is why recent emphasis on security measures have paid attention to biometric as means of identifying a person.
- Biometrics: Biometric is the technology of measuring personal features. Users are reluctant to memorize passwords and pin numbers. This reluctance is one of the driving forces behind the development of biometric. Also many people can share pin numbers then it is not uniquely but biometrics can specify the real person because it is unique. Some of the biological features that can be measured are:
  - ✓ Signature
  - ✓ Fingerprint
  - ✓ Voiceprint
  - ✓ Hand geometry
  - ✓ Eye retina
  - ✓ Facial recognition

As you can see in Table 2, there is a comparison between several factors of the various traditional and biometric identification methods.

- Mutual Authentication: When smart card put into smartcard reader, they verify to identify each other automatically [8]. For example Bob sends a number to Alice. Alice needs to use DES key to encrypt the number then Alice returns back the enciphered text to Bob. Enciphered text is decrypted by Bob and Bob compares this number with the number that he sent. If they be the same then Bob understands that the same key is shared by Alice [6].

TABLE 2: Compare several factors of the various traditional and biometric identification methods (Source: The IBM Smart Card Development Group)

	Acceptance	Cost of Enrollment	Rejects	Substitution	File Size (Bytes)	Relative Device Cost
PIN	50%	Low	1%	0.1%	1-8	Very cheap
Static Signature	20-90%	Low	5%	1%	1000-2000	Cheap
Static/Ext Signature	20-90%	Low	5%	0.1%	1000-2000	Cheap
Dynamic Signature	20-70%	Medium	1-20%	0.01%	40-1000	Medium
Fingerprint	0-100%	Medium	1-10%	0.1%	300-800	Medium to Expensive
Hand Pattern	0-90%	Medium	5%	1%	10-30	Medium to Expensive
Voice Pattern	100%	Low	10%	1%	100-1000	Cheap
Retinal Pattern	0-10%	High	1%	0.1%	80-1000	Very Expensive

3. PROPOSED MODEL

Based on related literatures review, three main constructs are established in this research, namely Security, Satisfaction and Adoption. Figure 1 shows a research model. But, in this study the focus is on the evaluating measurement models for security construct.

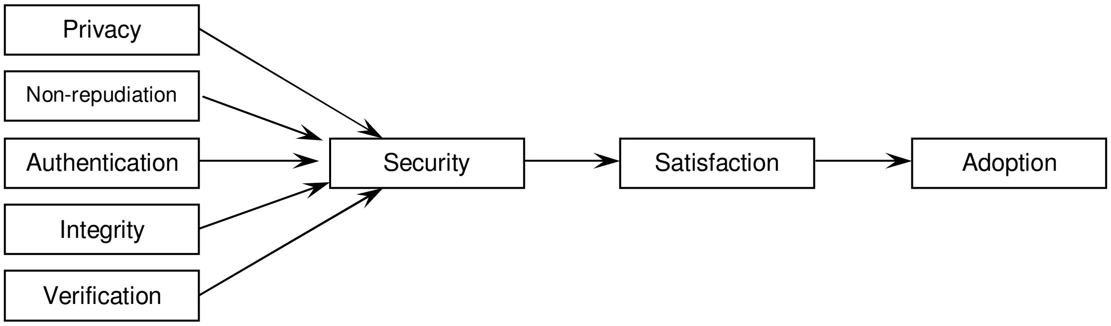

FIGURE 1: Research Model

3.1 Security Dimension

Some studies have reported that users' concern about security has increased and it has been known as one of the most significant factors for technology acceptance. In this study security is defined as "the degree to which a person feels that security is important to them and believes that using smart card is secure" [22]. It has been suggested by [23] that the increase in system security strength would protect the overall quality of the system perceived by users. By protecting the integrity, availability and confidentiality of the content in the system, security controls could help to protect the overall content quality of the system [23].

Content quality is a major determinant of overall information system quality [12], which has a positive effect on individual's perceived ease of use of information systems. Furthermore, [1] found that users' understanding of security issues and awareness of security threats greatly affect their perception of the usefulness of security mechanisms and the overall secured system.

There are several reasons one requires security in a smart card system. The principles being enforced are:

- Privacy: The act of ensuring the nondisclosure of data between two parties from third party.
- Non-repudiation: To confirm the origin of data is exchanged in transaction. Certain transaction, that is performed, never could be denied by party.
- Authentication: The process which specifying identity of person .In fact it specifies that someone or something is who or what it is claims to be.
- Integrity: The correctness of message that transmitted from the original to the recipient.
- Verification: Confirming the identity of cardholder is the useful act before using a card.

