TRUST BASED SECURITY MODEL FOR CLOUD SYSTEMS IN AN ORGANIZATION

MOHAMMAD SAALEM RAHMANI [1]*, ABULFATHI IBRAHIM SALEH AL-HUSSAINI [2], ADAMU ABUBAKAR IBRAHIM[3]

[1,2]Dept. of Information Systems, International Islamic University, Kuala Lumpur, Malaysia
[3] Dept. of Computer Science, International Islamic University, Kuala Lumpur, Malaysia

**Corresponding author: thesaalem@gmail.com*

(Received: 28th January 2021; Accepted: 4th July 2021; Published on-line: 30th September 2021)

ABSTRACT: Cloud storage has several advantages and benefits, including cost savings, increased adaptability, elasticity, and resource efficiency. For all of these advantages, there are also drawbacks and concerns for cloud users. The dispersed and opaque nature of cloud computing services creates several difficulties in their utilisation. As a result, users have little control over their data and information and are unclear if they can trust cloud providers. Consequently, the purpose of this research is to investigate the impact of customer and provider characteristics on cloud service outcomes, as well as the impact of *trust* on cloud service outcomes, and to see if *trust* mediates the relationship between customer and provider characteristics and cloud service outcomes. In order to fulfil the study's objectives, the measurement model, factor analysis, structural model assessment, and regression analysis were analysed. According to the study's findings, existing threats in cloud services are one of the reasons customers do not trust cloud service providers. Cloud services are unattractive because of the threats to privacy and security. This study also revealed that *trust* is critical for cloud service users and providers since it promotes utilisation, customer desire to use, and cloud service provider reputation. It was also observed that if there is no trust in these programmes, the results are quite bad. This research can help cloud service providers/developers understand why some individuals and organisations are unable to use their services.

KEY WORDS: *Cloud Computing, Trust, Cloud Computing Providers, Cloud Computing Outcome.*

1. INTRODUCTION

Cloud computing is consisting of software and hardware in data centres delivered as services and application through the internet (Ali, 2020). The term Software as a Service (SaaS) is used for these services, and the data centers hardware and software, also known as a “Cloud”. Recently, the Cloud Computing Service has received considerable attention from researchers (Tripathi & Sehgal, 2015). According to Shah (2014), the term cloud is used as a simile for "the internet" so cloud computing typically refers to computing based on the internet. Additionally

Shah proposed that cloud computing as the next generation of the internet, and rapidly becoming a common paradigm in which the digital access of computer resources is made available on request to users. Without thinking about owning the infrastructure and software, cloud computing is based on the notion of exchanging computer resources online. Mengistu, Alahmadi, Albuali, Alsenani and Che (2017) argued that current cloud infrastructure is mainly based on dedicated data centres where cloud networks are set up to host hundreds of thousands of dedicated servers. They stated that setting up the cloud data centre is costly and running the infrastructure requires expertise and a lot of resources, such as high cooling power and redundant power for guaranteed availability. For instance, 45% of the cost of the data centre goes to server procurement, 25% goes to advanced fault tolerance equipment, redundant power, cooling systems, and backup batteries, while 15% of the amortised total cost is accounted for by electrical costs consumed by the machines. As a new technology, the effects of cloud computing are significant as it makes it possible to store data on multiple servers and allows on-demand access to users, companies and governments. There is different implementation method of cloud either as a private cloud, public cloud, or hybrid situation. Cloud implementation may vary according to each organization's specific nature, including factors such as overall objectives, financial hardship, and risk profiles (Ramachandra, Iftikhar, & Khan, 2017; Shuaibu Hassan Usman, Mohammed Abdullah Bawazir, & Kabir, 2014).

Cloud storage provides users with great benefits and advantages (Tawalbeh, Darwazeh, Al-Qassas, & AlDosari, 2015). According to Sinha, Jain and Joshi (2014), there are several advantages of cloud computing to both end users and businesses of different sizes. The most significant advantage of cloud service is as a user, we do not need to worry about supporting the infrastructure or not having the necessary knowledge to develop and maintain the infrastructure, development environment or application because all these responsibilities have been shifted to someone else (cloud service provider). Manjeet Singh (2015) emphasized that basically, cloud computing works on a centralised system supplied by third parties. Cloud computing also offers third-party storage facilities. Cloud computing can also hire a complete platform for hardware resources, the development of software or the installation of an online platform. Cloud computing provides as-a-service, as-a-service platform and as-a-service software.

Kandel (2017) stated that the cloud usage refers to the use of users of different cloud services for various purposes. Due to various advantages such as reduction in cost, increased flexibility, elasticity and the efficient use of resources, cloud services are more and more common for different purposes such as testing and growth, larger data analyse, file storage, disaster recovery and backup. Ali (2020) argues that with the increase of cloud computing usage, this is subjected to various concerns like perceived *trust* of users. Aljazzaf, Perry and Capretz (2010) added that the relationship between a trustor and a trustee usually defines *trust*. Mayer et al (1995) stated that "the need of trust arises in a risky situation". There is confusion in human cultures regarding the behaviour of outsiders. Individuals who do not trust others will avoid interaction with them. In such ambiguous environment, *trust* plays an important role in enabling interaction. The subject that trusts a target party is a trustor. A target entity is a trusted entity and is known as the trustee (Aljazzaf, Perry, & Capretz, 2010). They also added that trust-building has more problems on the Internet. Many individuals are physically distanced and are probably completely

unknow in such an open online environment. Some companies use real names on the Internet and some have physical shops. That is not always the case, though. The bulk of individuals are not known physically and many are anonymous. Furthermore, the Internet has multiple domains and diverse demands, as in the real world.

