A model for increasing the security of internet of things in smart transportation systems

Sanee M.E.Sepasgozar[a,] Sharifeh Sargolzaei[b], Samad M.E.Sepasgozar[c], Imriyas Kamardeen[c] and Shokouh Sargolzaei[d]

[a] Master of Software Engineering, Iran
[b] Department of Architecture and Urban Planning, Art University of Isfahan, Iran
[c] Faculty of Built Environment, UNSW, Australia
[d] Department of Mathematician, Payam Nour University of Zabol, Iran
E-mail: sanee.mes@gmail.com, sargolzaeis@gmail.com, samad.sepasgozar@gmail.com, imriyas@unsw.edu.au, s_iauzh@yahoo.com

Abstract –

The usability of the Internet of Things (IOT) is accelerated by making intelligent and equipping different machines and devices with smart sensors. IOT is used in smart cities, transportation, construction cases. IOT has the capability to provide real-time information for drivers and citizens to design their routes to avoid traffic and reduce fuel consumption. However, there is a significant number of IOT barriers to IOT utilization such as the distrust of users and managers in sharing information, suspicion to privacy and the ease of using the relevant applications. Despite the importance of these factors, a model for predicting the use of this technology for specific disciplines has not yet been developed, especially for developing countries. Therefore, this research attempts to propose a model for prediction of application, taking into account the increased security of IOT in intelligent transportation. To this end, influential constructs on user trust were collected and tested by questionnaire from 62 experts. The data were analyzed using Smart PLS using confirmatory factor analysis. The results show that 11 hypotheses in the research have been confirmed. The results of this study are very important for technology specialists and urban managers to establish the IOT in the field of urban transport.

Keywords –

Security, Internet of Things, Smart Transportation, Model

1 Introduction

Application of new technologies such as Internet of things (IOT) helps to increase the performance of smart cities The high number of intra-city trips is one of the reasons that cause traffic jam and air pollution, which can be reduced or monitored using IOT applications. However, managers in developing countries have encountered barriers to adopt IOT such as uncertainty and lack of trust. Whereas the amount of users' activity in the urban areas of developed countries is dependent on the IOT measured from the number of connected devices to the Internet at the end of 2015, was about 4.9 billion [1]. This growing trend reflects the increasing impact of IOT in life. Therefore, in close future without IOTs we are not able to control digital things in our life [2]. Therefore, the issues of security and confidentiality need to be considered to increase the IOT adoption rate. The purpose of this paper is to provide a model to increase the security of IOT in smart transportation in developing countries.

The paper seeks to answer how we can increase the security of IOT in urban transportation in developing countries. To answer this, based on the factors taken from theoretical foundations and reviewing the literature of research, twelve hypotheses are developed. Then, using the Smart PLS software, through expert analysis and expert interviews, hypotheses are examined and ultimately we tried to provide an effective model for increasing the security of IOT in smart transportation. This can increase the security of the smart city network.

In general, the structure of this paper is as follows: the first part, entitled literature review, according to the interdisciplinary nature of the research, requires some concepts examined and a common view of them. Therefore, there is a common chapter in the topics of the security domain, the IOTs, and smart transportation. In this section, the models and theories used in the analysis are identified and, in continue, the status of the constructs related to the security of the IOTs in these models is identified. In the second part, the method of confirmatory factor analysis is introduced as a research method to test the hypotheses of the proposed model for increasing the security of IOT in smart transport in smart city. In the third part, the results of factor analysis are presented and the conceptual model of increasing the security of IOTs in the urban transport sector is tested, corrected and finalized in order to realize the smart urban management. Finally, the results of the analysis are summarized in the final section.

2 Literature Review

One of the most controversial topic in the area of security is the emergence of a new paradigm for IOTs, which include a range of electronic devices that can connect to the Internet. The problem anticipated in IOTs is that things cannot be safely stacked and there is not enough memory to install and run security software on them. Therefore, the network should be protected to detect violations and prevent the entry of attacks [1]. Web-based technologies are moving at a fast pace and realizing the ideas of the smart city. Despite the speed of technologies that guarantee the security of users and their information, it is far behind the technology itself, and there are fewer studies in the research literature. The IOT has shown its most importance and application in the field of urban transportation [3-8].

The review of the literature in this field requires a lot of vigilance. However, what has been tried in this research is to investigate the IOT, network security and smart transportation. So, in the following, we try to identify shortcomings in each of these three areas in order to identify the effective factors in increasing the security of IOTs in smart transportation. Over the past decade, the IOT has entered silently and gradually in our lives, and we need to thank the availability of wireless communication systems, which are increasingly used as a technology motive for highly smart monitoring and application control [9]. The IOTs can be a collection of Web services, devices (RFIDs), infrared sensors, global positioning systems, barcode scanners, networking, and etc. by using the conventional protocol, the exchange of information and communication in order to achieve identification, tracking, monitoring and smart management of objects are used [10]. In other words, the IOT can be seen as a new form of network based on the Internet, which is much larger. A network is made up of advanced computers [11]. In the area of security of IOTs, it can also be said that traditional security interactions and privacy enforcement, due to their limited computing power, cannot be directly applied to the IOTs; in addition, the large number of connected devices causes scalability issues. Simultaneously, in order to gain full acceptance by users, it is necessary to define valid security models, privacy, and trust in the context of the IOT applications projects [12]. The purpose of security is to ensure that data anonymity, confidentiality, and integrity are guaranteed, as well as authentication and authorization mechanisms to prevent unauthorized users (i.e. humans and devices) to access this system. While privacy requirements are in place, data protection and the confidentiality of personal information of users must be guaranteed, as devices may handle sensitive information (for example, user habits). Finally, trust is an important issue because the IOT environment is characterized by a variety of devices that must process and manage the data in accordance with the needs and rights of the users.