3.2 Satisfaction Dimension

Satisfaction of the computer system will have a direct effect on usage [9]. Bailey and Pearson defined satisfaction as ‘‘in a given situation, is the sum of one’s feelings or attitudes towards a variety of factors affecting that situation’’. The measure of computer satisfaction was developed from the comprehensive tool reported by [5].

4. METHODOLOGY

This study collected data samples by conducting online survey aiming at universities’ students as smart card users. Universities’ students were selected because students are usually among the most informed group of people in the society and aware of use of information technology [2]. six hundred and fourty samples were collected. The first section of the instrument assessed demographic characteristics. The second and third parts include twenty five-point Likert scale items ranging from strongly disagree to strongly agree. The questionnaire consists of thirteen measurement items in security section and six measurement items in satisfaction and adoption part. All the nineteen items (security, satisfaction and adoption measures) were used to run factor analysis by SPSS 16.0 for Windows. The value of Cronbach’s alpha (α) is above the 0.7 level and thus satisfies the reliability requirement.

5. RESULTS

Table 3 summarizes the demographic profile and descriptive statistic of the respondents.

TABLE 3: Demographic profile of the respondents

Demographic Variables	Frequency (N)	Percentage (%)
Gender		
Female	342	53.4
Male	298	46.6
Age		
20 and under	188	29.3
20-25	377	58.9
26-30	60	9.4
More than 30	15	2.4
Education		
Diploma	102	15.9
Bachelor Degree	511	79.9
Master Degree	21	3.3
PhD Degree	6	0.9

In the research model, a further satisfaction factor is security. As it is mentioned earlier, security itself has five principals which are privacy, integrity, non-repudiation, verification and authentication. Therefore, in order to measure the level of security in smart card technology and its importance for user acceptance of smart card technology, it is also needed to investigate these five aspects. Thus, in the survey, there are five items to measure the users’ opinion and their expectation about security of smart card technology and some items regarding to the security principals. Table 4 shows the percentage and frequency of the responses. First of all, once respondents were asked whether they trust on the smart card security or not, more than 84% of them cited their agreement while only 7% disagree or strongly disagree with it.

Moreover, in the next question, more than 77% of participants either agree or strongly agree that they are not concern about the security of smart cards whereas just 11% are concerned about it. Again, almost the same percentage recorded for smart card trustworthiness. On the other point of view, 92% of participants agree or strongly agree that security is important when using smart card. And finally, more than three quarters (80.4%) agree or strongly agree that smart card system is secure though 3.6% disagree.

As shown in Table 4, more than three quarters (80.3%) agree or strongly agree that in the smart card the message will be transmitted correctly from the original to the recipient. Additionally, another related question regarding the data integrity in the smart card system was posed and nearly three quarters (73.6%) either agree or strongly agree rather than (8.2%) disagree or strongly disagree that smart card prevents accidental loss of data and data decay. In terms of non-repudiation, more 77% of respondents agree or strongly agree that in smart card if a certain transaction is performed, it never could be denied by party while less than one tenth (8.1%) disagree. From the privacy view, nearly four out of five (79.3%) either agree or strongly agree that their information is well protected. Furthermore, more than three quarters (77.4%) either agree or strongly agree rather than less than one tenth (9.9%) disagree that they trust in the ability of a smart card system to protect their privacy.

TABLE 51: Frequency and percentage of respondents' response to the security section's items

Variables	Questions		Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree
Security	I trust in the technology that smart card system is using.	N	6	39	59	212	327
		%	1	6.2	9.1	33.6	51.0
	I am not worried about the security of smart card system.	N	6	68	89	252	245
		%	1.0	10.8	10.4	39.4	38.4
	Smart card systems are trustworthy.	N	6	14	124	299	196
		%	1.0	2.3	19.4	46.6	30.6
	Security will be important when using smart card.	N	6	6	38	218	365
		%	1.0	1.0	6.1	34.6	57.4
	Overall, the smart card system is secure.	N	12	10	99	271	245
		%	1.9	1.7	15.5	42.4	38.4
Data integrity	I feel that message will be transmitted correctly from the original to the recipient.	N	17	36	73	226	288
		%	2.7	5.6	11.4	35.3	45.0
	I believe that smart card prevents accidental loss of data and data decay.	N	22	30	116	296	174
		%	3.5	4.7	18.2	46.3	27.3
Non-Repudiation	I believe that in smart card if a certain transaction is performed, it never could be denied by party.	N	12	38	90	246	251
		%	2.1	6.0	14.1	38.6	39.2
Privacy	I believe that my information is well protected.	N	6	43	82	328	180
		%	1	6.8	12.9	51.2	28.1
	I trust in the ability of a smart card system to protect my privacy.	N	12	50	80	240	255
		%	2.0	7.9	12.6	37.5	39.9
Verification	I believe that smart card is able to confirm the identity of cardholder before using a card.	N	30	32	64	261	254
		%	4.7	5.0	10.0	40.8	39.5
Confidentiality and Authentication	Access to confidential information is strictly limited by the use of special codes and passwords.	N	43	42	110	213	228
		%	6.9	6.6	17.2	33.5	35.8
	Only authorized individuals are able to access to confidential information.	N	35	28	101	247	225
		%	5.5	4.4	15.9	38.8	35.3

