Evaluation of the UTAUT Model for Acceptable User Experiences in e-Government Physical and Virtual Identity Access Management Systems

Sara Jeza Alotaibi
Web and Internet Science, ECS
University of Southampton
Southampton, UK
sja2g09@soton.ac.uk

Dr. Mike Wald
Web and Internet Science, ECS
University of Southampton
Southampton, UK
mw@soton.ac.uk

***Abstract*—The modern world is populated with a great many physical and virtual IAMS (Identity Access Management Systems), where people need to maintain various login credentials. There is a key issue associated with this approach, which is the ability to remember this information; however, this can be circumvented to some degree through utilising an innovative approach of a single sign-in mechanism. Throughout the course of recent times, a number of different systems have been developed in order to deliver both virtual and physical IAMS. Moreover, in addition to a greater level of awareness to ensure interoperable virtual and physical IAMS are implemented, there is a pressing urgency for clear guidelines to be devised relating to the integration of: security, comprising identity; user experience, involving usability; and acceptability, encompassing accessibility. Very few models adhere to such guidelines; therefore, this paper seeks to deal with the pressing need to devise, implement and evaluate a model for acceptable user experience, enabling the successful integration of physical and virtual public services in an e-government context. In regard to the users' assessment, which tests the suggested Unified Theory of Acceptance and Use of Technology (UTAUT), it was observed that there is an indirect impact on behavioural intention to utilise a new prototype system (Ubiquitous Identity Access Management System "UbIAMS") through various factors, namely effort expectancy, performance expectancy and social influence, as well as through items relating to acceptability and user experience.**

Keywords- IAMS; UbIAMS; UTAUT; Security; User Experience; Acceptability; Performance Expectancy (PE); Effort Expectancy (EE) ; Social Influence (SI)

I. INTRODUCTION

The increase in system level integration [1], corporate network linking [2] and the provision of real-time business applications [3] are key components that drive the corporate organisational performance in a virtual environment. In order to achieve this level of business process efficiency, it is vital that the right access is provided to the right people at the right time [4]. In order to promote this level of access management, it is vital that the identity and role of people within an organisation is recorded and controlled in order to avoid entry by unauthorised personnel. Extant literature [5-6-7] documents the movement of business models from closed to open, wherein adoption of web enabled technologies, Internet and federated networks is the norm. This leads to the development of complexities when dealing with multiple users and providing access to the system. There may be a resultant increase in risks owing to the associated threats of open environments [8]. The adoption of identity management systems will help in converging business processes and technologies in a manner that promotes the security, trust and accessibility of identity systems.

An extensive literature review has been conducted with the aim of studying the existing systems that address identity management in both physical and virtual spaces. The study has revealed that many countries, such as those within Europe [9] and the Middle East [10], have taken the initiative of providing citizens with convenience and greater security measures through the introduction of different identity tokens, such as smart cards, biometrics, PINs and passwords, etc., in physical and virtual spaces identity management. Gemalto published a research paper highlighting the efforts of the Belgian government to introduce smart cards and PIN as the authentication mechanism of individuals in both physical and virtual spaces [11]. Their systems provide access to only a few specific government agencies and internet services.

The Austrian government has implemented the concept of integrated authentication systems in a most innovative way; the mandatory presence of a specific identity token has been eliminated from their systems [12]. Any mobile device or smart card—such as health insurance card or bank card, for example—can be used to serve as a Citizen Card that can provide access; however, the integration of the physical and virtual spaces is not mentioned in their systems. Al-Khouri discusses the endeavours witnessed in the UAE; the authentication mechanism has been incorporated with digital certificates of Public Key Infrastructure (PKI) capabilities [13]. The individuals are identified on the basis of their fingerprints and palm prints, with identity management systems deployed for very few government agencies and the online spaces of users. After conducting a thorough study of the available interoperable authentication systems explained in the previous papers [14-15], no system has been found through research activities that would successfully address the specific needs of the customers in such a way so as to make the user experience acceptable. With this in mind, this paper shall focus mainly on

acceptability (which includes accessibility, user experience involving usability) and security (containing identity), since the existing models are most lacking in addressing these individual elements.