Previous studies investigated sub topics of enabling technologies and middleware technologies in the IOT from the perspective of an application, analysis, and security and privacy issues with standardization, addressing, and the network is provided [13]. Security and privacy challenges were examined only from a legal perspective, with particular regard to the guidelines of the European Commission [14]; [15] in his paper discussed the Internet underwater objects, and only did a few notes present on the security issue; In another study [16], the advantages and disadvantages of centralized and dispersed architectures in terms of security and privacy on the IOTs, along with analysis of major attack patterns and threats, were examined. Yan et al. [17] focused solely on the issue of trust management in the IOTs.

Here are some brief references to some of the most important security issues on the IOTs. In relation to the issue of access control, various articles have addressed the subject from a variety of perspectives. For example, Ma et al. [18] is focused on the data literacy layer, which is responsible for the direct collection of information. An approach that addresses the outsourcing-data authentication problem can be found in [19, 20]. Sicari et al. [9] also suggests a semi-distributed approach. More precisely, in this research, a security framework and an access control model were proposed to secure the so-called DSMSs that extend the Borealis data flow engine to security requirements [21]. Finally, in [22], a UML conceptual model was defined for all objects and Internet architectures.

Review of resources about privacy on the IOT is also indicative of useful research. In the research [23], data labeling is proposed for managing the privacy of the IOTs; in [24], an access-controlled protocol by user is proposed; In [25], the continuous anesthetization of data flows was presented through the adaptive cluster; In [26], traditional privacy mechanisms are divided into two categories: optional access and limited access.

Another method, which uses a sign-on signing scheme to guarantee privacy on the Internet, is presented in the research [27]. [28] in their paper began to work on data mining privacy techniques, which aims to minimize the probability of disclosure of critical data and decomposing sensitive content.

In reviewing resources on the topic of trust of the IOTs are also briefly referred to several articles. [29] wrote about the evaluation of the trustworthiness of IOTs inputs. A similar methodology for evaluating reliability is provided by [30] on the so-called Internet of Social Things. This paradigm is due to the integration of the social networking concepts within the things of the Internet. The articles mentioned so far are merely to illustrate the large volume of studies on the dimensions of the IOTs. But this area of knowledge is less applicable to urban life applications and urban management.

The third area used in leading research to achieve the purpose of the research is smart transportation. The concept of smart city has been adapted from a variety of definitions that include the intelligent city, the information city, the knowledge city, the digital city, and the same concept as the smart city [31]. Cities play a prominent role in social and economic aspects all over the world [32]. The smart transportation system is a general term for the application of a combination of communication technologies, control and information processing for the transportation system. Using it will save lives, saving time, money, energy and environmental benefits.

An overview of the available resources shows that there are two theories of diffusion of innovation and technology acceptance model, which are rlated to technology acceptance dimensions. Having a special position in terms of both personal and psychological aspects, the technology acceptance model is one of the most widely-used models. This model addresses the causes of technology rejection from the psychological point of view for users. Other popularity that can be effective in achieving this goal is diffusion of innovation theory. This theory has redefined a set of constructs that can be used to study the adoption of individual technology.

The review of resources clearly refers to the extensive efforts of researchers in the field of the applicability of the IOTs. However, the lack of acceptance of this termination due to the lack of security in its application is one of the most important reasons that has not been tested in the field of smart transportation from the psychological point of view in developing countries. In the next section, with a closer focus on effective constructs in increasing the security of IOTs in the field of smart transportation, the paper is trying to provide an effective model in this regard.

3 Conceptual framework

In this part, the initial conceptual model to increase the security of IOTs in smart transportation is presented. Figure 3 illustrates the process of modeling the technology acceptance model by users in Iranian metropolitan areas in four main stages. In this research, in order to provide a proposed model for increasing the security of IOTs in smart transportation, the researcher is attempting to cover as broadly as possible a theoretical concept. For this purpose, both theories are used. Since the roots of the two models are common in some constructs, the two models can be considered together to provide the theoretical basis for their proposed model. In this paper, the implications of the proposed theory that affects the security of the IOTs in the field of smart transportation are introduced as construct, including the perceived usefulness, compatibility, or trial ability. In Figures 1 and 2, technology acceptance model and diffusion of innovation theory are introduced.

The investigating of the constructs of the models shows that the two constructs, the relative advantage and complexity, of the diffusion of innovation theory have the same concepts with the two constructs, perceived usefulness and perceived ease of use, respectively, of the technology acceptance model. As mentioned, the theoretical basis of the proposed research model was introduced in order to increase the security of IOTs in smart transportation as Fig. 4. Based on the theoretical foundations, eleven constructs are presented to provide the views and theories on which they are based. Table 1 lists the 12 final constructs used in the proposed model.