Regarding the verification of smart card technology, once respondents were asked that smart card is able to confirm the identity of cardholder before using a card, approximately four out of five (80.3%) either agree or strongly agree rather than below one out of seven (9.7%) disagree.

At last, nearly 14% of those responding either disagree or strongly disagree that access to confidential information stored in smart card chip is strictly limited by the use of special codes and passwords while almost 70% agree. In addition, another related item to smart card authentication was created that only authorized individuals are able to access to confidential information and more agree (74.1%) than disagree (9.9%).

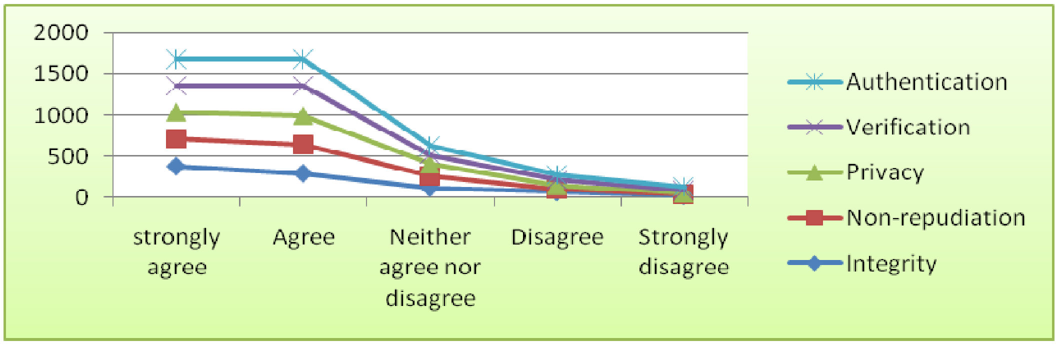

FIGURE 2: Users' opinions about smart card security principals

Figure 2 reveals the users' opinions about smart card security principals. As it is clarified from this Figure, the results in these five principals is to support of the previous question which was about the security of smart card and more than 80% of respondents recognized smart card as a secure device.

Therefore, as it is shown in Table 5, it can be concluded that the correlation between privacy, integrity, non-repudiation, authentication, verification and security is statistically significant. Furthermore, the correlation of all factors on security is positive.

Moreover, Table 6 indicates that there is a positive correlation between the total score of security and satisfaction (correlation coefficient = 0.732). Additionally, as the simple correlation of 0.621 between satisfaction and adoption indicates there is a fairly strong relationship between them. Therefore, it can be concluded that the correlation between security, satisfaction and adoption is statistically significant and positive.

TABLE 5: Correlation between security and security principals

		Security	Integrity	Non-Repudiation	Privacy	Verification	Authentication
Security	Pearson Correlation	1.000					
Integrity	Pearson Correlation	.340**	1.000				
Non- Repudiation	Pearson Correlation	.314**	.408**	1.000			
Privacy	Pearson Correlation	.428**	.363**	.242**	1.000		
Verification	Pearson Correlation	.317**	.222**	.203**	.307**	1.000	
Authentication	Pearson Correlation	.296**	.254**	.290**	.290**	.268**	1.000

**. Correlation is significant at the 0.01 level (2-tailed).

TABLE 7: Correlation between attitude toward use, satisfaction and adoption

		Adoption	Satisfaction	Security
Adoption	Pearson Correlation	1.000		
Satisfaction	Pearson Correlation	.621**	1.000	
Security	Pearson Correlation	.636**	.732**	1.000

**Correlation is significant at the 0.01 level (2-taile).

6. CONCLUSION

In order to use any new system and technology, it is needed that users can trust on it. Therefore, being secure can motivate consumers to accept any fresh technologies and smart card technology as well. Findings of this study demonstrate that most of the students (81.8%) found smart card secure so they trust on the smart card systems. Besides, more than nine out of ten stated that security will be important when using smart card. On the other point of view, anxiety which have a negative effect on the user satisfaction does not have large impact on the users acceptance because most of the users (76.3%) suppose that the messages will be transmitted correctly from the original to the recipient (card and card reader) and also they have faith that smart card prevents accidental loss of data and data decay. Additionally, the majority of the participants believe that smart card with the ability of limiting the access to the confidential information by using the special codes and passwords is able to confirm the identity of cardholder before using a card (verification and authentication).