This paper is organised in the following manner: firstly, the background of the proposed UTAUT model is explained in *Section 2*; *Section 3* disuses evaluation of the UTAUT model; *Section 4* disuses the data analysis; finally, *Section 5* ends the paper with a summary and suggestions for future work.

II. Proposed Conceptual UTAUT Model

The success of any technology is may be reflected by the number of good reviews or great revenue, but is also dependent on the factors that can help one comprehend the level of acceptance that can be expected from any technology. While many studies have utilised the technology acceptance models in investigating the adoption of various systems in different contexts, very few have utilised the UTAUT model. This research utilises the UTAUT model nd proposes an extension to the model. Extensive investigation on the research study has resulted in three dimensions that are security, which includes identity, user experience, comprising usability and acceptability, containing accessibility.

A. Research Model and Hypothesis Development

It is observed that the unified theory model combines the main features proposed by the eight acceptance theories and models, which were discussed in previous papers [15-16], and the UTAUT model identifies four main aspects which are directly related to the intention of a user. It is observed that these include performance expectancy, effort expectancy, social expectancy and the required facilitation. All of these factors are found to be identified as direct antecedents of the information system related behaviour of a user [17]. The demographics of the user, including age, gender, level of experience and willingness to use (voluntarism), are also taken into account by this theory [17]. There are three distinct features associated with this model: determinants, modifiers and results. The end result that the model aimed to ascertain is the user behaviour. Some demographics were identified to be modifiers, including age, gender and experience. Another factor which acted as a key modifier is the voluntariness of use. The three main determinants impacting the behavioural intention of individuals are performance expectancy, effort and expectation. Apart from those, facilitating conditions was a determinant which directly impacted user behaviour.

The adoption of UTAUT model in the context of IAMS will enable managers of security and identity management systems to weigh the introduction of new technology in different backgrounds and explain the behaviour of the user in relation to the acceptance of information technology [16]. Alotaibi and Wald stated that the intention to use the new prototype IAMS system (UbIAMS) may be influenced by performance expectancy, effort expectancy, social influence, and security and identity. Moreover, it may also be further stated that a strong intention to use any system is eventually translated into actual usage of the system [16].

While this study focuses only on performance expectancy, effort expectancy, social influence, and security and identity factors, a number of other aspects should be further investigated. Likewise, further work should be conducted if there are differences recognised amongst users concerning education, languages, culture, occupation, and income, all of which may affect the adoption of UbIAMS system. Fig. 1 shows the hypotheses to be used to test the system. The grey shaded boxes are not included in the current research study.

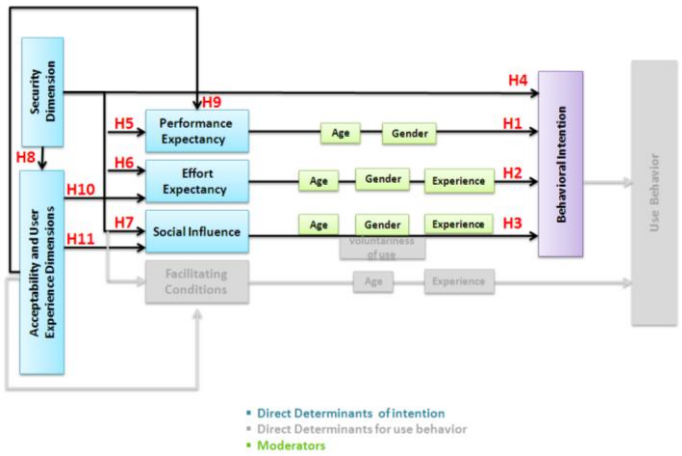

Figure 1. Hypothesis that used to test UbIAMS system [16]

The list of hypotheses that have been selected for the research study under discussion:

