International Journal of Computing and Digital Systems
ISSN (2210-142X)
Int. J. Com. Dig. Sys. 9, No.2 (Mar-2020)

http://dx.doi.org/10.12785/ijcds/090216

Key Factors Increasing Trust in Cloud Computing Applications in the Kingdom of Bahrain

Hayat Ali[1]

[1] *Department of Management Information Systems, Applied Science University, Aker, Kingdom of Bahrain*

Received 18 May. 2019, Revised 28 Dec. 2019, Accepted 26 Feb. 2020, Published 01 Mar. 2020

Abstract: During recent years, cloud-computing applications have been increasing. However, with this increase there are many concerns that affect the adoption of these applications. One of these is the perceived trust of users. This research investigates the factors that influence perceived trust in cloud storage based applications in the Kingdom of Bahrain. Toward this aim, this research followed a quantitative research approach where the main research strategy is based on the results of a questionnaire. Through the questionnaire, a proposed model was tested with 178 cloud storage application users in order to identify factors affecting their trust of cloud storage applications. The results revealed that security and reliability both directly affect users' trust in cloud storage applications. At the same time, backup and recovery, availability and cloud transparency all affect trust indirectly through security. The contribution of this research resides in proposing a new model of users' trust in cloud computing applications that can be added to other researchers' models in the field. In addition, the results of this research provide insights for the developers of cloud computing applications toward better perceived trust by users.

Keywords: Cloud Computing, Cloud Storage, Trust, Privacy, Security, Availability, Reliability

1. INTRODUCTION

Nowadays, with the widespread use of Internet-based systems and distributed applications, a revolution toward adopting cloud computing-based application has been triggered. Around the end of 2007, IBM adopted the cloud computing paradigm, followed by other companies such as Google (Google App Engine), Amazon (Amazon Web Services (AWS), EC2 (Elastic Compute Cloud) and S3 (Simple Storage Service). Apple (iCloud) and Microsoft (Azure Services Platform) have progressively embraced it and have introduced their own new products based on cloud computing technology [1].

Cloud computing is a model that enables ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources including network, server, storage, application and services, with minimum management effort or service provider interaction [2].

Reference [3] also claims that the cloud is a style of computing where massively scalable and flexible IT-related capabilities are provided "as services" to external customers using Internet technologies.

In spite of many advantages and increased popularity, cloud computing suffers from concerns over trust. Trust has been found to be one of the major challenges to the adoption of cloud computing, because mistrust affects users' decision to adopt, especially those users who have no direct control over their data lying in the cloud. Evaluating trust and its influence has therefore become a critical issue [4]. Reference [5] stressed that trust and security are two of the most critical obstacles for the adoption and growth of cloud computing today. Therefore, this research investigates the factors that influence perceived trust toward the adoption of cloud storage-based applications in the Kingdom of Bahrain.

This paper is organized as follows: first, an overview of cloud computing and storage is presented, including its status in the Kingdom of Bahrain; second, works on trust in cloud storage are reviewed; third, the trust model and hypotheses are presented; fourth, the research methodology is discussed; then the results are presented and discussed, ending with the conclusion and suggestions for future work.

E-mail: hayat.ali@asu.edu.bh

2. CLOUD COMPUTING AND CLOUD STORAGE

Reference [6] considers that cloud computing refers "to both the applications delivered as services over the Internet and the hardware and systems software in the datacenters that provide those services. The services themselves have long been referred to as Software as a Service (SaaS), so we use that term. The datacenter hardware and software is what we will call a "Cloud".

Reference [7] from the National Institute of Standards and Technology (NIST), USA presented five essential characteristics of cloud computing including on-demand self-service, broad network access, rapid elasticity and automatic resource optimization. They identified various service models of cloud computing, as follows:

- ***Cloud Platform as a Service (PaaS)*** through which the consumer deploys on to the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider of Infrastructure as a Service (IaaS).
- ***Cloud Software as a Service (SaaS)*** through which the customers can use only the provider's applications running on a cloud infrastructure ***without*** managing or controlling the underlying infrastructure including network, servers, operating systems, storage, or even individual application capabilities.
- ***Cloud Infrastructure as a Service (IaaS)*** through which the customer is provided with processing, storage, networks, and other fundamental computing resources which they are ***able to deploy*** to run arbitrary software, including operating systems and applications.