Since consumers have lack of control over cloud services, they are unable to use technological measures for the protection of their data from unauthorised access, secondary use or any other form of violence. They should instead rely on contracts or other confidence mechanisms to try and enforce reasonable use in conjunction with compensatory mechanisms for a violation, such as protection, legal proceedings, or fines for breach of service level agreements (SLAs) (Pearson & Benameur, 2010). There are necessarily some overlaps and interdependency between mentioned issues and I believe that this study will find out the relations and outcomes of these issues on each other.

2. LITERATURE REVIEW

According to Aljazzaf, Perry and Capretz (2010), *trust* means, reliability; *trust* in integrity; trustful expectations; obligation or responsibility on someone in whom *trust* or authority is placed. As they said, *trust* is an intentional psychological state, based on positive expectations of another's intentions or behaviour. They also analysed *trust* in the online and offline world. In cloud service, we will be concerned about online and offline *trust* because cloud services are engaged with both. Online *trust* is the willingness of one party to be vulnerable to other parties' activities on the basis that others will take a specific action which is important for the trustee regardless of the ability of another party to monitor or control them.

Gokulnath and Uthariaraj (2016) also argued that the key issues in the cloud implementation barricade are security and *trust*. A comprehensive survey on 2017 by Ramachandra, Iftikhar, and Khan has been done on security in cloud computing. They have emphasized that all cloud service stakeholders (providers, consumers, auditors, brokers and carriers) must take the necessary precautions to ensure that the cloud computing platform is genuinely secure. Based on a case study, feedback on the service providers can obtain *trust* (Patil, Patil, & Patil, 2017). *Trust* has a huge impact on the deployment of cloud services. An experimental research by Prasad, Shah, Patel, and Bhavsar (2018) found out that Cloud applications are expanding and providers are also expanding. In this instance, trust management will be instrumental in determining the best cloud service (Prasad, Shah, Patel, & Bhavsar, 2018).

Adjei (2015) argued that, in that "I trust 'you' cannot be equated to 'you trust me', neither can *trust* be self-declared, and thus when people say 'trust me', question that usually follows is 'why'?". This has resulted in various conceptualizations of *trust*. Adjei also added that in cloud computing, there are different kinds of interactions with persons who are rarely known and may never meet the parties. In these circumstances, failure to be careful could have severe consequences. In cloud computing talks, the idea of confidence and *trust* is implied by the parties' expectations of willingness to action and react. In order to provide persistent *trust*, social and technological *trust* should be combined like companies who are owning good reputation in the market. Cloud customers must rely on contract or other *trust*

mechanism because they lack control of cloud resources and are not in a position to use technical mechanism to avoid secondary usage, misuse and authorise access. Other than *trust*, they can rely on other compensation like penalties for breach of service level agreement or insurance and court actions in the case of data breach (Pearson & Benameur, 2010). Reputation is another component of online *trust* which may be most valuable company assets. In order to choose a cloud service provider, customers can rely on the provider reputation and their transparency mechanism. In summary, the use of the cloud service involves trade-offs between safety, privacy, compliance, costs and benefits. IS success model is used for the evaluation of whether cloud service users are trusting providers or not and to find out the outcome of service provider's and consumer characteristics in cloud services. Furthermore, the mediation of *trust* among cloud service providers and consumers is examined.

3. THEORETICAL FRAMEWORK AND CONCEPTUALIZATION

Blueprint or research guide is a theoretical framework. It is a plan that offers several advantages for a research effort and which the researchers often borrow to develop their research (Adom & Hussain, 2018; Emad, Kamil, & Joe, 2018). They also argue that the theoretical framework provides a framework to demonstrate how researchers philosophically, methodologically, epistemologically and analytically define their studies. Although Grant and Osanloo (2014) stated that there is no perfect or right theories for a dissertation while there are some certain theories that are popular within each discipline. Past researchers (Adom & Hussain, 2018; Emad, Kamil & Joe, 2018) have also suggested several mechanisms for choosing a suitable theoretical framework. Moreover, they argued that the selection of a theory depends on the discipline or field of research meanwhile a theory adoption or adaptation must reflect the researcher understanding regarding the study and must be driving the study. To make an appropriate theoretical content selection, researchers must consider the principle guidelines of the study and should relate the problem. The researcher questionnaire and the study purpose must be included the necessary aspects of the theoretical framework and must be agreed with the assertions promulgated as well as the selected theory theorist. In this study, we selected the DeLone and McLean Information System Success theory.

DELONE AND MCLEAN INFORMATION SYSTEM SUCCESS THEORY

This paper adopted IS success model for the evaluation of whether cloud service users are trusting providers; and to find out the outcome of service provider's and consumer characteristics in cloud services. Furthermore, the mediation of *trust* among cloud service providers and consumers is examined. Factors for the success of information systems were very difficult to identify. DeLone and McLean in their paper "Information Systems Success: The quest for the dependent variable" have reviewed several definitions for IS success. DeLeon and McLean were also the pioneers of the IS success model for the evaluation of information system (IS) at the organizational level (Khader, 2016). According to Grover (1996), there is no definition of Information System success and every stakeholders have their own definition for assessing Information Systems success. "DeLone–Mclean model is an established and well-known information system (IS) model for assessing IS success" (Mardiana, Tjakraatmadja, & Aprianingsih, 2015). They also stated that

DeLone–McLean model is the most prominent although there are many other models for defining Information Technology success that have been introduced by other researchers.