- H1: There would be a significant positive relationship between performance expectancy and behavioural intentions to use UbIAMS.
- H1a: There would be a significant positive relationship between performance expectancy and behavioural intentions to use UbIAMS, and this relationship would be moderated by gender and age.
- H2: There would be a significant positive relationship between effort expectancy and behavioural intentions to use UbIAMS.
- H2a: There would be a significant positive relationship between effort expectancy and behavioural intentions to use UbIAMS, and this relationship would be moderated by gender, age and internet experience.
- H3: There would be a significant positive relationship between social influence and behavioural intentions to use UbIAMS.
- H3a: There would be a significant positive relationship between social influence and behavioural intentions to use UbIAMS, and this relationship would be moderated by gender, age and internet experience.
- H4: There would be a significant positive relationship between security and identity items and behavioural intentions to use UbIAMS.
- H5: Security and identity items will have an indirect effect on behavioural intentions to use UbIAMS through performance expectancy.
- H6: Security and identity items will have an indirect effect on behavioural intentions to use UbIAMS through effort expectancy.
- H7: Security and identity items will have an indirect effect on behavioural intentions to use UbIAMS through social influence.
- H8: Security and identity items will have an indirect effect on behavioural intentions to use UbIAMS through acceptability and user experience items.
- H9: Acceptability and user experience items will have an indirect effect on behavioural intentions to use UbIAMS through performance expectancy.
- H10: Acceptability and user experience items will have an indirect effect on behavioural intentions to use UbIAMS through effort expectancy.
- H11: Acceptability and user experience items will have an indirect effect on behavioural intentions to use UbIAMS through social influence.

III. Evaluation of the UTAUT Model

This section describes the approaches adopted in order to assess and examine the suggested model, Unified Theory of

Acceptance and Use of Technology (UTAUT) [16]. As detailed below, the user assessment approach comprises five phases.

A. The Development and Designing of a Prototype System (UbIAMS) and the Five Scenarios

The previous papers explained the models that form the basis of the development of UbIAMS [14-15-16-29]. The addition of the word 'ubiquitous' has transformed the conventional concept of being constrained in one place to being available in different spaces; this introduction enhances the application to physical, as well as virtual, spaces.

The relevance of a prototype in the development of a system cannot be overestimated. It bears even greater relevance when the concept of the system is innovative and has not been explored before. The premise of UbIAMS is innovative; therefore, the development of its prototype was achieved through extensive analysis of the features that should be included within it[1].

The development of the scenarios has been achieved by analysing the basic steps of the operations to be undertaken by any user in order to evaluate the extent of the functionality of the system. The scenarios have been designed after considering the level of computer skills, experience and age range of different types of user.

- Scenario 1: The first scenario is centred on creating a new account in which login credentials, preferred authentication tools and other information are registered in the system.
- Scenario 2: This scenario involves the usage of the USB that possesses the synced ID; this is used as the authentication tool in the system. Banking services are used in this scenario.
- Scenario 3: This scenario involves the use of government services by demanding the presentation of the biometric features of the user. The user has a number of options from which to choose in terms of biometric authentication.
- Scenario 4: The fourth scenario involves making changes in the personal settings of the user to protect his personal information and accordingly to enhance the level of privacy from any undesired source. Changes may also be made to alter the settings for font type, colour schemes, languages, etc.
- Scenario 5: This scenario involves the usage of the system on an alternate technology and platform for the analysis of the level of compatibility with multiple environments.

B. Questionnaire Development and Design

Sekaran & Bougie stated that the initial step in the measurement of the construct is to define the premise and scope of the construct that is desired to be measured [18]. Al-Qeisi also attempted to explain the difference between construct and variable, and highlighted that measurement is the only factor to be used to distinguish between them [19]. Al-Qeisi [19] quoted Sekaran & Bougie [18] and explained that the presence of an actual measure changes the construct into a variable.

Constructs and statements relevant to the research were adopted from Venkatesh *et al.* [17], with new statements related to new variables added by the researcher to provide better clarity. All the statements were evaluated using a five-point Likert scale ranging from 1 ('strongly disagree') through to 5 ('strongly agree') .

