*Journal of Computer Sciences and Applications, 2018, Vol. 6, No. 2, 69-74*
Available online at http://pubs.sciepub.com/jcsa/6/2/3

DOI:10.12691/jcsa-6-2-3

# Trust and Continuous Deployment of Cloud Computing: A Quantitative Analysis

**Kunle Elebute***

Department of Computer Science, Software Development and Security, University of Maryland University College, Largo, USA
*Corresponding author: princekay123@gmail.com

*Received July 07, 2018; Revised August 20, 2018; Accepted September 07, 2018*

**Abstract** In recent time, many studies have investigated the criteria that should guide a user when selecting a trustworthy cloud service provider. Similarly, factors influencing the user's decision to adopt cloud computing have been exhaustively discussed. However, it is still unclear if there is a correlation between a user's trust in the capability of a cloud provider and the user's decision to continuously deploy cloud computing. Using a multinomial logistic regression, this study analyzed responses from 176 information technology managers who were currently using cloud computing as at the time of the study. Results from the data analysis indicated a negative relationship between a user's trust in the capability of a cloud provider and the user's decision to continuously deploy cloud computing. Consequently, a cloud user who does not trust the capability of a cloud provider will be unwilling to continuously deploy cloud computing regardless of the benefits of the cloud platform. This study recommended a synergy between cloud users and cloud providers to bridge trust gaps and develop security plans and policies that will effectively tackle cyber-threats.

***Keywords:*** *cloud computing, trust, cloud provider, security, cyber-threats, multinomial logistic regression, cloud deployment*

**Cite This Article:** Kunle Elebute, "Trust and Continuous Deployment of Cloud Computing: A Quantitative Analysis." *Journal of Computer Sciences and Applications*, vol. 6, no. 2 (2018): 69-74. doi: 10.12691/jcsa-6-2-3.

## 1. Introduction

Since cloud computing evolved in the mid-2000s, many organizations have deployed it because of the benefits the platform offers compared to conventional hardware that is laced with horrendous maintenance hazards and expenses [1,2]. Aside from the pay-as-you-go nature and lower cost of setup, users have identified flexibility, scalability, convenience, compatibility, wide accessibility, and better performance as the enticing features of cloud computing [3,4,5]. However, cloud computing is not entirely safe from cyber-threats and security vulnerabilities [6]. Thus, the majority of cloud users are alarmed about the safety of cloud-stored data and will only trust a cloud service provider with a track record of secured cloud platforms.

The ability of cloud service providers to effectively manage user's trust in their capabilities to manage and resolve issues within their cloud platforms is a crucial strength that majority of cloud users treasure [7]. Thus, one of the most important questions technology suppliers, especially cloud service providers, desire an immediate answer to is: Will cloud users continue to use cloud computing if they do not trust the capabilities of cloud providers to keep the cloud safe?

To answer this question, it is imperative to understand what actions or inactions of the cloud service provider will help build trust and loyalty of the cloud users on their level of competence in providing solutions to security-related issues in the cloud. Many external factors beyond the control of the provider may cause dissatisfaction (to users) and eventually discourage users from developing trust in the capability of the cloud provider [4]. Importantly, however, most cloud users have trust issues because of the incompetence or failure of the cloud service provider to adequately address security vulnerabilities that expose cloud users to threats such as data theft, cyber-attacks, and external intrusions.

The purpose of this study was to investigate if there is a relationship between a user's trust in the capability of a cloud provider and the user's decision to continuously deploy cloud computing. Recent studies have failed to scrutinize if at all there is a relationship between a user's trust in the capability of a cloud provider and the user's decision to use cloud computing. This study fills this gap in knowledge and also created an opportunity for further research on the impact of trust on the user's continuous use of cloud computing.

## 2. Literature Review

This section discussed the nature of cloud computing as a new technology and the concept of trust and relationship building in the context of cloud adoption. It also explored factors that promote trust-building between a cloud service provider and the cloud users.