The cloud storage that is the focus of this research is an IaaS model, defined by Reference [8] as a service that maintains data, manages and backs it up remotely and makes it available to users over the network (via the Internet). Many providers offering free space as a cloud storage infrastructure, including DropBox, Google Drive, Box, Amazon, Apple Cloud and Microsoft SkyDrive.

Reference [9] identified many advantages of using cloud storage, including ease of management, cost effectiveness, lower impact of outages and upgrades, disaster preparedness, and simplified planning. Reference [10] described the main benefits of cloud storage as: "no need to invest any capital on storage devices, no need for technical expert to maintain the storage, backup, replication and importantly disaster management, allowing others to access your data will result with collaborative working style instead of individual work". They emphasized that although cloud storage offers a reduction in the capital investment cost, customers might still face some of the technical, integration, security and organizational issues at various levels that might hinder them using cloud storage. Reference [11] pointed out that trust is a critical obstacle for the adoption of cloud computing; it is the focus of this research.

3. CLOUD COMPUTING IN THE KINGDOM OF BAHRAIN

The Government of the Kingdom of Bahrain is committed to modernizing government ICT and leading by example in its use of cloud computing services [12]. Reference [13] stated that the government cloud is to be established initially on national data center assets (adapted for the cloud through virtualization) and connected through existing network infrastructures such as the GDNs, as well as the Internet. All future government projects should follow a clear direction to move to the cloud as stipulated by the government-approved cloud-first policy; this uses Amazon Web Services (AWS), as the leader for the seventh consecutive year in Gartner's IaaS Magic Quadrant [12]. Bahrain has adopts the cloud-first approach to reduce the cost of government ICT, increase security by using accredited platforms, increase productivity and agility, and improve citizen services [14].

4. TRUST CONCEPT IN CLOUD COMPUTING

The Oxford English Dictionary in 1971 defined trust as "confidence in or reliance on some quality or attribute of a person or thing, or the truth of a statement'. Reference [15] described trust as:

A mental state comprising: (1) expectancy - the trustor expects a specific behavior from the trustee (such as providing valid information or effectively performing cooperative actions); (2) belief - the trustor believes that the expected behavior occurs, based on the evidence of the trustee's competence, integrity, and goodwill; (3) willingness to take risk - the trustor is willing to take risk for that belief.

In cloud computing, Reference [16] explained that the term "trust" is often loosely used in the literature on the cloud as a general term for "security" and "privacy. Reference [17] referred the trust in cloud computing as "a measure of reputation of the specific CSP (Cloud Service Provider) which has some set of resources for users". They stated that there are various categories of trust in cloud computing, including reputation-based trust, SLA (Service Level Agreements) verification-based trust, policy-based trust, evidence-based trust and societal trust. Reference [18] discussed two types of trust which they described as hard and soft. Hard trust has attributes such

as “authenticity, encryption, and security” whereas soft trust refers to “human psychology, brand loyalty, and user-friendliness”. This research concerns about hard trust.

5. FACTORS AFFECTING TRUST IN CLOUD STORAGE

Reference [19] viewed trust as a measurable belief that utilizes experience to make trustworthy decisions, where trust is a social rather than the technical issue that Reference [20] stressed. The component of trust is an essential element in the wide use and implementation of cloud services [4]. Reference [21] explained that the one effective way to encourage the use of cloud technology is to reduce undesirable, yet possible behaviors via perceived trust of cloud technology. Reference [4] pointed out that in cloud computing scenarios, the cloud service users (CSU) put their digital resources in the hands of the cloud service providers (CSP), giving the CSP control over almost all the security factors; this implies that the CSP must indicate a proper level of trust if the CSU’s perceived trust is to result in their adoption of cloud services.

Many researchers have investigated the factors that affect trust in cloud storage. Reference [22] for example, pointed out that trusting in the online context was not a priority for many online users during the past decade. He stressed that unlike offline trust, online trust depends on the Internet and associated technologies. Technological determinants of online trust may include security features, privacy protection mechanisms, ease of use and system reliability.

On the other hand, Reference [23] stated that cloud computing was introduced as one of the most promising issues in Information and Communication Technology (ICT). They stressed that when user-critical data or resources are on the cloud, there should be a mechanism provided by the CSP to take care of accountability, privacy, auditability, reliability, security, data location, investigation, data segregation, integrity, backup and recovery, and privileged user access, as these elements can have a major impact on the level of user trust in the cloud.