The study tool design comprised three pages and a covering letter; this documentation provided insight into the aim behind the research, as well as the researcher's and supervisor's contact details. In total, there were four parts included in the measuring instrument: the first two parts were centred on demographic data; the third part considered the computer- and internet-related knowledge and experience of users; the final part considered the empirical measurements for the suggested model's constructs. The questionnaires in English and Arabic versions were published online[2].

C. Questionnaire, Prototype System and Five Scenarios Pre-Testing (Informal Pilot Study)

There was the selection of eight lay experts [20]; all of the subjects were the University of Southampton's Electronics and Computer Science School researchers or were postgraduates from the same institution, and all had experience in one of the study areas. The sample comprised three men and five women aged 20–50 years. Fundamentally, the subjects were recruited in consideration of their interest in the study.

This stage was adopted in order to gather insights and suggestions from lay experts in regard to the design of the questionnaire, as well as to ensure those conducting the assessment were well positioned to understand the individual scenarios, the instrument and the prototype system. During individual meetings with each lay expert, various suggestions were made in terms of which questions should be removed and how statements could be changed in terms of their phrasing. Following the gathering of feedback and the subsequent implementation of the necessary amendments, sixty questions were formulated for the questionnaire.

With regard to correct terminology use, the Arabic version of the questionnaire was checked and validated by Arabic PhD students. The final version of the questionnaire was compared and contrasted with the first in order to confirm translation validity. Following the finalisation of the translation, there was the conduction of a field test in order to ensure comprehension of all questions by the sample.

D. Solicit User Participation

Following the completion of an assessment using the lay experts, participants were identified in terms of age, experience and gender. They were contacted and their involvement requested two weeks prior to the research start date; this facilitated adequate time for individuals to deal with the request. The research targets only Saudi citizens utilising both virtual and physical public service.

E. Obtain Evidence and Conduct the Results

Subjects were not required to provide personal data or authentication instruments as they were going to complete the five scenarios that would provide all necessary data. Importantly, all data would be kept in the strictest of confidence. Furthermore, following the analysis of the answers and the evaluation of the model, all data would be destroyed.

[1] The prototype system is available at<http://ubiams.wordpress.com/>.

[2] https://qtrial.qualtrics.com/SE/?SID=SV_7VVL6fg0RLstqPr

This research achieved the approval of the Ethics Committee at the University of Southampton.

Before the research was carried out, participation was sought via email invitation, through which subjects were asked to be involved in the study. The sample was advised that all data given would be kept confidential, and that their involvement was entirely voluntary. The research was also recognised as being continuous for a two-month period.

IV. Data Analysis

The results are organised in the following way. The first section is a statistical analysis of the participants who took part in the survey. This is followed by results of the survey analysed with AMOS v20 and SPSS, evaluating the relationships between variables in the conceptual UTAUT-based model for integrating physical and virtual IAMS. This is then related to the testing of the hypotheses. Finally, how well the model fits is addressed by examining the indices tables generated from this analysis.

A. Sample Size

In research methodologies such as this, where survey research designs are used, the formation of a sample size is always an instrumental and important aspect of the study when it comes to the primary data collection procedure. Generally, there are two schools of thought: the first argues that the most appropriate number of people in the sample size should be proportional to the number of people in the population, and that the sample size should always be 20% or more of the population [21]; the other , which will be used in the case of this study, recommends that a generalised target of one hundred (100) respondents or more in the sample size is appropriate to achieve credible results. One researcher who agrees with the latter line of argument is Hair *et al.* [22] who wrote that it is 'generally accepted that the minimum sample size to ensure appropriate use of Maximum Likelihood Estimate is 100' . 253 respondents were used by the researcher for this study, which is a highly accepted value.

