2.3 Government to Business (G2B)

Public and private sectors are both able to sell their products easily with the help available on e-government. It facilitates the setting up of new businesses, with everything needed to do this being available online.

2.4 Government to Citizens (G2C)

One of the main purposes of e-government is to make it easier for citizens to access government services. It is crucial that all countries encourage their citizens to use the available e-government services because both parties can thus save time and effort.

Fig. 1 shows the four types of e-government services. G2C is the main focus of this paper as the research survey was designed to investigate citizens who are using e-government services and the security challenges that they face.

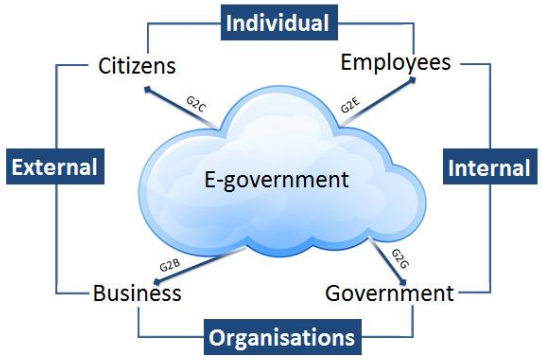

Figure 1. Types of e-government

3. Challenges of e-government

The success of an e-government project depends upon both the government and citizens of a country [2], [6]. The government must provide a high quality IT infrastructure, protect the privacy of its citizens and encourage them to use the available e-government services. However, even if the government fulfils its responsibilities, the e-government project will not be successful if citizens do not accept it and use the services provided. If privacy is not guaranteed, they may be reluctant to use these services [2].

Several studies have indicated the main challenges facing e-government. These challenges include: IT infrastructure; security issues, such as privacy and trust; availability; accessibility; computer literacy; management issues; website design; and lack of awareness. These challenges are summarised in Table I.

3.1 IT infrastructure

Information technology infrastructure refers to the technical components that are used in electronic services, such as hardware, software components and networks, which include both LANs (Local Area Networks) and WANs (Wide Area Networks). The observed challenges are:

3.1.1 Lack of hardware

Hardware components must be updated, and regular maintenance should be scheduled to make sure that the hardware is working effectively. However, the cost of purchasing and maintaining hardware can be an obstacle for some poor countries. The slow speed of the Internet is another obstacle for some countries. One of the main advantages of using e-government is that it saves users' time. However, if Internet speed is slow, this may not be the case, and thus citizens will continue to use traditional methods. Also, the Internet should be easy to access, especially with mobiles or smart devices, with wide coverage being provided. If the Internet is not easily accessible, citizens will be discouraged from using e-government services.

3.1.2 Lack of software

Software and databases that are used in e-government should be designed to cope with large amounts of data, to accept a huge number of access requests and to deal with different types of documents. A database with limitations will not be able to provide high quality services. It has been observed that some e-government services come to a halt when many users are trying to use them at the same time, such as when individuals are applying for scholarships, enquiring about final results and attempting to use services that are based on a first-come first-served basis. In addition, the software must be updated and the database must be backed up regularly.

3.1.3 Lack of system integration

A lack of integration is one of the main challenges when adopting e-government. The heads of department should work together as a team to avoid problems in the future. The design of the systems must also be clear. Furthermore, the communication system must be efficient to avoid any delays in the services.

3.1.4 Lack of data centralisation

Data centralisation plays an important role in the efficient delivery of e-government services to citizens; it can also make integrating the systems of

government departments easier. In addition, when citizens' data is saved in one place, each department will be able to access this data. Conversely, an absence of centralisation will result in each department using its own database. In this case, citizens' data will be duplicated, with each department they are dealing with saving it. The centralisation of data may not be possible in some countries, where this is against human rights. However, the absence or lack of data centralisation will limit the benefits of using e-government.

3.2 Security issues

Security can be defined as the protection of either data or systems from unsanctioned intrusions or outflows. It is one of the main factors that affect the adoption of e-government. Security issues can be either technical or non-technical and can be divided into four main categories, which are:

3.2.1 Information security

The definition of information security is "the subjective probability with which consumers believe that during information transit or storage their personal information will not be viewed, stored or manipulated by inappropriate parties, in a manner consistent with their confident expectations" [7]. Information security strategy is based on confidentiality, integrity and availability; this is called the CIA security triangle [8].