## 2.1. Cloud Computing

Cloud computing is a relatively new technology that has been widely described as a virtual platform that is provided on-demand, conveniently distributed, flexible in application, and accessed over the internet [8]. Unlike physical servers, cloud computing can be accessed from anywhere through internet connectivity and from almost any kind of device, including mobile and personal computers [9]. The use of cloud computing has improved the operations of many businesses and provided comparative advantage such that firms could save on the cost of maintenance, upgrade, migration, data protection, and data security [10]. However, security vulnerability and compatibility of cloud platforms with internal applications of most users have been a barrier to the use of cloud technology [11,12].

There are four popular deployment models of cloud computing, namely: public, private, community, and hybrid cloud models [13]. The public cloud is a platform available for general use whereas a private cloud is a customized platform for dedicated use of a particular customer [9]. A hybrid cloud is a combination of both public and private cloud while a community cloud is a shared computing platform for several organizations with common concern [12]. Cloud computing has three service models: software-as-a-service, platform-as-a-service, and infrastructure-as-a-service [8]. The SaaS platform allows users to run software over the internet, e.g. CRM applications [14]. The PaaS platform allows users to deploy applications but they do not fully control the underlying architecture, e.g. Google WebApps [6]. Finally, the IaaS platform provides access to all the infrastructure the users need, but all the resources are still managed by the cloud service provider, e.g. Amazon EC2 [15].

## 2.2. Trust and Relationship Building

Trust is a word that relates to the mutual confidence in a relationship between two parties [16]. Thus, the concept of trust revolves around relationships between a "trustor" and "trustee" [4]. In information technology, the trust could be described as a faith in the credibility of another entity, party, group, or process. Thus, a trust can be built, gained, or destroyed [17]. When a trust is built, both parties enjoy the mutual relationship and this promotes better productivity and teamwork [16]. In their study, [4] stated that trust can also be established between a machine and human. When such a trust level is established, a user becomes addicted to the trusted machine.

There is also a connection between trust and commitment. In their research, [16] conducted a research on the influence of trust and commitment to team working in virtual organizations. The study found that organization efficacy is powered by high trust level within virtual teams. Thus, low commitment level leads to lower trust level at both personal and organizational level.

## 2.3. Factors Affecting User's Trust in CSP

In the context of cloud implementation, trust is established between a cloud service provider and a user when the cloud user sees value in the services provided by the cloud provider. Many studies have given different explanations for what determines trustworthiness and what actions a cloud provider can perform to build user's trust. Based on recent literature, cloud service providers can establish trust of their cloud infrastructure users by delivering five crucial services to customers: a secured cloud platform, automation tools, effective auditing or activity monitoring, continuous user training, and efficient feedback system to capture user complaints.

Security of the cloud platform is one of the key factors that affect a user's trust in the capability of a cloud service provider [18]. Delivering a secured cloud platform will not only build trust but will equally guarantee loyalty and trust from cloud users [15]. Studies have shown that security of data is a great concern for the majority of cloud users [6,19,20]. [21] emphasized the importance of security, privacy, and trust to users interested in deploying mobile cloud. Evaluating 30 mobile computing architecture literature, the study found that 22% of the research identified security, privacy, and trust as a major concern to mobile cloud users. Therefore, cloud users tend to develop trust when they believe their data stored on the cloud are safe from unauthorized invasion and breaches.

Another strategy for trust building is automation and flexibility in the use of cloud platform. According to [6], convenience and flexibility is a feature of cloud computing that attracts users to cloud computing. Therefore, cloud service providers need to develop automation tools that will be convenient and easy to use for customers. Providing platforms with credible tools and mechanisms that will help customers "automate the process of managing, maintaining, and securing the infrastructure" [22]. [4] also listed flexibility to meet customer need as an important criterion for building trust and for selecting a cloud service provider.

A constant and effective auditing and activity monitoring of the cloud platform will assist cloud service providers to build trust and loyalty from the customers [23]. Most cyber-threats and attacks are a result of security vulnerabilities that allow intruders to have unauthorized access to the cloud platform [6]. The situation is worse on the cloud platform since users do not have full control of their virtual servers. In their study, [24] advocated for effective monitoring applications or programs that will constantly monitor activities and prevent security breaches on the cloud platforms. With the provision of activity monitoring applications that regularly scan for intrusions, cloud providers will earn the trust of their clients.