B. Computing Reliability of a Questionnaire

In research surveys and primary data collection exercises such as this one, reliability generally refers to the consistency of measure [23]. In modern studies, the use of Cronbach's Alpha has been accepted as a credible means of measuring the reliability of questionnaires. From the Cronbach's Alpha, the general score achieved must be closer to 1.00 and in the range of 0.70 to 0.95 in order to achieve acceptable reliability of the questionnaire. Meanwhile, owing to the compact nature of scales given in the questionnaire and the evenness of number of questions under each variable, the coefficient recorded was 0.7, meaning the researcher achieved reliability of questionnaire.

C. Calculate Frequencies and Percentages

Although there has been a general acceptability of the sample size used by the researcher (because the sample size is 253, which is far above the accepted size of 100), there still remains a lot more for the researcher to do in terms of ensuring that internal validity is totally justified. One such need is to ensure that there is evenness in the demographic characteristics of the respondents. It is recognised that 64.82% of respondents were females whilst 35.18% were males. Indeed, this is a biased representation in terms of gender. This is because, taking the average scale as 50%, it is expected that the range of differential between the two scales, given as males and females, will not be more than 5%. However, on this occasion, the difference is up to 29.64%, meaning the line of responses could be biased towards or against one gender. As far as the age range is concerned, it can be said that a very fair distribution of results was achieved. This is because the modal age range of 30–39 years is also the median age range. In terms of respondents' usage of the internet, responses received are highly favourable for effective academic and conceptual contribution to the study. This point is made against the backdrop that all respondents were internet users and, of the numbers, the modal score was those who had used internet for more than two years. Because the research problem is based on information and communication technology and, for that matter, internet knowledge, this demographic provision could not be overlooked.

In terms of the six major variables set and the various questions and data received on them, a very interesting trend of results was noticed, as shown in Table I since the interpretive attitudes were that respondents generally agreed with most questions.

TABLE I. DESCRIPTIVE STATISTICS OF UTAUT-BASED MODEL VARIABLES

	No. of items	N	Mean	Attitude
Security and identity	23 items	253	3.347	Neither agree or disagree
UX and acceptability	16 items	253	3.399	Agree
Performance expectancy	5 items	253	3.635	Agree
Effort expectancy	5 items	253	3.502	Agree
Social influences	1 items	253	3.375	Neither agree nor disagree
Behavioural intention	1 items	253	3.360	Neither agree nor disagree

D. The Output Generated from AMOS Based on the Survey

Fig.2 shows the output generated from AMOS based on the survey of 253 samples. The parameters generated in the following figure were estimated using the Maximum Likelihood method. This method was chosen over Generalised Least Squares because Maximum Likelihood attempts to maximise the probability of getting the data for covariance or correlation matrix [24].

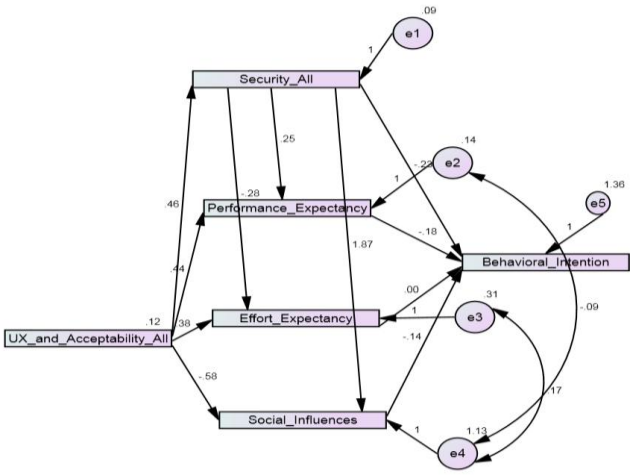

Figure 2. Standardised output estimates for UTAUT-based model

From the output of estimates detailed by the researcher, it can be noted that there was a connection between e2 and e4 as literature shows that performance expectancy is highly related and, for that matter, dependent on, social influence [25]. For example, in systems where the social influence is lower in the sense that the people around the implementer do not seem to welcome the usage of the system, the chances are that the system will not be used at all; once the system is abandoned, its efficacy (performance expectancy) in terms of solving basic problems within the setting in which it is found cannot be appreciated. There was also a link between e3 and e4 owing to what literature says in support of effort expectancy and social influence as being related to and dependent on each other. In a study conducted recently [26], it was deduced that, because effort expectancy directly relates to how an individual acquires necessary skills and knowledge towards the application of the system, if there is no social acceptance, and thus lower social influence, the personalised effort to work around the system will be absent .