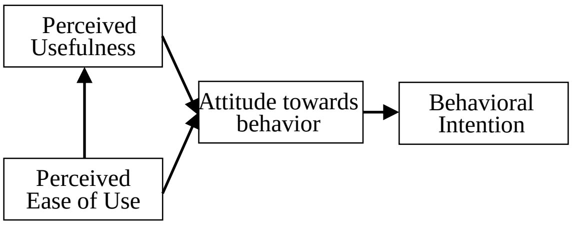

Figure 1. Technology acceptance model
Reference: [33]

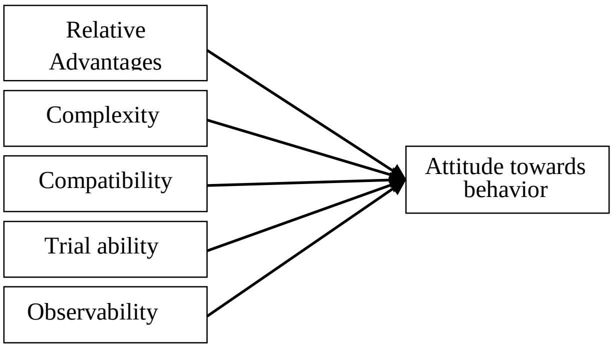

Figure 2. Diffusion of innovation theory
Reference: [34]

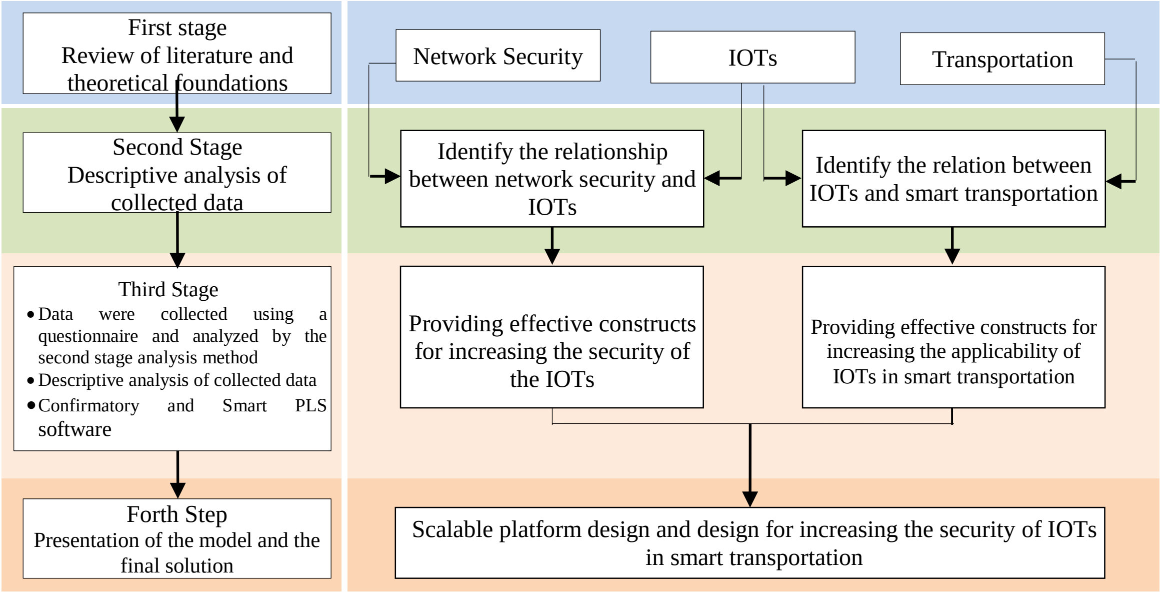
First stage
Review of literature and theoretical foundations
Second Stage
Descriptive analysis of collected data
Third Stage
• Data were collected using a questionnaire and analyzed by the second stage analysis method
• Descriptive analysis of collected data
• Confirmatory and Smart PLS software
Forth Step
Presentation of the model and the final solution
Network Security
IOTs
Transportation
Identify the relationship between network security and IOTs
Identify the relation between IOTs and smart transportation
Providing effective constructs for increasing the security of the IOTs
Providing effective constructs for increasing the applicability of IOTs in smart transportation
Scalable platform design and design for increasing the security of IOTs in smart transportation

Figure 3. Conceptual model making process enhancement of security IOT in smart transportation

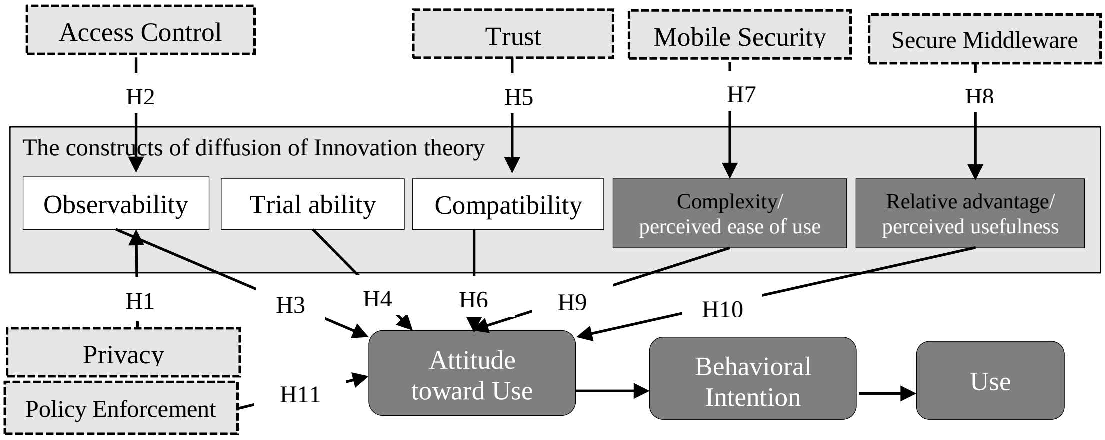

Figure 4. Theoretical basis of the proposed model for increasing the security of IOTs in smart transportation

4 Research Method

In this research, eleven hypotheses have been developed based on the relations among fifteen constructs taken from the theoretical foundations to achieve its goal of increasing the security of the IOTs. The main purpose of this paper is to formulate hypothesis and develop the conceptual model rather than analyzing the data which require further investigation.