Cloud service providers need to educate their clients about the inner workings of the cloud technology as well as the risks users could face while using the technology. For instance, Amazon which is a leading cloud service provider conducts annual user training, conferences, and on-the-site support service to address concerns of users and keep them up to date with new tools and technologies.

Finally, cloud service providers can build trust with their customers by providing a feedback mechanism through which the cloud service providers can receive user's complaints and comments. In a study, [18] developed a trust model that will entail collecting feedback from the users regarding the quality of services received. In the business of cloud hosting, "trust" is

connected to security, confidentiality, and privacy [24]. Users must be able to give feedback on how the services they receive meet their needs.

### 2.4. Managing Trust Issues as a CSP

The process of managing trust involves establishing and maintaining a relationship. Cloud service providers can manage trust in their capabilities by ensuring there is a healthy relationship with their clients. In a study, [25] proposed a trust-enabling framework to help providers build trust and reputation. The framework requires building trustworthy application models that users "can trust and willing to use" [25].

In another study, [24] proposed a trust-enhancing safety mechanism to be implemented by cloud providers to combat security vulnerability fears of cloud users who have to migrate their data to the cloud. This mechanism includes constant monitoring of activities using a load balancing technique to detect any anomaly and take proactive actions to remedy a breach in order to gain end user's trust. Findings of the study indicated that user's trust in a cloud service provider is largely dependent on the safety strategies built and implemented by the cloud provider.

In their study, [26] presented a strategy that will help organizations select a trusted cloud provider for their SaaS cloud platform. Exploring the security challenges in SaaS platforms, the study identified data privacy issues as the top concern for 49% of the respondents that participated in the study. Trust, according to the study, develops when there is less concern about security challenges on the cloud platform. Thus, the study proposed a checklist of four security controls – function, auditability, governability, and interoperability (FAGI) – that cloud service providers must meet before building credibility and enjoying the trust of the cloud users.

Furthermore, [27] investigated the root cause of trust issues between cloud user and cloud service provider. The study proposed a multi-faceted trust management strategy to provide support for users in recognizing credible cloud service provider. The trust management framework championed by [27] involves an instrument for evaluating security components and determine the trustworthiness or credibility of cloud providers. This model is similar to a framework proposed by [4], which is a feedback service model aimed at measuring the trust of cloud services for educational institutions.

### 2.5. Theoretical Framework

The theoretical background of this study is the technology acceptance model (TAM). Developed in 1986, the TAM theory explored factors that control consumer's acceptance of new technology [28]. In a research, [29] identified two assumptions for the TAM model:

1. Users are inclined to use technology if there is a perceived benefit for using it; and
2. Users are inclined to use new technology if there is a perceived ease of use [30].

The first principle of TAM framework is benefits. The model states that users are influenced by the benefits they derive from using a new technology, so the acceptance of new technology depends on how the product improves them [31]. The second principle defined user's motivation to use new technology in terms of the convenience or ease of use [28]. Thus, according to the TAM framework, the attraction for new technology is governed by the user's perception of benefits and ease of use.

The two principles in the TAM framework (benefits and convenience) are applicable to this study because, as discussed earlier, a user's trust in the capability of a cloud service provider depends on the exceptional service from the cloud provider. When a user derives benefit and convenience from the services provided (cloud computing), that user will trust the technology offered by the provider and also trust the capacity of the cloud service provider to deliver. Conversely, a dissatisfied user who does not derive any benefit or convenience from the services rendered will likely find that provider untrustworthy.

## 3. Methodology

### 3.1. Research Question and Hypotheses

The research question this study will answer is:

RQ1: *To what extent does a user's trust on the capability of cloud service provider correlates with user's decision to continuously deploy cloud computing?*

This study proposed one null hypothesis and one alternative hypothesis:

$H_0$1: *User's trust in the capability of a cloud provider does not significantly correlate with the user's decision to continuously deploy cloud computing.*

$H_a$1: *User's trust in the capability of a cloud provider do significantly correlate with the user's decision to continuously deploy cloud computing.*

The null hypothesis will be tested using a multinomial logistic regression.

