Cloud Trust Management – Issues and Developments

Isaac Odun-Ayo, *Member, IAENG,* and Blessing Ehi Idoko

***Abstract* — Cloud infrastructure is an evolving technology that offers organizations and enterprises the ability to access various elastic and scalable resources. The cloud provider offers application software that can be implemented by multiple users online. Also, the customer is provided with the capability of creating and deploying custom built applications relevant to the needs of the enterprise. In addition, scalable and elastic massive storage and computing resources is available in the different categories of cloud types. The decision for an organisation or enterprise to migrate and outsource applications to the cloud requires trust. Any customer wanting to adopt the cloud wants to be sure that the cloud provider can be trusted to meet agreed requirements. This study was executed by means of review of some literature available on cloud computing and trust management. The results indicated that users are not able to access services on their own terms, clearly eroding trust. In addition, application of encipherment in trust management was not discussed in details. Criteria for identifying quality cloud providers received less than 30% attention. Mechanisms for auditability and transparency which should have been given over 50% consideration, received less than 20%. This results will be beneficial to cloud service providers, cloud users and researchers alike.**

***Index Terms* – Cloud Services, Cloud Computing, Trust Management in Cloud Services**

I. INTRODUCTION

"CLOUD computing is a model for enabling universal, on-demand and convenient network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" [1]. Cloud computing is an IT evolution that is assisting businesses, enterprises, organizations and even individuals in accomplishing their IT goals. Business start-up to can utilize the cloud without having to invest in infrastructure. Enterprises can migrate some of their processes to the cloud, while individuals can also leverage the computing efficiency of cloud services. Cloud services is basically divided into three primary categories, the Platform-as-a-Service (PaaS), Software-as-a-Service (SaaS) and Infrastructure as-a-service (IaaS).

Manuscript received April 05, 2018; revised May 07, 2018. This work was supported in part by the Covenant University through the Centre for Research, Innovation and Discovery (CUCRID).

I. Odun-Ayo is with the Department of Computer and Information Sciences, Covenant University, Ota, Ogun State Nigeria. (+2348028829456; Isaac.odun-ayo@covenantuniversity.edu.ng)

B. I. Idoko is with the Department of Computer and Information Sciences, Covenant University, Ota, Ogun State, Nigeria. (+2348038178898; email: blessing.idoko@stu.cu.edu.ng)

In SaaS, service providers or cloud service providers (CSPs) deploy custom made applications on the Internet for user to access anywhere, anytime using suitable devices based on the cloud principle of multitenancy. This is usually at a fee, but cloud consumers do not have issues with the certificate or licenses. In PaaS, cloud service providers provide integrated development environment (IDE's) to enable consumers or users create and install their own software. Cloud consumers or users have complete access to the installed software, while the cloud service providers control the underlying infrastructure. In IaaS, the CSP offers storage and computing resources to users. Such CSPs have adequate infrastructure and large data centres sometime spread across geographical regions. The user has control over the application, OS and storage to a certain extent while the CSP controls the main infrastructure. Cloud computing is divided into four types of deployment - public cloud, private cloud, community cloud and hybrid cloud. The private cloud is for a particular organization that can only be accessed by members of that organization. The cloud is hosted by a third party agent or on-premise. The private cloud is considered more secure. Public cloud is for large organization and major CSPs with huge investment in infrastructure. Service is provided to customers at a cost over the Internet. Community clouds is managed and owned by several organizations coming together based on share common interest. Institutions and hospitals typically host community clouds. Community cloud can be hosted by third party agents. Hybrid cloud is the collection of either public, private or community clouds. Organizations can migrate auxiliary services to the public cloud while retaining core services on private clouds. In using the cloud, consumer have concerns bothering on certain aspects of the service. One of the major concerns of cloud users is the location of their data, hence the issue of trust. The cloud characteristics of multitenancy and virtualization also aggravate the trust factor between the cloud provider and users.