DeLone and McLean (1992) examined the current IS success definitions and measures, which are classified into six main categories: (1) the quality of the system; (2) the quality of information; (3) the usage of the data system; (4) the user satisfaction; (5) the effect of each individual; and (6) the impact of organisations. They created an inter-dependence multidimensional model of measurement between the various categories of success (Dwivedi, Wade, & Schneberger, 2012). According to them, they proposed an update on the service quality 10 years after the publication of the DeLone and McLean models, and (1) to reflect the significance of service and support in successful eCommerce systems; (2) to make use of the intent for measuring user attitude as an alternative measure of use; and (3) the primary differences between the update and the original model are to break the individual impact and the organisational impact into more parsimonious net benefits. This IS success model has been chosen because it categorises IS success factors as system quality, information quality, IS use, user satisfaction, individual and organizational impacts. The updated version of this success model also includes service quality in the prior model of DeLone and McLean (1992) as an important factor for customer satisfaction (Kim, Oh, Shin, & Chae, 2009).

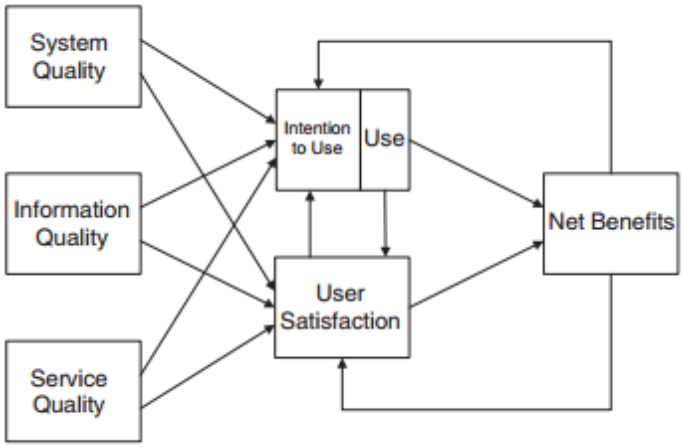

Fig. 1. Updated D&M IS Success Model

Our model is contructed based on the above theoretical framework (Fig. 1). The model considers consumer behaviour, provider behaviour and *trust* as the major factors influencing outcome and use of cloud computing services. Provider characteristic includes information quality, privacy protection and security protection. In the reminder of this study, we are going to examine whether consumers are trusting providers and how consumer characteristics and *trust* will affect the use of cloud computing.

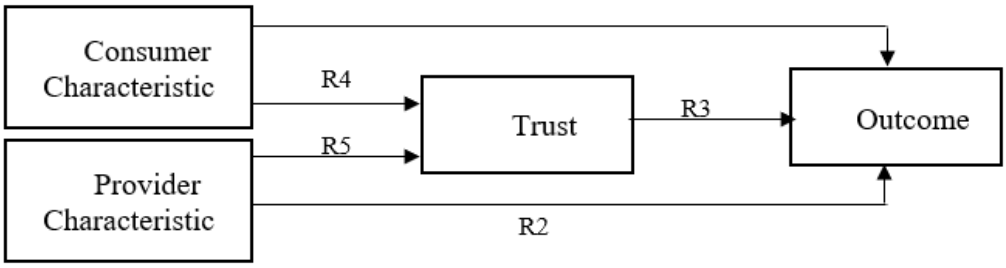

Fig. 2. Trust Based Model of Cloud Services

Research Hypothesis

H1 Customer characteristics positively influence cloud service outcome.

H2 Service providers characteristics positively influences cloud service outcome.

H3 There is positive impact of *trust* on cloud service outcome.

H4 *Trust* mediates the relationship of customer characteristics and providers characteristics with cloud service outcome.

4. RESEARCH METHODOLOGY

This research study adopted quantitative analysis approach. Moreover, quantitative analysis is a type of research approach that uses predefined methods like questionnaires, surveys and experiments (Saleh et al., 2020). It is defined by statistical analyses rather than subjective meanings of these results. The aim of quantitative approach is to collect numerical data in order to determine relationships among the variables. Thus, Boeren, (2018) and Apuke, (2017) argued that the main concern of the quantitative analysis is quantifying and evaluating factors in order to produce results that includes the utilization and analysis of the numerical data through using a certain mathematical technique. In addition, Williams, (2011) stated that quantity research approach starts with problem statement, hypothesis building or research questions, literature review and quantitatively analysis of the data. Thence, Creswell, (2003) and Williams, (2011) pointed out, that quantitative research approach "employ strategies of inquiry such as experiments and surveys and collect data on predetermined instruments that yield statistical data".

Also, in respect to the difference between qualitative and quantitative research, one of prime difference between qualitative and quantitative research methodology is that the quantitative methodology is to deal with testing yours prescribe hypothesis and looking forward at its causes, effects and predictions while qualitative methodology is to understand and interpret social interaction (Al-hussaini et al., 2019 ; Saleh et al., 2020).