As shown in Fig. 1, a quantitative confirmatory factor analysis was used to test the model of increasing the security of IOTs in smart transportation. Factor analysis is performed using Smart PLS software. A questionnaire was used to collect the data to test the hypotheses. This means that for each hypothesis related to model constructs, questions have been raised and forwarded in the form of a questionnaire among experts. To determine the sample size, based on the method of structural equations, ten times more than the number of markers forming a construct is selected as the sample size. Namely, in the model, identifying the instruments that have the largest number of constituent markers, and this amount is 10 times that of the desired sample size [35]. Since in this research according to Fig. 4, in the attitude construct, there are 7 indicators, the sample size was determined to be 70. This sample size is used to collect data through questionnaires forwarded. These individuals have been selected by experts in the field of transportation, computer and information technology in organizations under the supervision of the municipality of Tehran. 62 questionnaires were returned to perform the analysis. Therefore, the return rate of the questionnaire is 88%. The validity of the proposed constructs for the model is validated using a confirmatory factor analysis method. The Smart PLS was used to test the model. This software is used to analyze multi-construct data. Smart PLS is based on the estimation of the least number of variables in order to optimize the explanation of variance in the constructs dependent on the structural equation models. The purpose of this is to maximize the variance of dependent variables defined by independent variables [35].

Table 1. Reviewing Constructs Extracted from Theoretical Foundations, the three criteria of Cronbach's Alpha, AVE and CR for all constructs and Factor Loading of Research Questions

Models	Construct	Acronym	Cronbach's Alpha	CR	AVE	Measure	Loading
Technology Acceptance Model	Perceived Ease Of Use	PEOU	0.84	0.85	0.73	PEOU1	0.942
						PEOU2	0.963
						PEOU3	0.894
						PEOU4	0.741
	Perceived Usefulness	PU	0.75	0.85	0.66	PU1	0.892
						PU2	0.875
						PU3	0.908
	Attitude toward Use	AU	0.91	0.92	0.59	AU1	0.811
						AU2	0.829
						AU3	0.821
						AU4	0.987
						AU5	0.855
	Behavioral Intention	BI	-	-	-	-	-
Diffusion of Innovation Theory	Relative Advantages	RA	-	-	-	-	-
	Observation	OB	0.95	0.72	0.51	OB1	0.766
						OB2	0.946
						OB3	0.812
	Compatibility	CT	0.78	0.87	0.7	CT1	0.819
						CT2	0.926
						CT3	0.750
	Trial-Ability	TA	0.83	0.89	0.66	TA1	0.855
						TA2	0.705
						TA3	0.919
						TA4	0.760
	Complexity	CX	-	-	-	-	-
Security of IOTs	Secure Middleware	SM	0.76	0.82	0.7	SM1	0.776
						SM2	0.884
	Trust	TR	0.77	0.85	0.59	TR1	0.826
						TR2	0.716
						TR3	0.734
						TR4	0.883
	Mobile Security	MS	0.71	0.81	0.51	MS1	0.845
						MS2	0.977
						MS3	0.787
	Privacy	PY	0.83	0.73	0.54	PY1	0.884
						PY2	0.942
						PY3	0.722
						PY4	0.787
	Access Control	AC	0.83	0.91	0.84	AC1	0.747
						AC2	0.872
	Policy Enforcement	PE	0.86	0.91	0.72	PE1	0.840
						PE2	0.945
						PE3	0.856
						PE4	0.736

Note: average variance extracted (AVE), composite reliability (CR).

4.1 Hypotheses Formulation

In this section, research hypotheses that are presented on the basis of the relationships between the research constructs and the literature review are briefly presented. These relationships are shown in Figure 4.

- H1: Privacy has a negative relationship with observability in using IOTs in smart transportation.
- H2: Access Control has a negative relationship with observability in using IOTs in smart transportation.
- H3: Observability has a positive relationship with Attitude toward Use in using IOTs in smart transportation.
- H4: Trial ability has a positive relationship with Attitude toward Use in using IOTs in smart transportation.
- H5: Trust has a positive relationship with Compatibility in using IOTs in smart transportation.
- H6: Compatibility has a positive relationship with Attitude toward Use in using IOTs in smart transportation.
- H7: Mobile Security has a negative relationship with Perceived Ease of Use in using IOTs in smart transportation.
- H8: Secure Middleware has a negative relationship with Perceived Ease of Use in using IOTs in smart transportation.
- H9: Perceived Ease of Use has a negative relationship with Attitude toward Use in using IOTs in smart transportation.
- H10: Perceived Usefulness has a positive relationship with Attitude toward Use in using IOTs in smart transportation.
- H11: Policy Enforcement has a positive relationship with Attitude toward Use in using IOTs in smart transportation.

In continue, based on the analysis done on the hypotheses carried out using the data collected by the questionnaires, the hypotheses are either confirmed or rejected.