Reference [24] who pointed out that cloud computing delivers to organizations an on-demand service wherever it is needed that can be evaluated by many factors, including cost/benefit ratio, speed, required capacity, and whether data is regulated. They emphasized that organizations should pay close attention to reliability, security and the user’s requirements in order to gain customer trust. They introduced a trust model between user and cloud provider that measures three aspects of trust: service level agreement (SLA), cloud computing knowledge, and background of cloud and security.

Reference [25] drew attention to a different side of cloud computing trust, pointing out that auditors need to be involved with their organization’s cloud computing plans from the conception stage onwards, to help ensure the identification and mitigation of risks. They added that factors like security, standards in the cloud computing environment, performance issues, data migration, data management, availability and cloud transparency can affect user satisfaction.

Reference [26] suggested that the establishment of trust is based on the experience collected from previous interactions of entities. They pointed out that trust is related to the certainty that attributes such as honesty, dependability, timeliness, security, competence, reliability and truthfulness will perform as expected.

Also, Reference [27] pointed out that a high level of availability is probably one of most important driving forces behind switching to the cloud. Thus, end-user usage scenarios and service functionality have a direct impact on end-user availability requirements and expectations; availability in the broader picture can affect the security level of the overall cloud.

Reference [28] suggested many factors that should be taken into consideration in providing a trusted platform in the cloud, including confidentiality, data confidentiality, software confidentiality, privacy or security, data integrity, availability and data location.

Reference [4] saw trust as a social problem, not a purely technical issue. They presented the following trust elements of cloud service use that can affect user trust: location of stored data, data to be investigated, sharing of data, availability of service, long-term viability, compliance regulation and audit, backup and recovery of data, user access privileges, governance, transparency, effect of expired use, evaluation of trust based on records, repetitive access to cloud resources by users and actions based on analysis. Table 1 below summarizes the research reviewed.

TABLE I. **REVIEWED RESEARCH**

Authors	Research Title
Ritua, Randhawab, S., and Jainc. S. (2017)	Trust Models in Cloud Computing: A Review.
Kalloniatis, C. (2016)	Increasing Internet Users Trust in the Cloud Computing Era: The Role of Privacy
Darsi, P., Babu D, V., and Darsi, G. (2014)	Addressing Trust Issues in Cloud Computing
Uikey,C., and Bhilare, D. (2013)	A Broker Based Trust Model for Cloud Computing.
Manuel, P. (2013)	A Trust Model of Cloud Computing Based on Quality of Service
Rashidi, A and Movahhedinia,N. (2012)	Key Factors Increasing the Trust and Intention to Adopt Standard Cloud-Based Applications
Meixner,F., and Buettner,R. (2012)	Trust as an Integral Part for Success of Cloud Computing
Ahmad, S., Ahmad,B., Saqib, S.M and Khattak,M. (2012)	Cloud's Provider and Cloud's User

6. RESEARCH MODEL AND HYPOTHESES

Based on the literature review, we developed the model depicted in Figure 1.

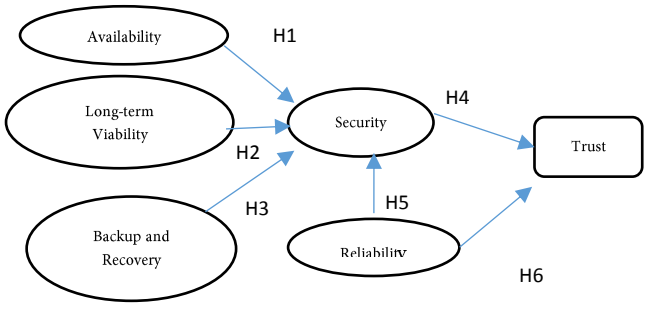

Figure 1. Resaech Model

The model shows six constructs, which are discussed below.

Availability

Reference [4] pointed out that users need their data to be available at all times on the cloud. Reference [23] stressed that cloud availability is an important issue and that access should be possible whenever requested. Reference [23] claimed that availability and security are inter-linked as security is tightly connected to availability and its components, such as incident management, monitoring and data access. Reference [28] also stressed that authorized users must be able to access their data via all resources, software and hardware, once they have logged in successfully. Reference [29] stressed that availability is one of the most critical information security requirements in the cloud. Accordingly, the following hypothesis is stated:

H1: Availability is positively related to security in cloud computing.