5. MEASUREMENT MODEL

In this section, PLS classical structural equation model (SEM) is utilized for the model design. It consists of two parts which are structural (regression) equation between latent variables and measurement model (factor analysis) (see Fig. 3).

Assessment of Indicator Reliability (Outer Loadings)

Indicator reliability is a measurement to determine whether the indicators are consistent in the way they are intended to be measured (Hair et al. 2017, Ramayah et al. 2018). They also added that the acceptable and suggested value for loadings is 0.70 while others proposed that a value of more than 0.5 is acceptable. After removing the indicators lower than 0.5, we can see in that in Table 1, the highest outer loading value is 0.908 (USEQ2) under the variable consumer characteristics and the lowest goes to INTQ5 with the value of 0.512 under the outcome variable.

Assessment of Internal Consistency Reliability (ICR)

Internal consistency can be analyzed and evaluated by Composite Reliability (CR). Values of composite reliability must be greater than 0.70 (Hair et al. 2017). Table 1 shows that the variables are reliable with internal consistency ranging from 0.833 to 0.928 and considered as satisfactory.

Assessment of Convergent Validity

Convergence validity indicates that indicators of a variable should share a high proportion of variance. Convergent can be tested by analysing Average Variance Extracted (AVE) values of all item's variables and AVE value should be higher than 0.5 (Hair et al. 2017, Ramayah et all.2018). As stated in Table 1, AVE's values for this analysis are of higher than 0.5 and achieved the criteria as suggested by Hari et al (2017). Only outcome variable AVE's value is lower than 0.5 which is 0.451.

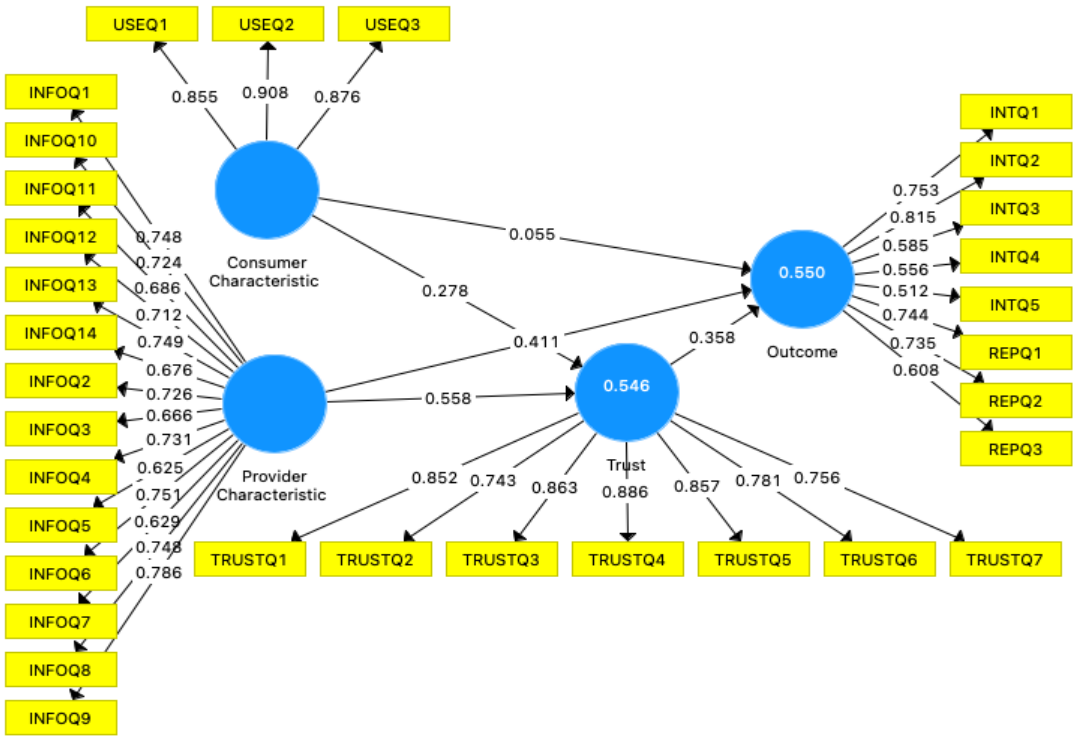

Fig. 3. Research Measurement Model

Table 1. Indicator Reliability, Converge Reliability, and Internal Reliability

Variables	Item	Loadings	AVE	CR	Rho_A
Provider Characteristics	INFOQ1	0.748	0.508	0.935	0.928
	INFOQ10	0.724			
	INFOQ11	0.686			
	INFOQ12	0.712			
	INFOQ13	0.749			
	INFOQ14	0.676			
	INFOQ2	0.726			
	INFOQ3	0.666			
	INFOQ4	0.731			
	INFOQ5	0.625			
	INFOQ6	0.751			
	INFOQ7	0.629			
	INFOQ8	0.748			
	INFOQ9	0.786			

Consumer Characteristics	USEQ1	0.855	0.774	0.911	0.862
	USEQ2	0.908			
	USEQ3	0.876			
Trust	TRUSTQ1	0.852	0.675	0.935	0.922
	TRUSTQ2	0.743			
	TRUSTQ3	0.863			
	TRUSTQ4	0.886			
	TRUSTQ5	0.857			
	TRUSTQ6	0.781			
	TRUSTQ7	0.756			
Outcome	INTQ1	0.753	0.451	0.865	0.833
	INTQ2	0.815			
	INTQ3	0.585			
	INTQ4	0.556			
	INTQ5	0.512			
	REPQ1	0.744			
	REPQ2	0.735			
	REPQ3	0.608			

- "All item loadings > 0.5 indicates indicator reliability" (Hulland, 1999, p. 1980).
- “All Average Variance Extracted (AVE) > 0.5 as indicates Convergent Reliability” (Baggozi and Yi (1988); Fornell and Larcker (1981)).
- “All Composite Reliability (CR) > 0.7 indicates internal consistency” (Gefen, et al, 2000).
- "All Cronbach's Alpha > 0.7 indicates indicator reliability" (Nunnally, 1978).