5 Data Analysis and Results

In order to evaluate the proposed model, the structural equation modeling is utilized using the Smart PLS 3.0 [36]. The paper also presents the results of two tests of the measurement model in terms of validity and reliability, the structure of the model in terms of the relationship among variables, and fitness of the model. If the model passes all three stages successfully, it shows the correctness of the selected constructs and their dependent terms. For testing the measurement models, we examined the ‘convergent validity’ and ‘discriminant validity’.

5.1 The Measurement Model

In this section, each of the proposed factors is referred to the construct and questions related to each construct. T-value is a test used to validate measurement models in statistics science. The t value for meaningful factor loads in the corresponding fields of each variable in the study indicates that the value greater than 2.66 is significant for the values of t obtained at the error levels of 0.01 [36]. Other indicators are categorized into two groups of convergent validity and discriminant validity for measuring the model of measurement. In the following, these two categories of tests are discussed.

5.1.1 Convergent Validity

Convergent validity is used to determine construct validity by defining factor loading, Cronbach's alpha, Average Variance Extracted (AVE), and Composite Reliability (CR) [40]. Table 1 shows the loading coefficients of the corresponding measures of each construct varying from 0.7 to 0.9. The load value of each item on the corresponding construct is well above the recommended value of 0.7 [39] indicating the proper and desirable load factor of each item on its related construct. Measures with the value of less than 0.7 can be omitted. Cronbach's alpha was applied to assess the validity of the measures. The CR coefficient distinguishes the correlation coefficient of measures in one dimension for fitting adequate measurement models [39]. The results validate the criteria as Cronbach's alpha is well above 0.7, and the AVE is also above 0.8, which surpasses the recommended threshold of 0.5 [39]. The CR is above 0.7 [38] for all constructs [39] excluding CT and PREL, which are very close to 0.7. The results validate that all criteria were satisfactory, since they are above the recommended values.

5.1.2 Discriminant validity

Divergence validity of the model was assessed through the comparison of the correlation coefficient of constructs with its indexes versus the correlation of that constructs with other constructs was presented. The results are shown in Table 2. According to [38], AVE the constructs located in main diameter of matrix are more than the correlation between them, which are arranged in the lower and left boxes of the main diameter. Therefore, it can be concluded that in the above model, the constructs interact more with their own indicators than with other constructs. This shows that the divergence validity of the model is appropriate.

5.2 Structural Model

To test the construct validity of factors in the model, a confirmatory factor analysis was conducted. To investigate the CFA using structural equation modeling, a model was first created based on the type of constructs such as observability and related measures of each construct such as OB1 to OB3. This analysis and model development were done in Smart PLS 3.0. The hypotheses were examined by assessing the parameters of the PLS structural model. The R^2 value for constructs vary from 0.16 to 0.92. The result of R^2 values shows the predictive power of the model including four dependent constructs is acceptable and indicates that the theoretical model explained a substantial amount of the variance in performance. The value of R^2 for observation, compatibility, perceived ease of use, and attitude toward use are 0.31, 0.3, 0.28, and 0.39, respectively. The standardized path coefficients also show the strength of the relationship between the independent constructs (e.g. PSY) and the four dependent constructs (e.g. OB). The multi-collinearity between the variables in our model was evaluated, and no cause was found for concern related to the variance inflation factor (VIF) criteria, as according to the Table 3 all of the values of VIF are below the proposed value of 5.00 [40]. In addition, the model's predictive relevance was assessed by using the blindfolding procedure [40]. The values of Q^2 which are greater than zero, indicate the sufficient predictive relevance of the model. If the model passes the determined tests in the confirmatory factor analysis method using smart PLS successfully, the proposed conceptual model and; in other words, the factors and the related questions (items) to each factor are verified. As the results are shown in Table 3, Access Control, Observability, Mobile Security, and Secure Middleware have not been able to explain more than 50% of the corresponding construct variance. The t-value was compared with the error level to assess the relationship between dependent constructs and independent constructs. Where the values are greater than of the minimum of 1.64 recommended by [40], all relationships were confirmed. At the error level of 0.01%, 0.05%, and 0.1. %, path coefficients with the minimum of 2.58, 1.96, and 1.64 in t-value are confirmed [40]. Table 3 shows that the value ranging from 0.03 to 30.79 and the hypotheses excluding H2, H7, and H9 are supported.

Table 2. Discriminant Validity

construct	PY	PU	PE	AC	OB	TA	TR	CT	MS	SM	PEOU
PY	**0.81**										
PU	0.49	**0.84**									
PE	0.63	0.83	**10.5**								
AC	0.43	0.17	0.36	**0.66**							
OB	0.63	0.43	0.54	0.13	**0.59**						
TA	0.29	0.52	0.68	0.31	0.47	**0.78**					
TR	0.39	0.71	0.76	0.23	0.56	0.75	**0.89**				
CT	0.51	0.72	0.72	0.23	0.5	0.53	0.78	**0.8**			
MS	0.72	0.48	0.48	0.19	0.23	0.09	0.39	0.45	**0.73**		
SM	0.62	0.45	0.4	0.02	0.28	0.02	0.29	0.44	0.08	**0.66**	
PEOU	0.64	0.84	0.91	0.46	0.52	0.59	0.84	0.83	0.56	0.48	**0.86**

Table 3. Results of the tested hypotheses including path coefficient, significance index and explained variance