Long-term viability

Reference [4] claimed that users require their data to be viable for a long time, so they cannot afford the service going down or anything happening to their data. Reference [3] confirmed that long-term viability is an important issue that affects security. Reference [30] agreed that security is related to the long-term viability of cloud computing, stressing that there should be a guarantee of data availability in the event of the service provider's bankruptcy or acquisition. Based on this, the following hypothesis is proposed:

H2: Long-term viability is positively related to security in cloud computing.

Backup and Recovery

Reference [4] proposed that users' data may be lost in the case of a disaster. Therefore, they proposed that the cloud provider must have techniques to recover data following a disaster or any circumstances leading to data loss. Reference [3] stressed that if a failure does occur with the cloud, it is critical to completely restore clients' data. As clients prefer not to let a third party control their data, this will cause an impasse in security policy in these challenging situations. Accordingly, the following hypothesis is stated:

H3: Backup and recovery is positively related to security in cloud computing.

Security

Reference [31] indicated that security concerns the confidentiality, integrity and availability of data or information, while Reference [25] pointed out that cloud security refers to policies, technologies and controls deployed to protect applications, data and associated infrastructure of cloud computing. Security plays a central role in preventing service failures and cultivating trust in cloud computing [32]. Therefore, the following hypothesis is stated:

H4: Security is positively related to the user's trust in cloud computing.

Reliability

Reliability refers to the belief that the cloud storage provider will do what it says it will do, that it acts consistently and dependably [33]. Reference [34] claimed that reliability is an important component of trust and referred reliability to the ability of a system or component to perform its required functions or operations under stated conditions for a specified period of time. Reference [5] also stressed that reliability contributes to establishing

trust in cloud services. A high level of trust and reliability has to be established because if the third party does not provide the correct means then it may lead to the information and data of a party being insecure [35]. Accordingly, the following hypotheses are stated:

H5: Reliability is positively related to security of cloud computing

H6: Reliability is positively related to the user's trust in cloud computing.

7. RESEARCH METHODOLOGY

Instrument Development

In order to investigate factors affecting users' perceived trust of cloud storage-based applications, quantitative research was conducted with data collected through a questionnaire. This consisted of three sections: personal information of the users, usage of cloud storage applications, and factors that affect the user's trust of cloud storage applications; a 5-point Likert scale was used, indicating strongly agree = 1 to strongly disagree = 5. The items for each of the seven variables shown in Figure 1 were derived from the literature.

Analysis of data

The data were analyzed using the Statistical Package for Social Sciences (SPSS). Multiple regression analysis was conducted, in addition to reliability and validity tests. The results provide the foundation for accepting or rejecting the hypotheses and answering the research question.

Research Sample

The population of this research is the users of cloud storage applications, and the sample was selected randomly. A total of 178 responses were collected. Table 2 shows the number of responses by gender and level of study; 38.8% of respondents were male, and level of education, which was subsequently found to be significantly correlated with users' trust in cloud storage applications, was predominantly undergraduate (72.5%).

TABLE II. DEMOGRAPHIC INFORMATION OF PARTICIPANTS

Demographic Profile		Percent (%)
Gender	Male	38.8
	Female	61.2
	Total	100.0
Level of Education	Secondary School Certificate	16.3
	Diploma Certificate	2.8
	Bachelor Degree	72.5
	Master Degree	5.6
	PhD	2.2
	Other	.6
	Total	100.0

Validity and Reliability Test

Most exponents extracted have a value of 0.5 and above [36] which is indicates internal consistency and proves that items are valid; one item whose value was less than 0.5, data location, was dropped. Table 3 presents the Cronbach's Alpha values for each factor accepted, ranging from 0.705 to 0.952. Long-term viability of 0.677 was also accepted [37].

TABLE III. **CRONBACH'S ALPHA FOR EACH FACTOR**

Factors	**Cronbach's Alpha**
Availability	.709
Long Term viability	.677
Backup and Recovery	.759
Security	.806
Cloud Transparency	.808
Reliability	.758
Trust	.728

8. Results Analysis

Usage of Cloud Storage Applications

Figure 2 shows the types of cloud storage used, based on the collected data. Drop Box is the most popular, used by 78.1% of respondents, followed by Google Drive at 57.9%. There was only one user of Flip Drive (0.6%).