Assessment of Discriminant Validity

Discriminant validity is used to reflect the extent to which the measure is unique and is not simply reflections of other variables. It means that subjective independence of every indicator on its latent variable. That means the construct should be distinct compared to other constructs. DV can be established when all the items have higher outer loading for their subsequent constructs than its cross loading. Discriminant validity assessment is by Fornell and Lacker's criterion, cross loading and Heterotrait-Monotrait (HTMT) (Hair et al., 2017, Ramayah et al. 2018).

According to Hair et al. (2017) and Ramayah et al (2018), in Fornell and Larcker Criterion, on diagonal value should be higher than off diagonal because the value on a diagonal is the square root a particular variable (AVE) as stated in Table 2.

According to Chin (2010), Chin (1998) and Fornell and Larcker (1981), Cross Loading Criterion is useful to reduce the presence of multicollinearity among latent variables which denoting that the AVE of must be higher than squared correlations between the latent variable and all other variables as illustrated in Table 3.

Another alternative approach is Heterotrait-Monotrait Ratio (HTMT). The correlation of Heterotrait-Monotrait Ratio (HTMT) is tested by running a bootstrapping with the 0.10 level of confidence. If the value is 1, means there may be lack of discriminant validity as mentioned in Table 4. So, better for the confidence interval value to be lower than 1 (Hair et al., 2017, Ramayah et al. 2018).

Table 2: Discriminant Validity using Fornell and Larcker's Criterion

	Consumer Characteristic	Outcome	Provider Characteristic	Trust
Consumer Characteristic	**0.880**			
Outcome	0.464	**0.672**		
Provider Characteristic	0.507	0.689	**0.713**	
Trust	0.561	0.676	0.699	**0.822**

Table 3: Indicator Cross Loadings

	Consumer Characteristic	Outcome	Provider Characteristic	Trust
INFOQ1	**0.337**	0.560	0.748	0.574
INFOQ10	**0.460**	0.504	0.724	0.545
INFOQ11	**0.363**	0.473	0.686	0.526
INFOQ12	**0.466**	0.454	0.712	0.550
INFOQ13	**0.465**	0.627	0.749	0.549
INFOQ14	**0.317**	0.502	0.676	0.458
INFOQ2	**0.301**	0.416	0.726	0.418
INFOQ3	**0.335**	0.457	0.666	0.524
INFOQ4	**0.362**	0.494	0.731	0.471
INFOQ5	**0.261**	0.400	0.625	0.354
INFOQ6	**0.304**	0.497	0.751	0.460
INFOQ7	**0.283**	0.481	0.629	0.404
INFOQ8	**0.368**	0.473	0.748	0.516
INFOQ9	**0.382**	0.481	0.786	0.554

INTQ1	0.396	**0.753**	0.541	0.498
INTQ2	0.399	**0.815**	0.585	0.515
INTQ3	0.265	**0.585**	0.432	0.400
INTQ4	0.246	**0.556**	0.375	0.345
INTQ5	0.233	**0.512**	0.375	0.411
REPQ1	0.372	**0.744**	0.463	0.457
REPQ2	0.332	**0.735**	0.454	0.440
REPQ3	0.207	**0.608**	0.426	0.530
TRUSTQ1	0.405	0.620	**0.629**	0.852
TRUSTQ2	0.327	0.554	**0.553**	0.743
TRUSTQ3	0.504	0.548	**0.634**	0.863
TRUSTQ4	0.501	0.603	**0.603**	0.886
TRUSTQ5	0.449	0.546	**0.523**	0.857
TRUSTQ6	0.533	0.503	**0.540**	0.781
TRUSTQ7	0.508	0.501	**0.524**	0.756
USEQ1	0.855	0.344	0.402	**0.451**
USEQ2	0.908	0.412	0.481	**0.515**
USEQ3	0.876	0.460	0.451	**0.510**

Table 4: Indicator Heterotrait-Monotrait Ratio (HTMT)

	Consumer Characteristic	Outcome	Provider Characteristic	Trust
Consumer Characteristic				
Outcome	**0.545**			
Provider Characteristic	**0.562**	**0.784**		
Trust	**0.632**	**0.779**	**0.751**	

Assessment of Structure Model (PLS Algorithm)

In this part, we will evaluate the structural model result through another 4 assessments: structural assessment for collinearity issues, asses of the level of R^2, asses the effective size of $F^{2,}$ and path coefficient. Hair et al. (2017) stated that a structural model can be used to evaluate the linear regression effects between endogenous variables. It can predict the relationship between all these variables. PLS-SEM main structure assessment models are path coefficients, R^2, F^2, $Q^{2,}$ and effect size (Hair et al., 2017, Ramayah et al., 2018).