However, issues with trust between CSP and cloud consumers has a drawback on the universal acceptance of cloud services as an outsourcing service. Trust is a social problem, but technological advancement can improve information credibility, reputation and trust on cloud services [2]. To increase the consumers' base of cloud services, CSPs must implement a trust and security mechanism to eliminate the fears of cloud users to the barest minimum. The issues associated with trust in cloud computing is not against the CSP, but cloud computing capabilities which are implemented on the cloud. It also does not lie in the technology, but it is due to the customer's lack of control over sensitive data assets, absence transparency and unclear security assurance. Trust is an act of believing, reliance and confidence in something that is expected to accomplish as promised [3]. It is confidence that a person has, that they can

ISBN: 978-988-14048-1-7
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

entrust others to take care of their valuable assets based on their competence, expertise and agreements. A system has low trust, if there is insufficient information about its expertise and experience. Problems with trust becomes a pertinent issue due to decentralization of data and distribution of resources beyond the perimeter of the user [4]. Due to the growing number of CSPs, cloud users also face the challenge of selecting the most efficient service provider. Trust and reputation systems are widely used in various software applications scenario that enables cloud consumers identify trustworthy and reliable service providers. A trust system plays a vital role in helping cloud consumers decide on resources that are suitable for hosting their software applications. The core objective of this paper is to examine the issues of trust management in cloud computing. The rest of the paper is as follows. Section 2 examines related work. Section 3 presents cloud computing characteristics and trust issues. Section 4 highlights cloud deployment models and top risks of cloud computing in providing trust. Section 5 focuses on cloud user requirements. Section 6 is on analysis and discussion. Section 7 is the conclusion of the paper and suggestion of further work.

II. RELATED WORK

In [5], a trust management system for cloud computing based on the issue of trust between the users and the CSPs is discussed. SLAs differ from one service providers to another hence the need for trust. The paper proposes a trust management system with metrics for identifying trust worthy CSPs and a trusted cloud service with secure data and resource provisions. [2] focuses on virtualization, privacy and data integrity as means of ensuring trust. A model comprising trust in terms of data is proposed between consumers and providers on the cloud. A critical review in [6] examines trust management in cloud computing which considers security as a vital component of trust management. The paper proposes a model for trust management system and carried out a comparison of trust systems. Establishing trust in cloud services in [7] presents the issues of trust with customer data being processed in remote locations by a cloud service provider. Various aspects relating to trust were discussed in the paper including diminishing control of the user. Trust in the cloud in [3] alludes to the fact that organisations will not host their software applications on the cloud without the guarantee of trust. The paper examines the TClouds model that is beneficial to all the parties utilizing the cloud. [4] focuses on utilizing third party agent checking, to control and manage trust in the cloud, which is concerned with having several unknown users whose intention may either be bad or good regardless of the cloud provider. The paper proposes a model with appropriate preferences to allow a user decide on a suitable cloud provider.

Trust frameworks for determining the security strength of cloud computing services in [8] focuses on the various security mechanism being used by the different cloud service providers. The paper proposes a trust model to evaluate the levels of security and determine a trust value. Trust in the clouds in [9] discusses the issue of trust in cloud computing in terms of consumers' perception. Several issues regarding cloud trust were discussed with a concern that regulation and technology should work seamlessly. Enhancing trust management in cloud environment in [10] examines the issue of trust between users and cloud providers in e-commerce. The paper proposes a trust management system to help in identifying trusted providers and safe transactions. In [11], trust is seen in terms of both technology and management. The paper conducted a survey based on security, ethics and data protection to enable trust between customers and providers. A novel trust management framework for multi-cloud environments based on trust service providers in [12] tackles the issue of trust on the cloud using trust service providers. The model makes use of information on compliance with SLA and satisfaction of the user to rate a cloud provider. A trust evaluation framework for cloud services in [13] applies an evaluation framework to determine trust in cloud services. Direct recommendation trust is utilized and the model proves to be effective.