### 3.2. Research Design

This study was a quantitative nonexperimental correlational study aimed at investigating the relationship between a dependent variable (user's decision to continuously deploy cloud computing) and an independent variable (user's trust in the capability of a cloud service provider). The philosophical foundation for this study was positivism – the worldview that knowledge is derived purely from "data, evidence, and rational considerations" [32]. The epistemological worldview adopted for this study was empiricism – the position that knowledge is derived from experience and objects of knowledge are independent of the researcher [32,33].

The population for this study was IT managers who were using cloud computing as at the time this study was conducted. All the respondents were over 18 years of age and are located within the United States. The respondents were sourced through a private polling platform with a technical panel consisting of IT managers from different industries. The IT managers were preferred because they were believed to be decision-makers who will make decisions to adopt cloud computing at their respective organizations [6]. The sample size was calculated using a GPower 3.0 software.

The survey instrument used in this study was previously developed and validated by [20]. Two sections of the instrument titled "Privacy Risk" and "Continuance Intention" were used. After pilot testing, [20] posted a Cronbach's alpha of 0.975 and reliability coefficient of 0.983 for privacy risk while continuance intention had a Cronbach's alpha of 0.779 and reliability coefficient of 0.827. These values show high validity and reliability of the instrument because of the high Cronbach's alpha computation [20,34].

An online survey was used to collect data because of its speed and convenience [6]. The respondents were randomly selected from a pool of qualified participants registered with the panelist service. A mass email was sent to a list of pre-registered IT managers on the platform of the polling firm. The email had a link to the survey. Interested respondents voluntarily clicked the link to participate in the study. The survey contained 18 questions, which the majority of the respondents completed within 4 minutes. An informed consent form was included in the survey to protect the respondents. A total of 176 valid surveys were collected and processed.

### 3.3. Data Analysis

Data collected for this study was analyzed using a multinomial logistic regression (MLR) model. The MLR is a statistical analysis applicable when the response variable has more than two possible categories or outcomes [34,35,36]. The MLR statistical model has been repeatedly used by many researchers to define relationships between a multiple-output dependent variable and independent variables [37].

The MLR model was applicable to this study because of the polytomous nature of the dependent variable. The dependent variable (user's decision to continuously deploy cloud computing) had three possible outputs ("No", "Undecided", "Yes") and were coded as 1, 2, and 3 respectively in the IBM SPSS version 24 used for the data analysis. The independent variable (User's trust in cloud provider) had an ordinal data type and was measured using a 5-point Likert scale.

All the four major assumptions of a multinomial logistic regression were satisfied by this study. The first is that the dependent variable for this study has more than two possible output. Second, the two variables in this study were continuous. Third, there is a perceived linear relationship between the dependent and independent variables of this study and the final assumption, fourth, is that there were no outliers in the dataset. A threshold of $p < .05$ was set to determine the significant level [34]. The MLR analysis included a test of model fitness, coefficient of determination, and likelihood ratio tests.

## 4. Results and Discussion

### 4.1. Demographics of Respondents

In Table 1, the demographic distributions of all the 176 respondents were presented based on gender, age, education, job title, and size of firms where the respondents were employed as at the time this study was conducted. In the dataset, 57.71% of the respondents were male while the remaining 42.29% were female, which shows an evenly distributed demographics. The table also shows that the highest age range of the respondents was 30-39 years with a percentage of 51.70 of the total population sampled. Furthermore, the majority of the respondents had bachelor's degree as their highest educational level with a percentage of 57.95.

**Table 1. Profiles of Respondents**

| Profile | Sample | Frequency | Ratio (%) |
|---|---|---|---|
| Gender | Male | 101 | 57.71 |
| | Female | 74 | 42.29 |
| Age | 18-29 years | 39 | 22.16 |
| | 30-39 years | 91 | 51.70 |
| | 40-49 years | 31 | 17.61 |
| | 50-59 years | 10 | 5.68 |
| | 60 years and above | 5 | 2.84 |
| Education | High School | 23 | 13.07 |
| | Bachelor Degree | 102 | 57.95 |
| | Graduate School or Higher | 51 | 28.98 |
| Job Title | IT Manager | 81 | 46.29 |
| | Senior Manager | 38 | 21.71 |
| | IT Executive (CIO, CTO, etc) | 18 | 10.29 |
| | IT Director | 30 | 17.14 |
| | Other | 8 | 4.57 |
| Size of Firm | Less than 250 Employees | 44 | 25.43 |
| | 250 – 499 employees | 35 | 20.23 |
| | 500 – 749 employees | 31 | 17.92 |
| | 750 – 999 employees | 19 | 10.98 |
| | 1000 employees and above | 44 | 25.43 |