Hs	Path Relationship	Std. Beta	Standardized Path Coefficient	Path Significance Index (t-value)	Decision	Explained Variance (R^2)	VIF	Q^2
H1	PY → OB	5.71	0.50	11.42	Supported ($p<0.001$)	0.51	2.04	0.31
H2	AC → OB	0.29	0.76	0.38	Not supported	0.16		
H3	OB → AU	9.61	0.40	24.02	Supported ($p<0.001$)	0.41		
H4	TA → AU	2.34	0.49	4.77	Supported ($p<0.001$)	0.5		
H5	TR → CT	22.79	0.74	30.79	Supported ($p<0.001$)	0.74	3.84	0.3
H6	CT → AU	2.52	0.70	3.6	Supported ($p<0.001$)	0.71		
H7	MS → PEOU	0.68	0.53	1.28	Not supported	0.34	1.51	0.28
H8	SM → PEOU	1.31	0.64	2.04	Supported ($p<0.05$)	0.24		
H9	PEOU → AU	0.03	0.92	0.03	Not supported	0.92		
H10	PU → AU	2.36	0.75	3.14	Supported ($p<0.001$)	0.76	4.16	0.39
H11	PE → AU	4.31	0.89	4.84	Supported ($p<0.001$)	0.9		

5.3 Fit Model

The third step that needs to be considered in the proposed model is the overall model fit index. Model fit index is an acceptable criterion for confirming the developed theoretical model using the collected data [41]. The method for calculating the overall model Goodness of Fit (GoF) index [42] is as follows:

$$GOF = \sqrt{\overline{Communalities} \times \overline{R^2}}$$

The Communalities value is obtained of the average shared values of all constructs or, in other words, it is obtained of the average variance extracted presented in Table 1. The R^2 value is also obtained from the mean R square or explained variance of all model' constructs in Table 3. R^2 of determination is a number that indicates the percent of variances in the dependent variable. If R^2 be 1, it indicates that the regression line perfectly fits the data. The amount of GoF was checked at three levels: GoFsmall = 0.1, GoFmedium = 0.25, and GoFlarge = 0.36. The amount of GoF more than 0.36 represents a perfect fit conceptual model of research [42]. Therefore, the value of 0.67 for GoF of present research model is suitable fit and the proposed conceptual model is confirmed.

In general, due to the proper quality of the measurement models, the structural model, and also the appropriate model fitness, it can be concluded that according to the confirmatory factor analysis for this study, the items of the questionnaire can be used to explain the identified factors or suggested constructs.

6 Discussion

The purpose of this study is to propose a conceptual model, which can be used for increasing the security of IOTs in smart transportation in developing countries. For this purpose, firstly, the literature on the three areas of the IOTs, the security, and smart Transportation have been investigated. Then, based on theoretical foundations, the research hypotheses were presented. These hypotheses have been investigated by confirmatory factor analysis and Smart PLS software. Further confirmation or rejection of hypotheses has been discussed, but a large amount of data is required to exactly test the hypotheses and generalize them. The contribution of this paper is to propose a conceptual acceptance model.

Two factors should be considered to confirm or reject the research hypotheses. The first factor is the path coefficient. The positive path coefficient represents a direct relationship between constructs and the negative path coefficient represents an indirect relationship. This value in large measure represents the power of the relation that decreases with the establishment of indirect relations from the magnitude of a path coefficient. The second factor is t value. The t-value was compared with the error level to assess the relationship between dependent constructs and independent constructs. Where the values are greater than of the minimum of 1.64 recommended by (Hair Jr et al., 2016), all relationships are confirmed. At the error level of 0.01%, 0.05%, and 0.1. %, path coefficients with the minimum of 2.58, 1.96, and 1.64 in t-value are confirmed (Hair Jr et al., 2016). The results of the table 3 show that the t-statistic for hypotheses with an error level of 0.001 is greater than 2.58, except for H8, which is more than 0.05 with an error level of 1.96. Based on this index, three hypotheses H2, H7, and H9 are rejected based on t value. In the first section, the hypotheses that have been confirmed are discussed, and the following three rejected hypotheses are introduced.

Another importance point related to hypotheses is the power of them. In this way, the greater amount of the coefficient, the more powerful hypothesis whether this is negative or positive. Therefore, the hypotheses are further reviewed on the basis of their power. As shown in table 3, H5 has a lot of power and is very close to reality. The sharp difference between this hypothesis and other hypotheses can be attributed to the importance of questions related to this construct in the questionnaire for questioners. Accordingly, trust in the IOTS in the transportation system is important in connection with technology adaptation to increase the security of the IOTs in the transportation system. It was stated in the hypothesis that the confidence would be obtained when the system could be compatible with the existing values and psychological needs of the recipients and their experiences. Therefore, systems in the IOTs must be compatible with the values and psychological needs of its adopters. The path coefficient of H1 is in second place. In this hypothesis, privacy, when using IOTs in the transportation system, has a negative relationship with one's perception of being viewed by others. The almost strong significance of this hypothesis is that IOT users in urban transport are important in protecting their privacy when using this technology. This hypothesis has a third degree of importance for users. In H11, it has been argued that the policies enforcement by planners and supersonic devices, when using IOTs in the transport industry, have a positive relationship with the perception of the proportion of increasing the security of the IOTs in the transportation system. Thus, users tend to display government agencies and administrators their supervisory role to increase the security of the IOTs. So they will feel more secure. This hypothesis can also confirm the results of the previous hypothesis (H1). In H3, it is stated that observation by supermodels, when using IOTs in the transport industry, has a positive relationship with the individual's tendency to increase the security of the IOTs. Therefore, this category will be the second most important issue for IOT users in the transportation system. H8 also states that the interconnection between the large number of communication devices at different levels in the middleware at the time of using IOTs in the transportation has a negative relationship with the perception of the person's ease of use of the system. H10 discusses about having a positive relation between the usefulness of using IOTs in the transportation and a person's perception of the security of IOTs and his attitude toward its application. According to H6, compatibility of IOTs in the transportation system has a positive relationship with the perception of the individual about increasing the security of the IOTs. H4 also states that the ability of an individual to test the IOTs in the transport industry has a positive relationship with the perception of the individual about increasing the security of the IOTs.