III. CLOUD COMPUTING CHARACTERISTICS AND TRUST ISSUES [5] [2] [6] [7] [3] [9]

A. *Characteristics of Cloud Computing*

Some characteristics of cloud computing is as follows [14] [15]:

a. Cloud broad network access: Cloud customers can access data and resources from any location with the aid of the internet through various types of platform.
b. Cloud measured service: Cloud services and resources are monitored and controlled by the cloud service providers through a pay-as-you-go payment plan. Users take advantage of these resources in a way similar to using gas, electricity and water.
c. Cloud reliability. This is accomplished by utilizing various redundant site. Efficient reliability of service is very good for disaster recovery.

B. *An Overview of Trust and its Issues*

Trust as a very complex belief [32]. Trust does not seem to have a unique definition in cloud computing. It can be defined as "levels of confidence in something or someone". Relating this to the cloud, it can be described as the level of satisfaction or confidence that a user has in the services that is been provided by a CSP. Trust is based on the confidence and assurance that data, humans, entities, information or processes will provide an expected result with a certain level of guarantee. Trust could relate to machine to machine, which allows the establishment of handshake protocols negotiated within certain protocol mechanism. It could also be in form of human to human interaction or human to machine in the case of a consumer that evaluates a digital signature on a website. Trust could also involve machine to human in a situation where a system depends on user input and instructions without general verification. In a more advanced consideration, trust is an important aspect for enhancing security and privacy considerations. Some of the common trust issues are:

ISBN: 978-988-14048-1-7
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

1) Control

Control is an important trust issue. A system is less trusted when users do not have control over their assets. For example, in withdrawing money from an ATM, the machine is trusted for an exact amount, because it is under the user's control. If a deposit is made the level of trust is less, because the users does not know what happens to the money.

2) Ownership: Cloud consumers feeling of ownership also guarantees trust in a system. A user might have confidence in an electronics payment platform and such a user buys product on the platform with a credit card, but may have limited confidence using a client's card because of the need to preserve the client's interest. Similarly, when organizations or enterprises release their applications and data to the cloud, it creates a twofold complex relationship. The enterprises must have confidence in the cloud service provider. The organization or enterprise must also ensure that its customers have reasons to have the same confidence in the service been provided to them.

3) Security: Security assumes a focal part in ensuring an organisation administration is not disappointed and also developing trust in the cloud. Specifically, CSPs need to secure the virtual condition which empowers them to run administrations for various customers and organisations. With regards to virtualization, the key security issues include information leakage caused by numerous occupants sharing physical assets and access control.

C. Trust Issues Application

Trust issues application can be demonstrated with a normal illustration. An organization Softcom handles medical services related pictures of its customers, the pictures are confidential and ought to stay private and secret. Softcom chooses to utilize CloudX an open cloud supplier situated in US for picture processing utilizing Softcom's Picture Expert programming on a remote application server. Extra picture handling undertaking, for example, sifting and looking through images is handled by ImagePro for CloudX's iFilter and iSearch frameworks. CloudX is also utilized for picture documenting.

At the CloudX site in U.S, ImagePro facilitated an application server running on a UNIX platform, processes the picture and stores them briefly on a Circle 1. CloudX now transmits the picture to another cloud site situated in Italy for extra handling by iFilter and iSearch, and afterward stores the pictures on another storage Circle 2. CloudX files the pictures on Plates 3, 4 and 5 physically situated in China. Its cloud framework division deals with those files. The structure proposes that Softcom utilizes three kinds of administrations in [5].

D. Process for Building Trust

To complete the process with CloudX, Softcom needs the accompanying confirmations with respect to its control of the information:

a. CloudX must advise Softcom when anyone gets to its pictures.
b. CloudX and its different destinations must not keep unapproved duplicates of Softcom pictures.
c. CloudX must destroy deposited or obsolete pictures at all destinations that it oversees.
d. Softcom must know where capacity and handling happens.