E. Analysis of indices

In statistical considerations such as this, where there are comparative variables to investigate, it is always important to undertake a variance test to establish how perfectly the comparisons made between the various variables match [27]. It is for this reason that the analysis of index has been carried out. As can be seen from Table II, the goodness of fit index will be taken as the basis of evaluation since all the remaining indices are derived from it. From this basis, it will be stated that the produced score of > 0.95 represents a good fit of variables as the average fit for a model to be accepted is 0.8 [28]. This is in line with this that the chi-square also produced (p = 0.510), which is a representation of a good fit model. Chi-square compares the default model and the independence model with the saturated model. The $\chi 2$ (chi-square) or CMIN = 1.346 in Table II shows that the UTAUT-based model (default model) is far closer to the saturated model than the independence model. It is statistically significant at p = 0.510, which is small. This result shows that this model still has 2 degrees of freedom (DoF) and with CMIN/DoF = .673, it demonstrates that no other path can be dropped in the UTAUT-based model in order to make it a closer fit.

TABLE II. MODEL FIT INDICES: CMIN

Model	NPAR	CMIN	DF	P	CMIN/DF
Default model	19	1.346	2	.510	.673
Saturated model[1]	21	.000	0		
Independence model[2]	6	250.220	15	.000	16.681

F. Significant Paths for the Regression and Covariance Data

Table III identifies the significant path, the critical ratio and the significance of path coefficients. When the critical ratio (CR) is outside the interval ±1.96 for a regression weight, that path is significant at the .05 level or better (that is, its estimated path parameter is significant). In the p-value column, three asterisks (***) indicate significance smaller than .001. SE is standard error and p the probability.

TABLE III. SIGNIFICANT PATHS FOR THE REGRESSION AND COVARIANCE DATA

	Regression/ Covariance			Estimate	S.E.	C.R.	P	Label	Significant Path
Covariance	SID	<--	UXA	.455	.055	8.269	***	H8	√
	PE	<--	UXA	.443	.077	5.760	***	H9	√
	EE	<--	UXA	.380	.115	3.290	.001	H10	√
	SI	<--	UXA	-.579	.219	-2.644	.008	H11	√
Regression	PE	<--	SID	.252	.078	3.227	.001	H5	√
	EE	<--	SID	-.276	.117	-2.355	.019	H6	√
	SI	<--	SID	1.867	.222	8.407	***	H7	√
	BI	<--	SID	-.233	.275	-.845	.398	H4	
	BI	<--	PE	-.182	.194	-.937	.349	H1	
	BI	<--	EE	-.005	.134	-.035	.972	H2	
	BI	<--	SI	-.144	.074	-1.951	.051	H3	

Detailed analysis of Table III identified a number of statistically significant paths within the model, shown in Fig. 3 with solid lines.

- UX and Acceptability (UXA) and Security and Identity (SID) are strongly correlated (significance smaller than .001).
- UX and Acceptability (UXA) and Social Influences (SI) are strongly correlated.
- UX and Acceptability (UXA) and Effort Expectancy (EE) are strongly correlated.
- UX and Acceptability (UXA) and Performance Expectancy (PE) are strongly correlated (significance smaller than .001).
- Security and Identity (SID) to Performance Expectancy (PE) is significant.
- Security and Identity (SID) to Effort Expectancy (EE) is significant.
- Security and Identity (SID) to Social Influences (SI) is significant (significance smaller than .001).