As the results of table 3 show these three hypotheses are rejected. H7 is about the complexity of relationships in mobile devices when using IOTs in the transportation. According to this hypothesis, mobile security will have a negative impact on the perception of ease of use in using this type of technology. H2 anticipated that there is an inverse relationship between the access control of users to resources and data by government and supranational institutions, and the perception of one's being seen by others. This matter that this hypothesis is rejected indicates that there is not a positive relation between these variables. In other words, controlling the access of users during the use of IOTs in the transportation system is negatively related to the perception of the person than to be seen by others. In H9, it is stated that the perceived ease of using the IOTs in the transport industry has a negative relationship with the perception of the person about the security of IOTs and his attitude towards its application.

7 Conclusion

The purpose of this study is to achieve a model for increasing the security of IOTs in smart transportation. For this purpose, based on the review of the literature, the model was first proposed and the results of the 62 questionnaires collected by the experts were analyzed using a confirmatory factor analysis method based on the structural equation model. The validity of this model is confirmed by using a t-student test with an error rate of 0.001%. The results of Tables 1, 2, and 3 confirm the appropriateness of the reliability and convergence validity of the research model. In addition, according to the results of the appropriate quality of the measurement model, the structural model, as well as the fit model that was calculated in formula 1, the theoretical model confirmed by using the collected data confirms. Because of the confirmatory factor analysis for this research, the variables of the design questionnaires in the research can explain the identified factors or suggested constructs.

The results of the confirmatory factor analysis carried out on the hypotheses in the proposed model, examine the confirmation or rejection of the hypotheses based on the path coefficients in them comparing the t-value at the standard error level. According to Table 3, hypotheses 2, 7, and 9 are rejected. But the strength of the hypotheses can be determined based on their path coefficient. So the hypothesis 5, which has the highest path coefficient, has the strongest effect. It was stated in the hypothesis that the trust would be obtained when the system was compatible with the existing values and psychological needs of the recipients and their experiences. Therefore, existing systems in the IOTs should be compatible with the values and psychological needs of its users. Hypotheses 3 and 1 also are too strong. Finally, hypotheses 2, 7, and 9, which are rejected hypotheses, have a low path coefficient and are weak. The conceptual model presented in this paper is important for transportation, information technology, computer and urban managers and decision-making organizations for the provision and deployment of the IOTs in the field of urban transportation. However, the statistical results may very in larger samples and different contexts. The proposed model helps to provide a powerful tool for increasing the security of IOTs to increase the level of user's interest in this technology.

References

[1] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, "Internet of things: Vision, applications and research challenges," Ad Hoc Networks, vol. 10, pp. 1497-1516, 2012.

[2] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things) IoT): A vision, architectural elements, and future directions," Future Generation Computer Systems, vol. 29, pp. 1645-1660, 2013.

[3] A. Amekudzi, L. Thomas-Mobley, and C. Ross, "Transportation planning and infrastructure delivery in major cities and megacities," Transportation Research Record: Journal of the Transportation Research Board, 2015.

[4] N. Zhong, J. H. Ma, R. H. Huang, J. M. Liu, Y. Y. Yao, Y. X. Zhang, et al., "Research challenges and perspectives on Wisdom Web of Things (W2T)," The Journal of Supercomputing, vol. 64, pp. 862-882, 2013.

[5] J. M. Morris, P. Dumble, and M. R. Wigan, "Accessibility indicators for transport planning," Transportation Research Part A: General, vol. 13, pp. 91-109, 1979.

[6] I. Mayeres, S. Ochelen, and S. Proost" ,The marginal external costs of urban transport," Transportation Research Part D: Transport and Environment, vol. 1, pp. 111-130, 1996.

[7] B. Donovan and D. B. Work, "Using coarse gps data to quantify city-scale transportation system resilience to extreme events," arXiv preprint arXiv:1507.06011, 2015.

[8] S. Sargolzaei, S. M. E. Sepasgozar, and M. Mojtahedi, "MODELING URBAN TECHNOLOGY ACCEPTANCE: FACTOR ANALYSIS APPROACH," in 16th International Conference on Construction Applications of Virtual Reality ,Hong Kong, 2016.

[9] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," Computer Networks, vol. 76, pp. 146-164, 2015.

[10] S. Babar, A. Stango, N. Prasad, J. Sen, and R. Prasad, "Proposed embedded security framework for internet of things (IoT)," in Wireless Communication, Vehicular

Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE), 2011 2nd International Conference on, 2011, pp. 1-5.

[11] R. Roman, C. Alcaraz, J. Lopez, and N. Sklavos, "Key management systems for sensor networks in the context of the Internet of Things," Computers & Electrical Engineering, vol. 37, pp. 147-159, 2011.

[12] J. Anderson and L. Rainie, "The Internet of things will thrive by 2025," Pew Research Internet Project, vol. 14, 2014.

[13] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," Computer networks, vol. 54, pp. 2787-2805, 2010.