Assessment of Collinearity

It is important to identify the collinearity issue because the same variables hypothesized may measure the same constructs, misleading findings. Researchers can find the level of acceptance by analyzing the Variance Inflator Factor (VIF) (Hair et al., 2017; Ramayah et al., 2018; (Lowry & Gaskin, 2014)).

There are two VIF values, which are inner and outer. This study looks for the inner VIF value only. To avoid collinearity issues, the VIF value should be lower than five and greater than 0.2 (Wong, 2013). Based on this rule, our values are below five, and it shows that there is no strong indication of collinearity issue as illustrate in Table 5.

Table 5: Collinearity Assessment

Variables	Outcome	Trust
Consumer Characteristic	**1.517**	**1.346**
Outcome		
Provider Characteristic	**2.032**	**1.346**
Trust	**2.203**	

Table 6: Assessment of Structured Model

H	Tested Path	Path Coefficient	Standard Error	T-Value	P-Value	F2	Decision	UL	LL
H1	Consumer Characteristic > Outcome	0.051	0.067	0.827	**0.409**	0.002	Not Supported	-0.062	0.157
H2	Consumer Characteristic > Trust	0.282	0.057	4.889	**0.000**	0.502	Supported	0.186	0.372
H3	Provider Characteristic > Outcome	0.417	0.066	6.231	**0.000**	0.182	Supported	0.309	0.517
H4	Provider Characteristic > Trust	0.559	0.046	12.175	**0.000**	0.125	Supported	0.487	0.635
H5	Trust > Outcome	0.360	0.073	4.910	**0.000**	0.12	Supported	0.247	0.486

Path Coefficients

In order to get path coefficients, we need to do bootstrapping in SmartPLS to obtain t-value. According to Peng and Lai (2012), bootstrapping analysis is used for evaluation of direct effect of our hypothesis relationships. He also added that if a t-value of 5% is greater than 1.96 (for a two-tailed test), the hypothesis is supported. Path coefficients vary between the value of -1 and +1, and higher absolute values more predictive (stronger) relationships between our constructs. There are three types of effects which are direct effect, indirect effect, and total effects. As stated, strong relationships (higher values) are most significant, and weak relationships (lower values) are considered less/not significant (Hair et al., 2016, pp. 206). Hair et al. (2017) suggested assessing the corresponding t-value through a bootstrapping procedure with a sample of 5000. The analysis of the hypothesis is as follows:

H1 The path coefficient value of the first hypothesis (H1) is 0.051, and the obtained t-value is 0.827, which is lower than 1.96. Consumer Characteristics to Outcome is not supported because the coefficient interval of H1 is -0.062 for the lower limit and 0.157 for the upper limit. This shows that 0 falls within the interval and indicates that Consumer Characteristics to Outcome is not supported (insignificant).

H2 The path coefficient value of second hypothesis (H2) is 0.282 and the obtained t-value is 4.889 which is higher than 1.96. Consumer Characteristics to Trust is supported because coefficient interval of H1 is 0.186 for the lower limit and 0.372 for the upper limit. This shows that 0 does not fall within the interval and indicates that Consumer Characteristics to Trust is supported (significant).

H3 The path coefficient value of third hypothesis (H3) is 0.417 and the obtained t-value is 6.231 which is higher than 1.96. Provider Characteristics to Outcome is supported because coefficient interval of H1 is 0.309 for the lower limit and 0.517 for the upper limit. This shows that 0 does not fall within the interval and indicates that Provider Characteristics to Outcome is supported (significant).

H4 The path coefficient value of fourth hypothesis (H4) is 0.559 and the obtained t-value is 12.175 which is higher than 1.96. Provider Characteristics to Trust is supported because coefficient interval of H1 is 0.487 for the lower limit and 0.635 for the upper limit. This shows that 0 does not fall within the interval and indicates that Provider Characteristics to Trust is supported (significant).

H5 The path coefficient value of fifth hypothesis (H5) is 0.360 and the obtained t-value is 4.910 which is higher than 1.96. Trust to Outcome is supported because coefficient interval of H1 is 0.247 for the lower limit and 0.486 for the upper limit. This shows that 0 does not fall within the interval and indicates that Trust to Outcome is supported (significant).

Coefficient of Determination (R2)

R^2 matrix shows the percentage of prediction or covariance in our model or simply, it measures the model's predictive accuracy. Generally, R^2 has three rules of thumb which are weak, moderate and substantial. R^2 with the value of 0.25 is considered week, 0.50 as moderate, and lastly with the value of 0.75 as substantial. Higher R^2 value establishes model's explanatory power (Hair et al., 2017, pp. 216). Based on our findings for this study, R^2 is 0.496 (almost 50 percent) which is considered as the moderate level (almost achieved moderate level).

Effect Size Assessment (F^2)

F^2 measure the contribution of independent variables to dependent variables of R^2 value change. The effective size clarifies any change in R^2 after the including or excluding of any particular latent variables from our model. It has three level which are weak effect with the value of $0.02 =< f^2 < 0.15$, moderate effect with the value of $0.15 <= f^2 < 0.35$ and strong effect with the value of $f^2 =>0.35$ (Hair et al., 2017, pp. 216). The results are shown in Table 4.15 which are H1, H2, H3, H4, H5 with their F^2 values. H1 is considered as weak because it falls in 0.02 to 0.15 interval while H3 is a medium effect in producing R^2 to Outcome with the value of 0.182. Lastly, H2 falls in 0.35 and above interval with the value of 0.502. So, Consumer Characteristics has a strong effect on producing R square to *trust*.