The results of this study illustrate that security has an important and positive effect on user satisfaction and consequently on user acceptance. It means that with increasing the level of security, the level of user acceptance will be increased. Finally, further investigation needs to be carried out in the future to identify factors that will provide users better understanding of the system and also establish new techniques to increase the security level of the smart card.

7. REFERENCES

[1] Adams, A. and Sasse, M. A. (1999), Users Are Not the Enemy. Why Users Compromise Computer Security Mechanisms And How To Take Remedial Measures. *Communications of the ACM*. 42(12), 42-46.

[2] I. Al-Alawi, & M.A. Al-Amer, “Young Generation Attitudes and Awareness Towards the Implementation of Smart Card in Bahrain: An Exploratory Study”. *Journal of Computer Science,* Vol. 2 No. 5, 2006, pp. 441-446.

[3] American National Standard Institute. (1985). *ANSI X9.17*. Financial institution key management (wholesale).

[4] Argy, P. and Bollen, R. 1999. Australia: raising the e-commerce comfort level. *IT Professional*, 1 (6), 56–57.

[5] Bailey, J. E., and Pearson, S. W. (1983). Development of a Tool For Measuring and Analyzing Computer User Satisfaction, *Management Science.* 29, 530–544.

[6] *Consultation on Australian Government Smartcard Framework*; *Smartcard Implementation Guide. (*2007). Australian government office of the privacy commissioner.

[7] Everett, D. (1993). Smart Card Tutorial, Part 11 The Development Environment. First Published in July 1993.

[8] Ferrari, J., Mackinnon. R., Poh. S., and Yatawara. L. (1998). *Smart Cards: A Case Study.* International Technical Support Organization IBM Corp.

[9] Igbaria, M. and Parasuraman, S. (1989). A path analytic study of individual characteristics, computer anxiety, and attitudes towards microcomputers. *Journal of Management.* 15(3)**,** 373-388.

[10] Leonard, L. N. K., Cronan, T. P., and Kreie, J. (2004). What influences IT ethical behavior intentions, planned behavior, reasoned action, perceived importance, or individual characteristics? *Information and Management*. 42(1), 143-158.

[11] Masrom. M, Ismail.Z, Ahmad. R and Taherdoost. H. (2009). Evaluating Measurement Models For the Acceptance of Smart Card Technology: Security Aspects. *Proceeding of the 3rd*

[12] *International Conference on Informatics and Technology, Kuala Lumpur, Malaysia*.170-175.

[13] Liaw, S.S., and Huang, H. M. (2003). An investigation of user attitudes toward search engines as an information retrieval tool. *Computers in Human Behavior.* 19(6), 751–765.

[14] National Institute of Standards and Technology. (1999). *FIPS 46-3*. The Data Encryption Standard.

[15] National Institute of Standards and Technology. (2000). *FIPS 196*. The Advanced Encryption Standard.

[16] Rankers, P., Connell, L., Collins, T. and Russell, D. 2001. Secure contactless smartcard ASIC with DPA protection, *IEEE Journal of Solid-State Circuits*, 36 (3), 559–565.

[17] Rankl, W. and Effing, W. 2003. Smart Card Handbook, John Wiley.

[18] Rivest, R., Shamir, A., and Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*. 21(2), 120-126.

[19] Shelfer, K., M., and Procaccino, J., D. (2002). Smart card evolution. *Communications of the ACM*. 45(7): 83-88.

[20] T. Kilicli, “*Smart Card HOWTO*,” 2001.

[21] Taherdoost. H, Masrom. M, and Ismail. Z. (2009). Evaluation of Smart Card Acceptance: Security, Technology and Usage. *Conference Proceedings of International Conference on e-Commerce, e-Administration, e-Society, and e-Education (e-case).* Singapore. pp.765-779.

[22] Vandenwauver, M. (1994). introduction to cryptography, Katholieke Universiteit Leuven.

[23] Vijayasarathy, L., R. (2004). Predicting consumer intentions to use online shopping: the case for an augmented technology acceptance model. *Information and Management*. 41(6), 747-762.

[24] Whitman, M., E., and Mattord, H., J. (2003). *Principles of information security*. Boston, MA: Thomson Course Technology.