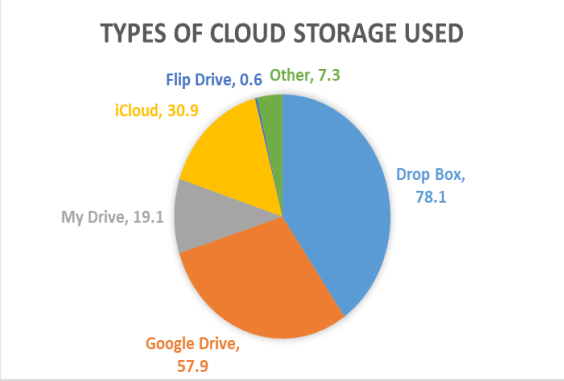

Figure 1. Types of cloud storage used

As the control of these applications is on the side of third party where the users' control is minimized, the users' trust level is affected. Therefore, the trust is an important aspect to be considered in the cloud storage environment specially that security threats are increasing making issues of security and trust the most important issues to focus on which have only been partially solved so far [5].

For the length of experience with cloud storage applications, the results indicate that the largest group is those with two or more years (60.7%). Only 9.6% have less than three months' experience.

For the usage of cloud storage, Figure 3 shows that 67.4% of users employ it for backup, followed by 62.4% for file sharing. Collaboration, at 20.8%, was the least popular use. The results show that file sharing and synchronization with other devices are both significantly correlated to trust; the other purposes were found not to be significantly correlated to trust.

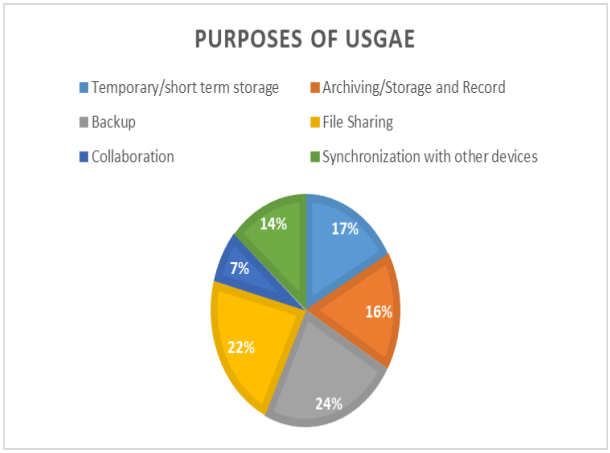

Figure 2. Purpose of use

In light of the results presented in Figure 3, the trust on cloud storage applications needs to be highly leveraged as it is mainly used for backup purpose. Thus, some mechanisms and factors needs to be considered so to play vital role in minimizing the negative perceived factors as well as to maximize the positive expectation toward better trust and adoption of these applications.

Hypothesis Testing

The regression analysis model in Table IV shows Availability, Long-Term Viability, Backup and Recovery, and Reliability as independent variables, and Security as the dependent variable, in line with hypotheses H1, H2, H3 and H5.

TABLE IV. **Coefficient values for Regression Model 1**

Coefficients[a]						
Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	.208	.315		.661	.510
	Availability	.163	.074	.156	2.203	.029
	Long Term Viability	.090	.075	.095	1.200	.232
	Backup and Recovery	.147	.065	.170	2.245	.026
	Reliability	.305	.075	.303	4.063	.000
a. Dependent Variable: Security						

Table IV indicates that all independent variables except Long-Term Viability have an effect on Security, significant at the P < 0.05 level.

Regression analysis model 2 in Table V shows that Security and Reliability (independent variables) have a significant effect on Trust (dependent variable) (P value < 0.05), reflecting hypotheses H4 and H6.

TABLE V. **COEFFICIENTS VALUES FOR REGRESSION MODEL 2**

Coefficients[a]						
Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
2	(Constant)	.566	.225		2.518	.013
	Security	.433	.061	.428	7.102	.000
	Reliability	.440	.061	.432	7.165	.000

Table VI summarizes these results from SPSS, according to which the hypotheses are accepted or rejected.