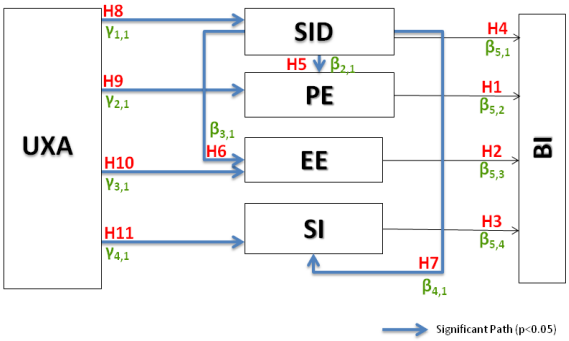

Figure 3. UTAUT-based model showing the statistically significant path

Fig. 3 shows a model that leads up to the statistical hypothesis. Generally, the figure shows the six major variables and how they relate to one another in terms of the hypotheses set out for the study. The arrows used show the numerous variables that have any relations and the kind of hypothesis that can be constructed between them. All in all, there will be eleven major hypotheses arising from eleven major connections. It must be stated, however, that the values of regression coefficient for the various connections forming the hypothesis show that there are stronger hypothetical bases and weaker ones.

The major basis for proving and disproving the hypotheses was the significant path examined using regression and covariance data as explained in Table III. The first four hypotheses were not proved, whilst the remaining hypotheses were proved.

V. Conclusion and Future Work

The future of identity access management systems is strongly dependent on the providers and architects of these systems in order to keep up the demands of the public and address the needs of a new generation user. It was established by Alotaibi *et al*. [29] that no single sign-in service could be used across all federated access management systems, thus requiring the user to create different accounts. Through the current research, it has been established that there is a need for an ubiquitous system. UbIAMS System not only offers a single sign-in on all Federated Access Management system (FAMS), but can also cater to all different needs of users, such as needs to personalise the service with respect to language, culture, disabilities, trust, or privacy etc., thereby establishing the need for future research in this area, as shown in detail [29].

Based on the new UTAUT, the items related to security and identity would have an indirect effect on behavioural intentions to use UbIAMS through performance expectancy, effort expectancy, social influence, and through items pertaining to acceptability and user experience. Moreover, in relation to acceptability and user experiences, it was recognized that their items would also have an indirect effect on behavioural intentions, specifically to use UbIAMS through performance expectancy, through effort expectancy and through social influence.

The final conclusion of this research is that the new UTAUT model helps achieve some appreciation of the solutions in this particular area, such as through the UbIAMS, which is expected to attract the attention of many government organisations to improve security, acceptability and user experience.

References

[1] Gaedke, M., Meinecke, J., & Nussbaumer, M. (2005, May). A modeling approach to federated identity and access management. In Special interest tracks and posters of the 14th international conference on World Wide Web(pp. 1156-1157). ACM.

[2] McQuaide, B. (2003). Identity and Access Management. Information Systems Control Journal, 4, 35-38.

[3] Moeller, R. (2010). Identity and Access Management. IT Audit, Control, and Security, 472-485.

[4] Cser, A., Nagel, B., Balaouras, S., & Hayes, N. M. (2010). Identity and Access Management Adoption in Europe: 2009—Uptake of Individual Technologies Is Low, But Cloud Options Hold Promise. Forrester Research, 14.

[5] Koelewijn, G., Sodoyer, I. B., Geers, I. H., & Bakker, R. (2009). Identity & Access Management.

[6] Perkins, E. L., & Allan, A. (2005). Consider identity and access management as a process, not a technology (Vol. 129998). Technical report.

[7] Gunter, C. A., Liebovitz, D., & Malin, B. (2011). Experience-based access management: A life-cycle framework for identity and access management systems. IEEE security & privacy, 9(5), 48.

[8] Goth, G. (2005). Identity management, access specs are rolling along.Internet Computing, IEEE, 9(1), 9-11.

[9] Bruegger, B. P., Hühnlein, D., & Kreutzer, M. (2007). Towards global eID-Interoperability. Biometrics and Electronic Signatures - BIOSIG, 127-140.

[10] Laser Card. (2009). The Kingdom of Saudi Arabia National ID Card An Uncompromising Commitment to Document Security. Secure ID Solutions.