### 4.2. Descriptive Statistics

The descriptive statistics of the data set was computed to calculate the mean, standard deviation, variance, skewness, and kurtosis of the distribution. The essence of this process is to check the normality of the data [34,36]. Table 2 displayed the results of the descriptive (statistics) of the two variables in this study.

**Table 2. Descriptive Statistics**

| Variable | *M* | *SE* | *SD* | Variance | Skewness | *SE* | Kurtosis | *SE* |
|---|---|---|---|---|---|---|---|---|
| TCP | 3.650 | .081 | 1.079 | 1.165 | -.569 | .183 | -.490 | .364 |
| DCC | 1.620 | .062 | .817 | .668 | .809 | .185 | -1.019 | .367 |

### 4.3. Hypothesis Testing

Table 3 displayed the overall measure of the MLR model, which is expected to show if the coefficients of the model were statistically significant. Results from the data analysis show a final sig column with $p = .000$, which implies that the full model fits the data well and is statistically significant. The results displayed in Table 3 indicated that the final model was significant, $\chi 2 = 31.719$ (8), $p < .000$, which implies that the independent variable (user's trust in the capability of cloud service provider) significantly predicted the dependent variable (user's decision to continuously deploy cloud computing) better than the intercept-only model.

**Table 3. Model Fitting Tests**

| Model | Model fitting criteria | Likelihood ratio tests | | |
|---|---|---|---|---|
| | -2 log likelihood | Chi-square | *df* | Sig. |
| Intercept-only | 57.711 | | | |
| Final | 25.992 | 31.719 | 8 | .000 |

A goodness of fit model was used to determine the difference between observed and expected probabilities [38]. Information from Table 4 presented the statistical data of the goodness of fit results for the research question examined in this study. The result shows that: Pearson $\chi^2$ =.000, (0), $p$ = .00, which implies that the result was significant since $p$ > .05. Therefore, the model was a good fit.

**Table 4. The Goodness of Fit Tests**

| Test | Chi-square | *df* | Sig. |
|---|---|---|---|
| Pearson | .000 | 0 | .00 |
| Deviance | .000 | 0 | .00 |

Finally, Table 5 displayed the likelihood ratio tests for the data analyzed. A likelihood ratio test measures the influence of the independent variable (user's trust in the capability of a cloud provider) on the model. As displayed in Table 6, the user's trust in a cloud provider (TCP) had a value of $p$ = .000, which was statistically significant. Therefore, the independent variable was a significant predictor of the dependent variable in the model.

**Table 5. Likelihood Ratio Tests**

| Effect | Likelihood ratio tests | | | |
|---|---|---|---|---|
| | Model Fitting Criteria -2 Log Likelihood of Reduced Model | Chi-square | *df* | *p* |
| Intercept | 25.992 | .000 | 0 | . |
| TCP | 57.711 | 31.719 | 8 | .000 |

## 4.4. Discussion

The null hypothesis ($H_0$1) for this study stated that there is no correlation between a user's trust in the capability of a cloud provider and the user's decision to continuously deploy cloud computing. Results from the data analysis (chi-square test of independence) show $\chi 2$ = 31.719 (8), $p$ < .000, which is a statistically significant result that provided statistical support to reject the null hypothesis. This result has a p-value ($p$ = .000) that was less than the established threshold ($p$ < .05). Therefore, this study rejects the null hypothesis. The data analysis provided a statistically significant basis for the position that there is a significant relationship between a user's trust in cloud service provider's capability and the user's decision to continuously deploy cloud computing.