3.2.2 Perceived risk

Received risk is defined as the negative consequences that a customer is worried about when he/she carries out an action, such as making a wrong payment decision [1]. Belanger et al. [9] indicate that users are most worried about the perceived risk of e-services when they apply for a service or share their information. In addition, users with limited ICT skills will be more concerned about the perceived risks.

3.2.3 Privacy

In e-government services, privacy is one of the most crucial concerns of users, many of whom may be wary of their personal information being kept on file [8]. This is likely to have a negative impact on their use of e-government services [1].

3.2.4 Trust

Many research studies have indicated the importance of trust (Trust of the Internet (TOI) and Trust of Government (TOG)) in relation to users' acceptance of new technologies [4]. When their trust is low, users will spend more time on and put more effort into using e-government services. Increasing the levels of trust will allow users to employ e-government services more easily since it will reduce their anxiety while carrying out the procedures. The best way to develop the trust of users is to reduce the risks associated with e-government services.

3.3 Availability

The availability of e-government services 24 hours a day every day is one of the main benefits of e-government. However, sometimes services are unavailable or users cannot access them easily. Many factors may affect the availability of services, such as the system's inability to accept a lot of requests at the same time; this can lead to services working very slowly or even stopping altogether. Also, services can be halted due to several types of attack, such as Denial of Service (DoS).

3.4 Accessibility

E-government must be designed to allow all users to access the services easily, which means taking into consideration people with disabilities. Users must also be encouraged to use the e-government services, and multi channels must be provided to allow users to access them. For example, the government of Qatar provides free wireless Internet to its citizens, which helps them access and use e-government services [3].

3.5 Lack of awareness

According to several studies, lack of awareness is one of the barriers to the usage of e-government. It has been shown that awareness plays an important role in the acceptance of new technologies, and a lack of it inevitably influences potential users of e-government [10]. Governments are responsible for increasing their citizens' awareness and for devising appropriate strategies and plans to this end.

3.6 ICT skills

Citizens require two types of skills to use e-government services: firstly, general skills in using computers, known as computer literacy; and secondly, specific skills related to information security.

3.6.1 Computer literacy

Computer literacy refers to the ability and knowledge that people need to use computers and new technologies. In his study, Odat [6] indicates that there is a lack of IT skills among leaders, employees, citizens and disabled people. This is

considered to be one of the main barriers to the use of e-government.

3.6.2 Background in information security

Citizens who are using e-government services should at least have a general background in information security. Increasing users' knowledge of information security will make them more confident when using e-government services.

3.7 Website design

Suitable website design encourages citizens to use e-government services, and certain important factors, such as usability, accessibility and perceived ease of use, need to be considered when designing the website [1]. Also, the website should contain information security instructions since citizens will not use e-government if security is not guaranteed.

3.8 Culture

Culture plays an important role in the adoption of e-government, with resistance to change being one of the main cultural factors influencing adoption [1], [3]. In addition, religion and the tribal system in some countries are significant factors in the adoption of e-government, as are other cultural issues, such as language and education.

Table 1. Challenges of E-Government Adoption

Challenges	Examples	References
IT infrastructure	• Lack of network capacity and bandwidth • Highly complex current systems • Weakness in the integrated government systems • Software and hardware not updated, especially security applications • Confusing database design that is difficult to integrate	[6], [11], [12]
Security issues	• Lack of user privacy • Citizens of some countries lack of trust in the Internet and their government • Lack of user confidentiality • Lack of protection during the transition process • Users' concerns about perceived risks • Lack of physical security equipment	[1], [6], [13]
Availability	• Services not available when the information is requested • Lack of protection of the services from DoS attack • Services working slowly, making the task unsuccessful	[14], [15]
Accessibility	• Limited access to channels for e-government users • Limited network coverage • Difficulties faced by disabled users when accessing the services	[6]
Lack of awareness	• Users' lack of security awareness • Sharing sensitive information and passwords • Using unauthorised documents and applications	[6], [8]
ICT skills	• Lack of ICT skills among e-government users, including citizens, employees and leaders • Lack of information security background among e-government users	[6], [16]
Website design	• Perceived usefulness • Perceived ease of use • Lack of navigability	[17]
Culture	• Resistance to change • Religious and tribal issues • Issues regarding multiple languages	[3], [18]

A review of the literature reveals limitations in terms of investigating the relationship between these challenges and making e-government services secure. For example, as previously stated, culture is one of the factors that can influence the adoption of e-government. However, little has been done to identify the relationship between culture and e-government security. The same applies in terms of investigating the relationship between user awareness, which is also a major factor in e-government adoption, and e-government security [6]. Thus, there is a need to examine the relationship between these challenges and e-government security. Consequently, this paper conducts a survey that attempts to address this issue, investigating current security challenges.