[11] Gemalto. (2009). The identity card program in Belgium. Retrieved from http://www.gemalto.com/brochures/download/gov_belgium_id.pdf

[12] Rössler, T. (2008). Giving an interoperable e-ID solution: Using foreign e-IDs in Austrian e-Government. Computer Law & Security Review, 24(5), 447-453. doi:10.1016/j.clsr.2008.07.006

[13] Al-khouri, A. M. (2006). UAE National ID Programme Case Study. International Journal of Human and Social Sciences, 1(2), 62-69.

[14] Alotaibi, S., Wald, M. (2012) IAMS framework: A new framework for acceptable user experiences for integrating physical and virtual identity access management systems. In, *2012 World Congress on Internet Security (WorldCIS). The IEEE World Congress on Internet Security (WorldCIS-2012)* New York, US, Institute of Electrical and Electronics Engineers, 17-22.

[15] Alotaibi, S. , Wald, M. (2012) Security, user experience, acceptability attributes for the integration of physical and virtual identity access management systems. In, *2012 International Conference on Information Society (i-Society). The IEEE International Conference on Information Society (i-Society 2012)* New York City, US, Institute of Electrical and Electronics Engineers, 277-282.

[16] Alotaibi, S. and Wald, M. (2012) Towards a UTAUT-based model for studying the integrating physical and virtual identity access management systems in e-government domain. In, *The 7th IEEE International Conference for Internet Technology and Secured Transactions (ICITST-2012), London, GB, 10 - 12 Dec 2012.*

[17] Venkatesh, V., Morris, M., Davis, G., & Davis, F. (2003). User Acceptance of Information Technology: Toward a Unified View. MIS Quarterly, 27(3), 425-478.

[18] Sekaran, U., Bougie, R., 'Research Methods for Business- Fifth Edition', John Wiley and Sons, 2009.

[19] Al-Qeisi, K. (2009). Analyzing the Use of UTAUT Model in Explaining an Online Behaviour: Internet Banking Adoption. Brunel University.

[20] Rubio, D. M., Berg-Weger, M., Tebb, S. S., Lee, E. S., & Rauch, S. (2003). Objectifying content validity: Conducting a content validity study in social work research. Social Work Research, 27(2), 94-104. doi:10.1093/swr/27.2.94

[21] Stat Trek. 2012. Sample Size: Simple Random Samples. [Online] http://stattrek.com/sample-size/simple-random-sample.aspx [May 20, 2013].

[22] Hair, J., Black, W., Babin, B., and Anderson, R. (2010). *Multivariate data analysis* (7th ed.): Prentice-Hall, Inc. Upper Saddle River, NJ, USA. pp. 23.

[23] Gandal N. 2002. Compatibility Standardisation and Network Effects. Oxford Review of Economic Policy. 18(1).

[24] Blunch, N. J. (2008). Exploratory Factor Analysis *Introduction to structural equation modelling using SPSS and AMOS* (pp. 70). London: Sage Publications.

[25] Ajzen, I. and Fishbein, M., (1980), Understanding Attitudes and Predicting Social Behavior. Prentice-Hall, Englewood Cli_s, N.J, paperback ed edition.

[26] Ajzen, I. (1985). From Intentions to Actions: A Theory of Planned Behaviour. Edited by Khul, J. and Beckmann, J. Springer-Verlag, and Berlin Heidlberg. New York Tokyo.

[27] Foster I. 2002. The Grid: Computing without bounds. Scientific American. 23(1).

[28] The South Hill Enterprise. 2012. The Chi-Square Test. [Online] http://www.science-projects.com/Chi2.htm [May 19, 2013]

[29] Alotaibi, S., Wald, Dr. M., and Argles, D., (2011) From Access Management System (AMS) to a Ubiquitous Access Management System (UbAMS), over Federated Access Management System (FAMS). In, *MUE 2011 Workshop: The IEEE/FTRA International Workshop on Multimedia, Communication and Convergence technologies (MCC 2011), Crete, Greece, 28 - 30 Jun 2011.* IEEE Press and will be included in the IEEE Xplorer.