TABLE VI. **SUMMARY OF THE HYPOTHESIS RESULTS**

Hypotheses	Accepted/Rejected
H1: Availability is positively related to Security in cloud computing.	Accepted
H2: Long-term viability is positively related to Security in cloud computing.	Rejected
H3: Backup and Recovery is positively related to Security in cloud computing.	Accepted
H4: Security is positively related to the user's Trust in cloud computing	Accepted
H5: Reliability is positively related to Security of cloud computing	Accepted
H6: Reliability is positively related to the user's Trust in cloud computing.	Accepted

9. DISCUSSION

Trust plays an important role in every field of life. It is viewed as a measurable belief that utilizes experience to make trustworthy decisions (Sun, Chang, Sun, and Wang, 2011).

To use the cloud computing applications, the users have to allocate their resources in the datacenter of cloud provider where they do not have control over their files which makes the trust a critical issue for them. Therefore, the cloud providers need to concern about some factors to eliminate the risks and increase their trust.

After analysing the collected data, it was found that all the factors to some extent affect the user's trust toward cloud storage applications, either **directly** or **indirectly** through security. For the **indirect effect** on trust through security, it was evident that **availability** and **cloud transparency** have a greater impact on security than other factors.

For **availability,** the results confirmed Reference [27] claim that availability and security are closely inter-linked. Thus, cloud storage applications should be available to users whenever they request access, to ensure their feeling of security and therefore trust.

For **long-term viability**, the results did not support Reference [30] and Reference [3] who claimed that it is an important issue that affects security. The reason may be that our sample comprises ordinary users who are not a business or organization that requires their files to be stored long term for auditing purposes. These users might not be concerned if their cloud goes down or if other companies acquire the data center, as they do not think about this from a professional or business point of view.

For **backup and recovery**, the results were consistent with Reference [5] concern that the cloud provider must have techniques to recover from any data loss; Reference [3] also stressed that that if a failure occurs with the cloud, it is critical to completely restore clients' data.

For the **direct effect** on trust, **reliability** and **security** were found to have a significant effect on users' trust. For **reliability**, the results support Reference [34] and Reference [5] claims that it is an important component of trust, through which the cloud storage application should be able to perform its required functions or operations under stated conditions for a specified period of time. Such results provide insight for developers, that the cloud environment should be implemented in such a way as to give users confidence in all aspects of reliability, to ensure their trust toward better adoption. For **security**, Reference [32] emphasized that security plays a central role in cultivating trust in the cloud. Therefore, the cloud computing application providers should deploy security policies, technologies and controls to protect applications, data and associated infrastructure. The results also showed a relationship between **reliability** and **security** in cloud computing. Thus, the provider should provide a safe, reliable computing environment, making the information and data of users secure [35].

For managing the trust through what is called "Trust as a service", there are many trust management models for cloud computing environment that were proposed by many researchers [38, 34. 39].

Reference [38] presented four Trust as a service Management Techniques which includes Policy as a Trust Management Technique (PocT) so to establish trust among parties and has been used in cloud environments, Recommendation as a Trust Management Technique (RecT). Recommendation, Reputation as a Trust Management Technique (RepT) as the feedback of the various cloud service users can influence the reputation of a particular cloud service either positively or negatively, and Prediction as a Trust Management

Technique (PrdT). Prediction as a trust management technique (PrdT) that is useful when there is no prior information regarding the cloud service's interactions.

Reference [34] also examined how trust value is calculated based on credential four attributes such as availability, reliability, turnaround efficiency and data integrity.

Furthermore, Reference [39] proposed a management model for Trust as a service taking into account criteria of quality of service such as cost, response time, bandwidth, and processor speed, and so on it considers the speed of implementation of works.

10. CONCLUSION AND FUTURE WORKS

This research measures factors affecting users' trust of cloud storage applications in the Kingdom of Bahrain. To achieve this objective, a research model was proposed by combining different factors identified from the literature review: Availability, Backup and Recovery, Long-Term Viability, Security and Reliability. A questionnaire was distributed to users of cloud storage applications in Bahrain.

It was found that all the stated factors except one contribute to affecting the level of users' trust in cloud storage application the exception is Long-Term Viability. Thus, Reliability and Security have direct impacts on Trust in cloud storage applications, while Availability, Backup and Recovery have indirect impacts on Security. These factors, combined with security, greatly affect trust in cloud storage applications.