[14] R. H. Weber, "Internet of Things–New security and privacy challenges," Computer Law & Security Review, vol. 26, pp. 23-30, 2010.

[15] M. C. Domingo, "An overview of the internet of underwater things," Journal of Network and Computer Applications, vol. 35, pp. 1879-1890, 2012.

[16] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed internet of things," Computer Networks, vol. 57, pp. 2266-2279, 2013.

[17] Z. Yan, P. Zhang, and A. V. Vasilakos, "A survey on trust management for Internet of Things," Journal of network and computer applications, vol. 42, pp. 120-134, 2014.

[18] J. Ma, Y. Guo, J. Ma, J. Xiong, and T. Zhang, "A hierarchical access control scheme for perceptual layer of IoT, Jisuanji Yanjiu yu Fazhan/Comput," Res. Dev, vol. 50, pp. 1267-127.۲۰۱۳ ,۵

[19] S. Papadopoulos, Y. Yang, and D. Papadias, "Continuous authentication on relational streams," The VLDB Journal—The International Journal on Very Large Data Bases, vol. 19, pp. 161-180, 2010.

[20] S. Papadopoulos, Y. Yang, and D. Papadias, "CADS: Continuous authentication on data streams," in Proceedings of the 33rd international conference on Very large data bases, 2007, pp. 135-146.

[21] D. J. Abadi, Y. Ahmad, M. Balazinska, U. Cetintemel, M. Cherniack, J.-H. Hwang, et al., "Design issues for second generation stream processing engines," in Proc. of the Conference for Innovative Database Research (CIDR), Asilomar, CA, 2005.

[22] P. Mahalle, S. Babar, N. R. Prasad, and R. Prasad, "Identity management framework towards internet of things (IoT :(Roadmap and key challenges," in International Conference on Network Security and Applications, 2010, pp. 430-439.

[23] D. Evans and D. M. Eyers, "Efficient data tagging for managing privacy in the internet of things," in Green Computing and Communications (GreenCom), 2012 IEEE International Conference on, 2012, pp. 244-248.

[24] X. Huang, R. Fu, B. Chen, T. Zhang, and A. Roscoe, "User interactive internet of things privacy preserved access control," in Internet Technology And Secured Transactions, 2012 International Conference for, 2012, pp. 597-602.

[25] J. Cao, B. Carminati, E. Ferrari, and K.-L. Tan, "Castle: Continuously anonymizing data streams," IEEE Transactions on Dependable and Secure Computing, vol. 8, pp. 337-352, 2011.

[26] J.-c. YANG and B-.x. FANG, "Security model and key technologies for the Internet of things," The Journal of China Universities of Posts and Telecommunications, vol. 18, pp. 109-112, 2011.

[27] J. Su, D. Cao, B. Zhao, X. Wang, and I. You, "ePASS: An expressive attribute-based signature scheme with privacy and an unforgeability guarantee for the Internet of Things," Future Generation Computer Systems, vol. 33, pp. 11-18, 2014.

[28] A. Ukil, S. Bandyopadhyay, and A. Pal, "IoT-privacy: To be private or not to be private," in Computer Communications Workshops (INFOCOM WKSHPS), 2014 IEEE Conference on, 2014, pp. 123-124.

[29] F. Bao and I.-R. Chen, "Dynamic trust management for internet of things applications," in Proceedings of the 2012 international workshop on Self-aware internet of things, 2012, pp. 1-6.

[30] M. Nitti, R. Girau, L. Atzori, A. Iera, and G. Morabito, "A subjective model for trustworthiness evaluation in the social internet of things," in 2012 IEEE 23rd International Symposium on Personal, Indoor and Mobile Radio Communications-(PIMRC), 2012, pp. 18-23.

[31] J. H. Lee, M. G. Hancock, and M.-C. Hu, "Towards an effective framework for building smart cities: Lessons from Seoul and San Francisco," Technological Forecasting and Social Change, vol. 89, pp. 80-99, 2014.

[32] V. Albino, U. Berardi, and R. M. Dangelico, "Smart Cities: Definitions, Dimensions, Performance, and Initiatives," Journal of Urban Technology, vol. 22, pp. 3-21, 2015.

[33] F. D. Davis, "Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology," MIS quarterly, pp. 319-340, 1989.

[34] E. M. Rogers, "Diffusion of innovation5th ed," ed: New York: Free Press, 2003.

[35] V. Vinzi, W. W. Chin, J. Henseler, and H. Wang, Handbook of partial least squares: Springer, 201.۰

[36] C. Ringle, S. Wende, and A. Will, "Smart PLS 2.0 M3, University of Hamburg," ed, 2005.

[37] L. J. Cronbach, "Coefficient alpha and the internal structure of tests," psychometrika, vol. 16, pp. 297-334, 1951.

[38] J. Nunnally, "Psychometric methods ",ed: New York: McGraw-Hill, 1978.

[39] C. Fornell and D. F. Larcker, "Evaluating structural equation models with unobservable variables and measurement error," Journal of marketing research, pp. 39-50, 1981.

[40] J. F. Hair Jr, G. T. M. Hult, C. Ringle, and M. Sarstedt, A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM): Sage Publications, 2016.

[41] A. Davari and A. Rezazade, Structural Equation Modeling by PLS Software Jahad Daneshgahi, 2014.

[42] M. Wetzels, G. Odekerken-Schröder, and C. Van Oppen, "Using PLS path modeling for assessing hierarchical construct models: Guidelines and empirical illustration," MIS quarterly, pp. 177-195, 2009.