4. Adoption models

The success of e-government services relies upon user acceptance. Thus, adoption models need to address any issues related to user acceptance. A number of models have previously been used to investigate the acceptance of new technology. The most important of these is UTAUT because it consolidates eight popular models: Theory of Reasoned Action (TRA), Theory of Planned Behavior (TPB), Technology Acceptance Model (TAM), Diffusion of Innovation (DOI), Motivational Model (MM), Social Cognitive Theory (SCT), Model of PC Utilisation (MPCU) and a combined TPB-TAM model. The original data that had been used in each of the eight models was used in the UTAUT model's validation process. Thus, the UTAUT model is able to address 69% of the issues

covered by the other eight. However, it has been postulated that UTAUT does not focus sufficiently enough on security challenges, for example trust [4]. In addition, Alzahrani et al. [3] indicate that UTAUT should address privacy and cultural issues.

The UTAUT is based upon the theory that four core constructs determine user behaviour, as follows:

4.1 Performance expectancy

Performance expectancy is defined as "the degree to which an individual believes that using the system will help him or her to attain gains in job performance". This construct covers the following elements of different models and theories: perceived usefulness, relative advantage, job-fit, outcome expectations and perceived relevance [19].

4.2 Effort Expectancy

Effort expectancy is defined as "the degree of ease associated with the use of the system" [19]. This construct was taken from TPB, TAM, TAM2, TRA, IDT and MPCU. There are two elements to this construct: perceived ease of use and complexity.

4.3 Social Influence

Social influence is defined as "the degree to which an individual perceives that important others believe he or she should use the new system" [19]. This construct was taken from TPB, TAM2 and MPCU and covers the following elements: subjective norm, social factors and image. Venkatesh et al. [15] found that social influence plays an important part in the acceptance of new technology. Users may not use the new technology if their family and friends influence them not to do so.

4.4 Facilitating Conditions

Facilitating conditions are defined as "the degree to which an individual believes that an organisational and technical infrastructure exists to support the use of the system" [19]. This construct was taken from MPCU, IDT and TPB; it also covers perceived behavioural control and compatibility. This construct directly affects usage behaviour, while the others affect behavioural intention.

Use behaviour is affected directly by facilitating conditions and indirectly by performance expectancy, effort expectancy and social influence.

5. E-government security survey

The aim of this survey is to investigate the current security threats facing the end-users of e-government services and to identify the impact of other general challenges associated with e-government security. Most surveys that refer to e-government security focus on the adoption of e-government services. For example, Alshehri and Dew [18] concentrate on the challenges associated with the adoption of e-government services. Their findings indicate that lack of security is the third most serious challenge, with 46.6% of the participants citing it. Thus, this survey focuses on security challenges in particular as well as other factors that influence the security of e-government.

5.1 Survey methodology

This survey consists of 17 main questions, the majority of which are multiple choice. A Likert scale (1-5) is also used, with the responses ranging from "strongly agree" to "strongly disagree". The survey, which is in both Arabic and English, was distributed via the Internet and hosted online by the Centre for Security, Communications and Network Research (CSCAN) at Plymouth University. There are three main sections in this survey. The first section asks for general information about the respondents, such as age, gender, educational background, employment status, information security background and nationality. The second section focuses on the participants' e-government usage, which includes analysing their experience of using e-government services and determining the current challenges. The third section looks at the participants' experience of e-government security. This is the most important section in the survey as it covers the security issues in e-government as well as analysing the respondents' experience of e-government security. The survey starts with a consent question to confirm that the participant is 18 years old or above and to ensure that he/she understands and accepts the conditions of taking part in the survey. The survey was written in the simplest terms possible in order to make it clear and easy for the participants, members of the public with no specialist knowledge, to understand. The survey was tested and reviewed by both academic staff and members of the public to ensure that it was written in an accessible way. It was also approved by the faculty ethics committee.

5.2 Survey findings

312 participants answered the survey in full. However, only 255 of them used e-government services, while 57 did not. Only the participants of those who used e-government services were taken into account. 29% of the participants who did not use e-government services indicated that this was because most government services are not available online, while 11.6% said they did not have faith in e-government security. 73.1% of all the participants were from Saudi Arabia, while 11.2% were from the United Kingdom and 15.7% were from other

countries. Table I shows the profile of the participants who answered the survey in full.