This research has many limitations that can be considered for further investigation. For example, the sample size is small, and a larger sample size is needed before any generalization of the results can be made. Also, this research can be expanded to include cloud use for business purposes, which would give a different perspective of trust and the factors affecting it.

REFERENCES

[1] Jing, X a and Jian-jun,Z. (2010) A Brief Survey on the Security Model of Cloud Computing. Ninth International Symposium on Distributed Computing and Applications to Business, Engineering and Science (DCABES), Hong Kong IEEE, pp. 475 – 478. Aug 2010.

[2] Dhiman, A., and Joshi, M. (2014) Analysis of Performance for Data Center under for Private Cloud through Cloud Computing. *International Journal of Engineering and Computer Science* (IIECS), 3(6), pp. 6422-6431.

[3] Sabahi, F. (2011). Cloud Computing Reliability, Availability and Serviceability (RAS): Issues and Challenges. *International Journal on Advances in ICT for Emerging Regions*, 4(2), pp.12-23.

[4] Rathi, K and Kumari, S. (2015) Analyzing and Surveying Trust In Cloud Computing Environment. *Journal of Computer Engineering* (IOSR-JCE) 17(3), pp. 66-70.

[5] Meixner, F. and Buettner, R. (2012). Trust as an Integral Part for Success of Cloud Computing. In Proceedings of *The Seventh International Conference on Internet and Web Applications and Services*, May 27 - June 1, 2012, Stuttgart: Germany, pp.207-215.

[6] Armbrust M, et al. (2009) Above the clouds: a Berkeley view of cloud computing. Available from: https://www2.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.pdf

[7] Mell, P. and Grance. T. (2009) The NIST The NIST Definition of Cloud Computing. Available from: https://www.nist.gov/system/files/documents/itl/cloud/cloud-def-v15.pdf

[8] Neelima, M., and Padma, M. (2014) A study on cloud storage. *IJCSMC*, 3(5), pp.966 – 971.

[9] Wu, et al. (2010) Cloud Storage as the Infrastructure of Cloud Computing. In Proceedings: 2010 International Conference on Intelligent Computing and Cognitive Informatics, 22-23 June 2010, Kuala Lumpur, pp. 380-383.

[10] Rajan, R., and Shanmugapriya, S. (2012) Evolution of Cloud Storage as Cloud Computing Infrastructure Service.*IOSRJCE.1* (1), pp.38-45.

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

[12] iGA(2017) Cloud Computing Initiatives. Available from: from: https://www.bahrain.bh/

[13] Sukumaran, H. and Al-Mutawha, K. (undated) Bahrain Cloud Transformation: Cloud First in eGovernment. Available from: http://www.iga.gov.bh/Media/Pdf-Section/Bahrain%20Cloud%20Transformation_Cloud%20First%20in%20eGovernment.pdf

[14] National Enterprise Architecture (2019) Cloud-First Policy. Available from: http://www.nea.gov.bh/Cloud-First-Policy

[15] Mayer, R., Davis,J., and Schoorman,F. (1995) An Integrative Model of Organizational Trust: Past, Present, and Future," *Academic of Management Rev*. 20 (3), pp. 709–734.

[16] Huang, J. and Nicol, D. (2013) Trust mechanisms for cloud computing. Journal of Cloud Computing: Advances, Systems and Applications Advances, Systems and Applications 2(9).

[17] Ritua, Randhawab, S., and Jainc. S. (2017) Trust Models in Cloud Computing: A Review. *International Journal of Wireless and Microwave Technologies* 7(4), pp. 14-27

[18] Uusitalo, I., Karppinen, K., Juhola, A., & Savola, R. (2010) Trust and cloud services-an interview study. In Cloud Computing Technology and Science (CloudCom), 2010 IEEE Second International Conference on (pp. 712-720). IEEE.

[19] Sun,D Chang, G., Sun,L., and Wang,X. (2011) Surveying and Analyzing Security, Privacy and Trust Issues in Cloud Computing Environments. Procedia Engineering 5, pp. 2852-2856.

[20] Hwang, K., and Li, D. (2010) Trusted Cloud Computing with Secure Resources and Data Coloring. *IEEE Internet Computing* 14(5), pp.14-22.