IV. CLOUD DEPLOYMENT MODELS AND TOP RISKS OF CLOUD COMPUTING TO PROVIDING TRUST

Cloud computing deployment models as follows [30]:

a. Private: This is a type of cloud computing where the infrastructure is operated only for the need of an organization. Accessibility is just within the concerned organization's private network. Its management is done internally or can be outsourced to a third party possibly off-premise.
b. Public: This is a cloud infrastructure designed for delivering services to the public and accessible by all users.
c. Community: This is a type of cloud computing where the cloud infrastructure is shared by several organizations with common concerns.
d. Hybrid: This is a combination of either private or public clouds, which allows for portability of application and data. The combined cloud types that are pooled operate alone.
e. Partner: This a special arrangement for particular organisations in which services are provided.

A. Top Risks of Cloud Computing To Providing Trust

Cloud computing allows the cloud service provider to have total control of the user's data and resources leading to trust and security issues, because the user should have the right to know where their data is stored and how such data is being accessed [31]. Although these issues can be handled by adding precautionary trust mechanism like encryption and strong authentication procedure, it still should not prevent the users from knowing and having control over their data. Hence the need for more transparency on the part of the cloud providers to ensure trusted governance issues. Some major and ongoing risks to cloud computing are:

a. Loss of Governance.
b. Inadequate transparency and auditability by CSPs.
c. Inadequate tracking of access history.
d. Insufficient data source of virtual and physical servers

V. CLOUD USERS REQUIREMENTS

The cloud user's requirements can be classified as follows:

A. Security Requirements [32]

Suffice to mention that having a secure cloud from a provider's point of view does not mean that it is secure for the users. The security requirements for a cloud user includes confidentiality, availability, and accountability.

1) Confidentiality

Confidentiality deals with security of information, because once data leaves an organisation's data centre, it can no longer be considered secured [33]. Specialized instruments

ISBN: 978-988-14048-1-7
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

like encryption and access control, and additional legitimate assurances are used to achieve confidentiality. Since a large portion of services in the cloud are delivered via remote connection, attack strategies, such as phishing, fraud, and abuse of software vulnerabilities can still succeed. Frequent use of login credentials (username and password) also increases the impact of such attacks. Some cloud approaches seem to also add other risk to the scenario. For example, it is possible for a malicious user to have access to other user's credentials. This makes it easy to spy and manipulate data, also falsify and redirect the legitimate user's information to an illegitimate site. Similarly, the process of organizing data has an effect on data loss and leakage [33]. This is because an organization's data may be stored on servers in another country, which is a natural source of concern to most organisations. Another issue of trust deals with the length of time that an organisation's data is kept by a cloud service provider. The provider may keep the data even after it has been deleted by the owner organisation. The cloud service provider also has the capacity to delete or even modify an organisation's data without adequate backup leading loss of data permanently [33].

2) Availability:

Availability refers to being able to use the system whenever there is a request for it. This is generally enhanced by appropriate service level agreements, good infrastructure and adequate capacity on the part of the cloud provider. All major cloud providers give 99.99% availability and uptime guarantees to their customers [33]. Usually such availability could be for a single server directly associated with specific users or for all their servers located in different data centers across the world. On the contrary, business discontinuity affects the users badly since the "as a service" process on the cloud provides resources and offers them as a service that could be disrupted.

3) *Accountability*:

Cloud computing does not make it clear on how privacy of data provided by the user is guaranteed on the cloud, since different privilege levels are provided on the cloud [33]. There are privilege levels for the CSPs, the user, the cloud administrators, owners of data, which are offered and used on the cloud. Facilities such as strong identification process, appropriate authentication and strict access control, and adequate logging of transactions and afterward critically reviewing these logs and tracking malicious attempts are regular methods for handling accountability in cloud computing [33]. The vulnerability of such user privileges and tasks definition associated with data ownership, access control, infrastructure maintenance, and many others can also encourage business or legal conflict.