Table 2. Demographic information of the participants

Demographic Variable	Categories	Response Frequency	Percent
Gender	Male	219	70.2
	Female	93	29.8
Age (years)	18-29	166	53.2
	30-39	116	37.2
	40-49	23	7.4
	50-59	7	2.2
	60+	0	0
Country of Resident	Saudi Arabia	228	73.1
	United Kingdom	35	11.2
	Other	49	15.7
Educational Level	Secondary School	58	18.6
	Diploma/ Bachelor	182	58.3
	Master/ Doctorate	69	22.1
	Other	3	1.0
Employment Status	Student	92	29.5
	Government employed	131	42.0
	Private sector employed	47	15.1
	Self-employed	39	12.5
	Other	3	1.0
Information Security Awareness	Basic	206	66.0
	Intermediate	84	26.9
	Advanced	22	7.1

The majority of the participants who used e-government services through the Internet preferred to do so on either a laptop or desktop, as shown in Fig. 2, which means that the focus should be on this communication channel rather than others.

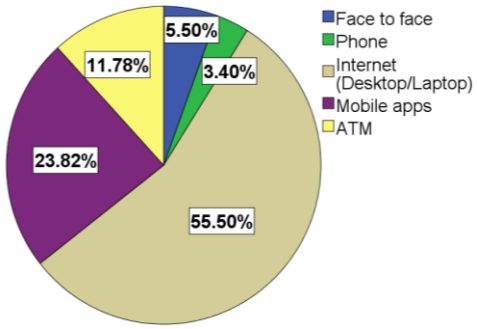

Figure 2. Preferred methods of applying for government services

The majority of the participants were male, with females accounting for only 29.8%. This bias towards males is due to men being more likely to use government services in Saudi culture.

Seven main statements in the survey relate to security challenges. These statements were ranked based on the percentage of participants that either selected agree or strongly agree, as is shown in Table 3.

Table 3. Ranking of statements

Rank	Statement	Agreement
1	Security advice provided to users via the media and e-government websites is very limited.	86.7%
2	User awareness is one of the main factors that affects e-government security.	85.5%
3	Most of the current security issues are non-technical, such as lack of users' awareness and lack of trust.	72.9%
4	Culture and social relationships play an important role in e-government security.	62.4%
5	The website design of e-government services influenced me in determining the level of e-government security.	60.0%
6	I'm worried about my privacy when using e-government services.	49.8%
7	I do not trust the e-government security.	40.8%

The findings indicate that most of the current security challenges associated with the adoption of e-government are of a non-technical nature, such as lack of user awareness, as is shown in Table 4, and thus the main focus should be on these areas.

5.2.1 Security advice statement

The first statement is related to the security advice available in the media and on government websites. 54.1% of the participants who used e-government services strongly agreed that the advice given on government websites and in the media is very scant. In addition, 32.5% of the participants agreed, 1.6% disagreed and only 0.4% strongly disagreed with this. One participant mentioned that most e-government websites do not provide enough security advice while a few of them provide very extensive information regarding security. This participant suggested that more advice should be given but in a simple way. In addition, the participant mentioned that some government websites provide information in order to protect themselves and to make it clear that the user is responsible for using the service, which might deter users from using the service.

5.2.2 User awareness Statement

The second statement is related to user awareness, and it is clear from the participants' responses that the majority agreed that user awareness is one of the main factors affecting the security of e-government. Table 4 shows that 55.7% of the participants who used e-government services strongly agreed and 29.8% agreed with the statement, while only 3.1% disagreed and 1.6% strongly disagreed. User awareness was mentioned many times in the participants' comments, and other comments were made in relation to the awareness of government employees and decision makers in the e-government program. One participant said that most of the current security problems stemmed from a lack of awareness amongst users. Another participant said:

"There is a lack of awareness, not only with users, but also with employees and managers who work in e-government. Awareness needs to be increased for both of them."

This participant also said:

"…There is a lack of information security skills with the programmers who develop the government websites. An information security course must be given for those programmers. Also, a course on information security must be given to university students…"

5.2.3 Non-technical statement

The third statement investigates whether most of the current security threats come from the non-technical side. The participants' responses in Table 4 show that 72.9% agreed that most of the current security threats come from the non-technical side, whereas only 6.7% of the participants disagreed with this.