The implication of these results is that there is a significant negative relationship between a user's trust in the capability of a cloud provider and a user's decision to continuously deploy cloud computing. Thus, any occurrence of a breach of trust by a cloud provider can significantly influence the user's decision to continue to deploy cloud products provided by that particular service provider. This results resonated with many of the findings discussed earlier in the literature review.

# 5. Conclusion

This study concludes that trust is a crucial factor when choosing to adopt or continue to use a new technology like cloud computing. Many studies have shown that trust is the key criterion that cloud users should include in their evaluation checklist while shopping for a cloud service provider. This particular study aimed to extend this further by investigating if at all there is a correlation between user's trust in a cloud provider and user's decision to use cloud computing.

This study will benefit both the cloud service providers and cloud users. Cloud service providers need to understand that being trustworthy will increase the loyalty of cloud users as noted by [24]. Therefore, cloud service providers must strategically earn the trust of users by addressing security issues, making cloud platforms more robust and automated, actively monitoring activities to detect anomalies, and continuously educating users about cloud functionalities and flexibility. Importantly, user training must include security awareness and data privacy protection.

There were two limitations to this study. Firstly, the study did not exhaustively discuss all the root causes of trust concerns by cloud users; the focus of this study was security-driven trust concerns. Future study can expand this to capture non-security related trust issues cloud users experience when dealing with cloud service providers. Secondly, the respondents that participated in this study were restricted to information technology managers who were using cloud computing as when the study was conducted. Future study can explore a more robust population that will include both information technology managers and regular cloud users.

# References


[1] Lian, J. (2015). Critical factors for cloud based e-invoice service adoption in Taiwan: An empirical study. *International Journal of Information Management, 35*(1), 98-109.

[2] Shiau, W. L., & Chau, P. Y. (2016). Understanding behavioral intention to use a cloud computing classroom: A multiple model comparison approach. *Information & Management, 53*, 355-365.

[3] Hew, T. S., & Kadir, S. L. S. A. (2016). Predicting the acceptance of cloud-based virtual learning environment: The roles of self-determination and channel expansion theory. *Telematics and Informatics, 33*(4), 990-1013.

[4] Jabbar, S., Naseer, K., Gohar, M., Rho, S., & Chang, H. (2016). Trust model at service layer of cloud computing for educational institutes. *The Journal of Supercomputing, 72*(1), 58-83.

[5] Sabi, H. M., Uzoka, F. M. E., Langmia, K., & Njeh, F. N. (2016). Conceptualizing a model for adoption of cloud computing in education. *International Journal of Information Management, 36*(2), 183-191.

[6] Elebute, K. (2018). *Cyber-attack, intellectual property theft, and organizations' continuance intention to use cloud computing: A quantitative correlational study*. Dissertation, Capella University.

[7] Siadat, S., Rahmani, A. M., & Navid, H. (2017). Identifying fake feedback in cloud trust management systems using feedback evaluation component and Bayesian game model. *The Journal of Supercomputing, 73*(6), 2682-2704.

[8] Mell, P., & Grance, T. (2011). The NIST definition of cloud computing. *NIST Special Publication, 800*(145), 7.

[9] Ramachandran, M., & Chang, V. (2016). Towards performance evaluation of cloud service providers for cloud data security. *International Journal of Information Management, 36*(4), 618-625.

[10] Oliveira, T., Thomas, M., Baptista, G., & Campos, F. (2016). Mobile payment: Understanding the determinants of customer adoption and intention to recommend the technology. *Computers in Human Behavior, 61*, 404-414.

[11] Arpaci, I. (2016). Understanding and predicting students' intention to use mobile cloud storage services. *Computers in Human Behavior, 58*, 150-157.

[12] Ghorbel, A., Ghorbel, M., & Jmaiel, M. (2017). Privacy in cloud computing environments: a survey and research challenges. *The Journal of Supercomputing, 73*(6), 2763-28.

[13] Astri, L. Y. (2015). A study literature of critical success factors of cloud computing in organizations. *Procedia Computer Science, 59*, 188-194.

[14] Singh, A., & Chatterjee, K. (2017). Cloud security issues and challenges: A survey. *Journal of Network and Computer Applications, 79*, 88-115.