6. DISCUSSION

This paper includes some important parts that indicates the implication of this study, limitations, suggestions for potential enhancements in the future, and overall conclusion of the study.

As a new technology, cloud computing has a major effect on businesses as it makes it possible to store information on multiple servers and allow on-demand access to users, companies and governments. Cloud storage provides users with great benefits to both end users and businesses of all sizes. These benefits are but not limited to cost efficiency, convenient resource availability, backup, recover, robust, scalability, performance, quick deployment, easy integration, multiple

location, device diversity and location independence. With these great benefits, there are some disadvantages like security issues, privacy issues, vendor lock-in, downtime, limited control, technical complexity and susceptibility.

Many organisations are currently not inclined to use cloud services since *trust* is a serious issue avoiding to share sensitive information to cloud service providers who are owning full access. Cloud service consumers believe that cloud service providers should apply proper mechanisms for detecting and preventing security threats.

Furthermore, DeLone and McLean Information System Success theory has been selected for the theoretical framework. This model is used to help for the evaluation of cloud service users usability success and find out whether *trust* has any influence on cloud service usage or not? Consumer characteristics which is usability has been checked to find out the Outcome with and without *trust*.

Moreover, a questionnaire was designed to carry out questions consist of the independent and dependent variables. The questionnaire was consisting of demographic section, and a section of cloud services related questions. After collecting the required number of responses, it has been converted to numeric to import to Statistical Package of Social Science (SPSS) and SmartPLS to analyze the purpose and achieve research objective accordingly. Assessment of reliability, assessment of normality and descriptive analysis have been done in SPSS. SmartPLS has been used for the model measurement.

7. Implication of the Study

In recent years, while users are using a variety of conveniently available cloud services, data protection has become an issue, especially with many privacy leak scandals such as images, videos and other personal information. It is important to take the applicable solutions in order to protect privacy and security in the cloud. The literature review of this paper will help providers and customers to find out the security and privacy risks as are currently present in computing systems. Meanwhile, this study will help cloud service users to find out about security issues, privacy and other problems related to their data misuse. So, they may be much carious to choose the proper cloud service provider and services.

As stated in the previous section, *trust* establishment by cloud service providers has positive effects on cloud services usage. Any effort by cloud computing providers to build *trust* reduces user concerns and pushes service providers closer to the *trust* and good reputation threshold. As we may know that *trust* cannot be purchased. Thus, providers and customers need to know about each other and reasons which are causing distrust among them. This study will help cloud service providers and developers to know the reasons why some people and organizations are not willing to use their services.

Additionally, the presented data and information in this research can be useful for other students and researchers for further study and investigation. This paper is to provide people who serve or use the concept and mentality of *trust* for the future needs.

8. Limitation and Recommendation for the Future Work

This study focuses on cloud service consumers. Due to the COVID-19 pandemic, access to cloud service providers organizations is deemed challenging. We believe that the collected responses from cloud service providers are not enough to know about their mechanism about trust establishment and necessary detective procedures for threats. Moreover, as we may know that we are not authorised to view the cloud providers' real environment. Because of given the in-depth nature of the data, research on a larger scale is very difficult to collect further data to achieve the best result from the cloud service providers side.

Another limitation is that data of this study have been collected from about 12 countries. So far, security issues are pointed out as bottleneck for the cloud services trust. Usage of cloud service may vary in other countries in term of use. Hence more data from different locations may result in usability, security, and maybe *trust*. Conversely, usability of cloud could services and other related objectives can be examined for further results in the future.

Unfortunately, *trust* between cloud service providers and end-users is still a concern that needs more research. According to the survey done by Tripathi and Sehgal in 2015 and found out that organizations, government authorities, and end-users are using cloud computing services rapidly. However, *trust* is still a major issue in a cloud computing environment. Cloud service providers are keeping the private information of organizations and end-users. Due to this, nowadays, the trust issue is becoming important in a cloud computing environment. Many works have been done to find a solution and improve the acceptance of trust issues among end-users still a future work for some researchers. So, because of these security issues and threats, *trust* remains a barricade among providers and users.

9. Conclusion

Cloud Computing is in demand since it does not requires physical acquisition of computing systems. Therefore it saves individuals and organizations time and cost management. Typical perceived barriers in the adoption of cloud services include privacy and security issues. The main objective of this study is to evaluate *trust* among providers and consumers. This study concludes that *trust* has an enormous role in deployment, usage, and willingness to use these services. As we illustrated, distrust arises when cloud service consumers know that there is no full control over their information. Security and privacy are other issues that altogether affect the trust and outcome of cloud services.

Most IT organizations and other individuals will be using cloud services in the future. So, the user and provider need to trust each other. Furthermore, it is very important to achieve our main objective: *trust* to use cloud services. One of the reasons that users do not trust cloud service providers is existing threats. These threats cause unwillingness to use cloud services. This study found that *trust* plays an enormous role for cloud service users and providers because it increases usage, willingness to use, and cloud service providers' reputation. This study showed that the Outcome is really low if there is no trust in these services.