5.2.4 Culture Statement

The fourth statement is related to culture and social relationships and their impact on e-government security. It is clear from the responses that culture and social relationships strongly influence e-government security. 38.8% of the participants strongly agreed that culture and social relationships play an important role in e-government security. One of the participants mentioned that information about users might be obtained from a friend or relative who works on the e-government program. Clearly, this can threaten the privacy of users.

5.2.5 Website design statement

The fifth statement investigates the relationship between website design and security. Table 4 shows that 60% of the participants agreed that website design influences them in determining the security level of any government website. When the participants' responses were analysed based on their information security background, the results were almost the same. However, a difference was identified after comparing the participants' responses based on nationality. It was found that 37% of the participants from Saudi Arabia agreed with this statement, wheras only 24.1% of the participants from the United Kingdom agreed with it.

5.2.6 Privacy statement

The effect of security challenges is different in developed and less developed countries. The responses of the participants from Saudi Arabia and those from the United Kingdom to a privacy statement revealed that the percentage of participants who disagreed with this statement is similar in both countries, as is shown in Fig. 3 and Fig. 4. However, the participants in Saudi Arabia were more worried about their privacy than those in the United Kingdom. The responses revealed that this is primarily because e-government services in Saudi Arabia are linked to a national ID number, whereas in the United Kingdom they are not. The Saudi participants also mentioned that some of their personal information can be obtained through their national ID number. This ID number can be found on the Internet or in a newspaper, and it can be used in some e-government services to obtain personal information about a user. In addition, it may be easy to obtain the personal information of users via an unscrupulous government employee who has access to an e-service database, as was mentioned by one of the participants. This participant also suggested that there should be an organisation to monitor access to the database to protect the privacy of users and to set policies to track unauthorised access. Governments that use data centralisation are able to provide more services as some e-government services need to be processed by two or more government departments. However, public perception seems to be that data centralisation compromises security, and this may deter them from using the services.

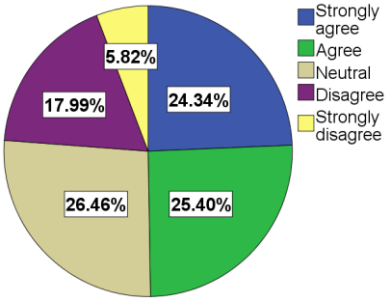

Figure 3. Privacy statement (participants who live in Saudi Arabia)

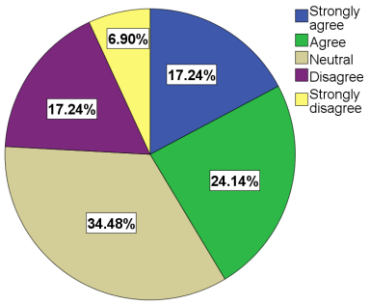

Figure 4. Privacy statement (participants who live in the UK)

5.2.7 Trust Statement

Trust in e-government is based on TOI and TOG, as mentioned above. With regard to TOI, a participant evaluated the security of e-government by

the number of successful attacks that e-government services had been subjected to:

"*The security in e-government is very weak and the large number of successful attacks is strong evidence."*

Other comments similar to the one above were also made. However, one participant mentioned that he did not trust the security of e-government, not because of a lack of security but because he was confident that hackers could break into any system, which led him to avoid carrying out any financial transactions over the Internet.

TOG clearly plays an important role in e-government. A participant said:

"I'm sure that my information and details in the e-government will be used against me when I face problems with the government"

Table 4 summarises the participants' responses to the seven statements.

Table 4: Participants' responses to the seven statements

Statement	1	2	3	4	5
Security advice	0.4	1.6	11.4	32.5	54.1
Users' awareness	1.6	3.1	9.8	29.8	55.7
Non-technical	1.2	5.5	20.4	38.4	34.5
Culture	3.5	15.3	18.8	23.5	38.8
Website design	3.9	11.8	24.3	35.7	24.3
Privacy	5.1	18.4	26.7	26.3	23.5
Trust	5.9	24.3	29.0	22.4	18.4
Please note: 1 Strongly disagree, 5 Strongly agree					

6. Conclusion and future work

The main purpose of this paper has been to investigate the current security challenges encountered in the adoption of e-government. A set of challenges was identified through a review of the literature, and their relevant significance was investigated by conducting a survey. The survey findings confirmed that security plays an important role in the adoption of e-government, and hence, an e-government adoption model would need to take this into account. They also revealed that non-technical issues are particularly important among security concerns about e-government. As such, it is important for future research to consider these challenges and incorporate them into an e-government adoption model. Due to its popularity and relevance to e-government, the UTAUT model would be the preferred choice as the basis for the future proposed e-government model.