[21] Gefen, D.; Karahanna, E., and Straub, D.W.(2003) Trust and TAM in Online Shopping: An Integrated Model. *MIS Quarterly* 27 (2003), 1, pp. 51-90

[22] Kallonjatis, C. (2016). Increasing Internet Users Trust in the Cloud Computing Era: The Role of Privacy. *J Mass Communication Journalism*, 6(3), pp. 2-5.

[23] Rashidi, A. and Movahhedinia, N. (2012). A Model for User Trust in Cloud Computing. *International Journal on Cloud Computing: Services and Architecture(IJCCSA)*, 2(2), pp.1-8.

[24] Ahmad, S., et al. (2012). Trust Model: Cloud's Provider and Cloud's User. *International Journal of Advanced Science and Technology*, 44(2012), pp.69-79.

[25] Darsi, M., Babu, D. V. and Darsi, C. (2014). Addressing Trust Issues in Cloud Computing. *International Journal of P2P Network Trends and Technology (IJPTT)*, 4(2014), pp.42-48.

[26] Uikey, C. and Bhilare, D. (2013). A Broker Based Trust Model for Cloud Computing. *International Journal of Emerging Technology and Advanced Engineering*, 3(11), pp.247-252.

[27] Czarnowski, A. P. (2014). Service Availability (in the clouds). AVET INS/ EuroCloud Polska. Warsaw.

[28] Vaish, A., Kushwaha, A., Das, R. and Sharma, C. (2013). Data Location Verification in Cloud Computing. *International Journal of Computer Applications* 68(12), pp.23-26.

[29] Ramgovind, S.,and Eloff, M.M., Smith, E.(2010). The management of security in cloud computing. In: The Proceedings of IEEE Conference on Information Security for South Africa, 2-4 Aug. 2010, Johannesburg, South Africa, South Africa.

[30] Sailaja, D. and Usharani, P. (2017). Cloud Computing Security Issues, Challenges and its Solutions in Financial Sectors. *International Journal of Advanced Scientific Technologies, Engineering and Management Sciences (IJASTEMS*, 3 (Special Issue.1), pp. 190-196.

[31] Robinson, N.; Valeri, L.; Cave, J. et al., 2010: The Cloud: Understanding the Security, Privacy and Trust Challenges. Report prepared for Unit F.5, Directorate-General Information Society and Media, European Commission; http://cordis.europa.eu/fp7/ict/security/docs/the-cloud-understanding-security-privacy-trust-challenges-2010_en.pdf.

[32] Bhosle, P., and Kasurka, S. (2013) Trust in Cloud Computing. *International Journal of Advanced Research in Computer Engineering & Technology* 2(4), pp. 1541- 1548.

[33] Paine, K. (2013). Guidelines for Measuring Trust in Organizations. 1st ed. [ebook] Gainesville: University of Florida. Available at: http://www.instituteforpr.org/wp-content/uploads/Guidelines-for-Measuring-Trust-KDP-4-13.pdf.

[34] Manuel, p. (2013). A trust model of cloud computing based on Quality of Service. *Annals of Operations Research*, 233(1) pp. 281–292.

[35] Manchanda, S., Parashar, V., Bhatia, V., and Prabhakar, N. (2015) Challenges to Security and Reliability in Cloud Computing. In Proceedings of Information Science, Electronics and Electrical Engineering (ISEEE), 2014 International Conference on, 26-28 April 2014, Sapporo: Japan

[36] Bowling, A. (2002) Research methods in health: investigating health and health services, 2nd edn. Berkshire: Open University Press.

[37] Hair, J. F. et al. (1998). Multivariate data analysis (5th Ed.). New Jersey: Prentice Hall.

[38] Noor, T.H., Sheng, Q.Z., Zeadally, S., & Yu, J. (2013). Trust management of services in cloud environments: Obstacles and solutions. *ACM Computing Survey*, 46(1), article 12

[39] Gholami, A, and Ghobaei-Arani, M. (2015) A Trust Model Based on Quality of Service in Cloud Computing Environment. *International Journal of Database Theory and Application* 8(5), pp.161-170.

Dr Hayat Ali is an assistant Professor at applied Science University, Department of MIS. She received her PhD degree in Business Administration (Information Systems division) from the University of Manchester. She got a Postgraduate Certificate in Academic Practice (PCAP) from York St. John University, UK since 2008. She has a senior academic fellowship from Higher Education Academy (HEA) in UK. She has many publications in Scopus indexed journals as well as many conferences.