This study help cloud service providers/developers know why some people and organizations are unwilling to use cloud services. This study's theoretical

contribution is to give people who serve or use the concept and mentality of *trust*. Meanwhile, this study also help cloud service users find out about security issues, privacy, and other problems related to their data misuse. This study also collected data from providers and users. Still, I believe that cloud service providers' collected responses are not enough to know about their mechanism of trust establishment and necessary detective procedures for threats. Therefore, offered services to consumers should be secure, trusted, and the provider should have a good reputation in the market or among their customers.

REFERENCES

Adjei, J. K. (2015). Explaining the role of trust in cloud computing services. *Info*, 17(1), 54–67.

Ali, H. (2020). Key factors increasing trust in cloud computing applications in the Kingdom of Bahrain. *International Journal of Computing and Digital Systems*, 9(2), 309–317.

Aljazzaf, Z. M., Perry, M., & Capretz, M. A. M. (2010). Online trust: Definition and principles. *Proceedings - 5th International Multi-Conference on Computing in the Global Information Technology, ICCGI 2010,* (April 2014), 163–168.

Apuke, O. (2017). Quantitative research methods: A synopsis approach. *Arabian Journal of Business and Management Review (Kuwait Chapter)*. 6. 40-47.

Boeren, E. (2018). The methodological underdog: A review of quantitative research in the key adult education journals. *Adult Education Quarterly*, 68, 63-79.

Chin, Wynne. (2010). How to write up and report PLS analyses. *Handbook of Partial Least Squares*. 655-690.

Creswell, J. W. (2014). *Research Design: Qualitative, Quantitative and Mixed Methods Approaches (4th ed.)*. Thousand Oaks, CA: Sage.

Gefen, D.W., Straub M.-C. & Boudreau. (2000). "Structural equation modelling and regression: Guidelines for research practice", *Communications of the Association for Information Systems*, Vol. 4, 1 - 78.

Fornell, C. & Larcker, D.F. (1981) *J. Mark. Res.* 1 39-50.

Gokulnath, K., & Uthariaraj, R. (2016). A Survey on Trust Models in Cloud Computing. *Indian Journal of Science and Technology*, 9(47), 1–7.

Nunnally, JC. (1978). An overview of psychological measurement, B Wolman (Ed.), *Clinical Diagnosis of Mental Disorders: A Handbook*, Plenum Press, New York.

Kandel, C. S. (2017). Cloud-based Services Users and Trust Issues - A Comparative Study of Gender and National Culture Perspectives Chetan Sharma Kandel.

Mengistu, T., Alahmadi, A., Albuali, A., Alsenani, Y., & Che, D. (2017). A "No Data Center" Solution to Cloud Computing. *IEEE International Conference on Cloud Computing, CLOUD,* 2017-June, 714–717.

Patil, D., Patil, P., & Patil, P. (2017). Establishing Cloud Computing Security in trust-based Cloud Service Provider. *International Journal of Engineering Technology Science and Research*, 4(4), 166–168.

Pearson, S., & Benameur, A. (2010). Privacy, security and trust issues arising from cloud computing. *Proceedings - 2nd IEEE International Conference on Cloud Computing Technology and Science, CloudCom 2010,* 693–702.

Peng, D.X. & Lai, F. (2012), "Using partial least squares in operations management research: a practical guideline and summary of past research", *Journal of Operations Management,* Vol. 30 No. 6, pp. 467-480.

Prasad, V. K., Shah, M., Patel, N., & Bhavsar, M. (2018). Inspection of Trust Based Cloud Using Security and Capacity Management at an IaaS Level. *Procedia Computer Science*, 132 (Iccids), 1280–1289.

R. C. Mayer, J. H. Davis, and F. D. Schoorman. (1995). "An integrative model of organizational trust," *The Academy of Management Review*, vol. 20, no. 3, pp. 709–734, 1995.

Ramachandra, G., Iftikhar, M., & Khan, F. A. (2017). A Comprehensive Survey on Security in Cloud Computing. *Procedia Computer Science,* 110(2012), 465–472.

Ramayah, T., Hwa, C., Chuah, F., Ting, H. & Memon, M. (2018). *Partial Least Squares Structural Equation Modeling (PLS-SEM) using SmartPLS 3.0: An Updated and Practical Guide to Statistical Analysis*.

Sarstedt, M., Ringle, C., & Hair, J. (2017). *Partial Least Squares Structural Equation Modeling*. 10.1007/978-3-319-05542-8_15-1.

Shuaibu, H. U., Mohammed Abdullah Bawazir, & Kabir, A. M. (2014). Cloud Computing: A Strategy to Improve the Economy of Islamic Societies. *International Journal of Computer Trends and Technology (IJCTT),* 9(7), 387–392.

Singh, M. (2015). Study on cloud computing and cloud database. *International Conference on Computing, Communication and Automation, ICCCA 2015*, 708–713.

Tawalbeh, L., Darwazeh, N. S., Al-Qassas, R. S., & AlDosari, F. (2015). A secure cloud computing model based on data classification. *Procedia Computer Science,* 52(1), 1153–1158.

Tripathi, M. K., & Sehgal, V. K. (2015). Establishing Trust in cloud computing security with the help of inter-clouds. *Proceedings of 2014 IEEE International Conference on Advanced Communication, Control and Computing Technologies, ICACCCT 2014*, (978), 1749–1752.

Wong, K. K. K.-K. (2013). Partial Least Squares Structural Equation Modeling (PLS-SEM) Techniques Using SmartPLS. *Marketing Bulletin*, *24*(1), 1–32.