7. Acknowledgements

The authors would like to acknowledge King Abdulaziz City for Science and Technology (KACST) for funding this research.

8. References

[1] Alateyah, S., Crowder, R. M. and Wills, G. B. (2012) "Citizen adoption of E-government services", *Information Society (i-Society), 2012 International Conference on*. IEEE, pp. 182-187.

[2] Sang, S., Lee, J.-D. and Lee, J. (2009) "E-Government challenges in least developed countries (LDCs): a case of Cambodia", *Advanced Communication Technology, 2009. ICACT 2009. 11th International Conference on*. IEEE, pp. 2169-2175.

[3] Alzahrani, M. and Goodwin, R. (2012) "Towards a UTAUT-based Model for the Study of E-Government Citizen Acceptance in Saudi Arabia", *Proceedings of World Academy of Science, Engineering and Technology*. World Academy of Science, Engineering and Technology.

[4] Al-Sobhi, F., Weerakkody, V. and El-Haddadeh, R. (2011) "The relative importance of intermediaries in egovernment adoption: A study of Saudi Arabia", *Electronic Government.* Springer, pp 62-74.

[5] Yanqing, G. (2010) "E-Government: Definition, Goals, Benefits and Risks", *2010 International Conference on Management and Service Science*. pp. 1-4.

[6] Odat, A. M. (2012) "E-Government in developing countries: Framework of challenges and opportunities", *Internet Technology And Secured Transactions, 2012 International Conference for*. IEEE, pp. 578-582.

[7] Chellappa, R. K. and Pavlou, P. A. (2002) "Perceived information security, financial liability and consumer trust in electronic commerce transactions", *Logistics Information Management*, 15 (5/6). pp 358-368.

[8] Syamsuddin, I. and Hwang, J. (2010) "A new fuzzy MCDM framework to evaluate e-government security strategy", *Application of Information and Communication Technologies (AICT), 2010 4th International Conference on*. IEEE, pp. 1-5.

[9] Belanger, F., Hiller, J. S. and Smith, W. J. (2002) "Trustworthiness in electronic commerce: the role of privacy, security, and site attributes", *The Journal of Strategic Information Systems*, 11 (3). pp 245-270.

[10] AlAwadhi, S. and Morris, A. (2009) "Factors influencing the adoption of e-government services", *Journal of Software*, 4 (6). pp 584-590.

[11] Ebrahim, Z. and Irani, Z. (2005) "E-government adoption: architecture and barriers", *Business Process Management Journal*, 11 (5). pp 589-611.

[12] Alateyah, S., Crowder, R. M. and Wills, G. B. (2013) "Identified Factors Affecting the Citizen's Intention to Adopt E-government in Saudi Arabia", *International Journal of Social Science and Engineering*, 7 (8). pp 886-894.

[13] Zhang, W. (2010) "E-government information security: Challenges and recommendations", *Computer Application and System Modeling (ICCASM), 2010 International Conference on*. IEEE, pp. V15-11-V15-14.

[14] Khan, F., Khan, S. & Zhang, B. (2010) 'E-Government Challenges in Developing Countries: A Case Study of Pakistan', *Management of e-Commerce and e-Government (ICMeCG), 2010 Fourth International Conference on*. IEEE, pp. 200-203.

[15] Zulhuda, S. (2012) "The state of e-government security in Malaysia: reassessing the legal and regulatory framework on the threat of information theft", *1st Taibah University International Conference on Computing and Information Technology (ICCIT 2012)*, pp. 812-817.

[16] Hwang, M.-S., Li, C.-T., Shen, J.-J. and Chu, Y.-P. (2004) "Challenges in e-government and security of information", *Information & Security*, 15 (1). pp 9-20.

[17] Rehman, M. and Esichaikul, V. (2011) "Factors influencing the adoption of e-government in Pakistan", *E-Business and E-Government (ICEE), 2011 International Conference on*. IEEE, pp. 1-4.

[18] Alshehri, M. and Drew, S. (2010) "Challenges of e-Government Services Adoption in Saudi Arabia from an e-ready citizen Perspective", *World Academy of Science, Engineering and Technology*, International Science Index 42, 4(6), pp. 834 - 840.

[19] Venkatesh, V., Morris, M. G., Davis, G. B. and Davis, F. D. (2003) "User acceptance of information technology: Toward a unified view", *MIS quarterly*, pp 425-478.