[15] Chiregi, M., & Navimipour, N. J. (2016). Trusted services identification in the cloud environment using the topological metrics. *Karbala International Journal of Modern Science, 2*(3), 203-210.

[16] Crossman, A., & Lee‐Kelley, L. (2004). Trust, commitment and team working: the paradox of virtual organizations. *Global networks, 4*(4), 375-390.

[17] Ryzhova, S. V. (2017). Trust and ethnic tolerance in the face of social change. *Sociological Research, 56*(3), 197-217.

[18] Shaikh, R., & Sasikumar, M. (2015). Trust model for measuring security strength of cloud computing service. *Procedia Computer Science, 45*, 380-389.

[19] Halabi, T., & Bellaiche, M. (2017). Towards quantification and evaluation of security of Cloud Service Providers. *Journal of Information Security and Applications, 33*, 55-65.

[20] Yang, H., & Lin, S. (2015). User continuance intention to use cloud storage service. *Computers in Human Behavior, 52*, 219-232.

[21] Noor, T. H., Zeadally, S., Alfazi, A., & Sheng, Q. Z. (2018). Mobile cloud computing: Challenges and future research directions. *Journal of Network and Computer Applications, 115*, 70-85.

[22] Abbadi, I. M., & Martin, A. (2011). Trust in the Cloud. *Information Security Technical Report, 16*(3-4), 108-114.

[23] Rizvi, S., Karpinski, K., Kelly, B., & Walker, T. (2015). Utilizing Third Party Auditing to Manage Trust in the Cloud. *Procedia Computer Science, 61*, 191-197.

[24] 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*, 1280-1289.

[25] Moyano, F., Fernandez-Gago, C., & Lopez, J. (2013). A framework for enabling trust requirements in social cloud applications. *Requirements Engineering, 18*(4), 321-341.

[26] Tang, C., & Liu, J. (2015). Selecting a trusted cloud service provider for your SaaS program. *Computers & Security, 50*, 60-73.

[27] Chong, S. K., Abawajy, J., Ahmad, M., & Hamid, I. R. A. (2014). Enhancing trust management in cloud environment. *Procedia-Social and Behavioral Sciences, 129*, 314-321.

[28] Agag, G., & El-Masry, A. A. (2016). Understanding consumer intention to participate in online travel community and effects on consumer intention to purchase travel online and WOM: An integration of innovation diffusion theory and TAM with trust. *Computers in Human Behavior, 60*, 97-111.

[29] Davis, F. D. (1993). User acceptance of information technology: System characteristics, user perceptions and behavioral impacts. *International Journal of Man-Machine Studies, 38*(3), 475-487.

[30] Wallace, L. G., & Sheetz, S. D. (2014). The adoption of software measures: A technology acceptance model (TAM) perspective. *Information & Management, 51*(2), 249-259.

[31] Dibra, M. (2015). Rogers theory on diffusion of innovation: The most appropriate theoretical model in the study of factors influencing the integration of sustainability in tourism businesses. *Procedia Social and Behavioral Sciences, 195*, 1453-1462.

[32] Creswell, J. W. (2014). *Research design: Qualitative, quantitative and mixed methods approaches* (4th ed.). Thousand Oaks, CA: Sage Publications.

[33] Cooper, H. (2016). *Research synthesis and meta-analysis: A step-by-step approach* (5th ed.). Washington, DC: Sage Publications.

[34] Field, A. (2013). *Discovering statistics using IBM SPSS Statistics* (4th ed.). Thousand Oaks, CA: Sage.

[35] El-Habil, A. M. (2012). An application on multinomial logistic regression model. *Pakistan journal of statistics and operation research, 8*(2), 271-291.

[36] Vogt, W. P. (2007). *Quantitative research methods for professionals in education and other fields.* Boston, MA: Pearson Custom Publishing.

[37] Badri, M., Toure, F., & Lamontagne, L. (2015). Predicting unit testing effort levels of classes: An exploratory study based on multinomial logistic regression modeling. *Procedia Computer Science, 62*, 529-538.

[38] Goeman, J. J., & le Cessie, S. (2006). A goodness‐of‐fit test for multinomial logistic regression. *Biometrics, 62*(4), 980-985.