B. Privacy Requirements

Moving part of an organization's IT resources to the cloud environment involves giving partial privileges to the CSP. The level of control has to do with the type of deployment model. For example, in IaaS model, the organization only gives the provider management of their hardware and network. In other words, accepting a cloud approach means entrusting its IT device control to a third party, hence loosing partial or complete control over data and resources [33]. Such practices impacts negatively on data integrity, since users are not sure if their data is stored correctly by the cloud provider, and that it is protected from unauthorized alteration be it planned or unplanned.

VI. ANALYSIS AND DISCUSSION

There are several authors and researchers that have done a lot of work in the area of cloud trust management. Major topics in the area of cloud trust management were extracted from the work of some of these key authors. The findings from reviewing such papers are outline in Table 1 and discussed in subsequent paragraphs.

TABLE I
PARAMETERS USED IN VARIOUS LAYERS TO ANALYSE CLOUD TRUST MANAGEMENT ISSUES

Author	Accessibility/Consistency	Identifying quality cloud providers	Reputation trust model	Credibility, Privacy	Scalability and Applicability	Standardized SLAs	Encipherment in Cloud	Auditability
Talal H Noor et al , (2013)			*	*	*			
Habib, S.M et al. (2011)	*	*	*			*		
Abawaj y, (2011)	*		*					
Grandis on, T. and Sloman (2000)	*		*					
(Qiang et al. (2011)					*			
Marudh adevi et al. (2014)						*		
Abassi et al. (2012)					*			
Jingwei Huang and David M Nicol, (2013)			*			*		
S. Pearson and A. Benameur, (2010)						*	*	
S. Bhattachar ya and C. R. S. Kumar								*
M. Alouane and H. E. L. Bakkali			*					*

A. Reputation Trust Framework:

In reputation trust framework, cloud trust management is based on consumer's feedback and reputation. The

framework collects the customer's feedback to carryout qualitative measurement of the level of trust being provided by the service provider. The feedback is based on various security parameters and QoS offered by the cloud service providers. Reputation of an entity is the collective contribution of an organization towards an entity. It is the value showing the trustworthiness. Cloud service providers with high level of reputation will be the most trusted among cloud consumers or the community of cloud users [22]. Fairly sufficient attention was given to this topic by the papers examined, as this was discussed by 54% of the authors.

B. Recommendation Trust Framework

Flavio et al., stated that if two entities such as trustor or trustee have no direct access or interaction, establishment of trust is done via a third party recommendation by the auditor which is also known as recommended trust. This allows the users some level of trust in the cloud provider [23] [24]. A trust process that examines a complete trust value using three parameters which are customer's self-trust, third party trust and friend's trust on service providers is discussed in [25]. [26] proposed recommendations based on trust models in service oriented computing. The model of the trust schemes in service oriented computing (TRSC) allows evaluation of cloud services using both the direct and recommendation trust. Web portals are the tools where cloud service providers register their services and cloud consumers also register their requirements and get recommendation feedback.

C. Cryptography, Credibility and Privacy

D. One valuable approach to protect key prerequisites such as trustworthiness and privacy in distributed computing, is to encode information before, during and even after transport through the web to ensure it is secure. As the cloud specialist organization handles the data its clients, and may offer it intentionally to outsiders, there is a critical requirement for information security, for example, encryption. One strategy for accomplishing this is by utilizing a mix of encryption components. The hidden procedure and trust-building measure utilized is pre-web or pre-egression encryption (PIE). This implies scrambling information with the user's particular encryption keys before sending it to the cloud. The encryption keys are in the control of the information proprietor just as they are kept by the cloud specialist from outsiders. After the information is scrambled locally it will leave the local premises and travel through the wide area network [27]. Cryptography, credibility and privacy are key aspects of cloud trust management, but only 18% of the important authors selected for this review examined these topics.

E. Certifications, Standards Compliance and IT Service Quality

Cloud trust requires a strong and reliable establishment to rely upon. There is an arrangement of providing trust building measures in the field to benchmarks consistencies and affirmations, three of which are extremely valuable. The primary trust-building measures expects that providers should help cloud users select the correct cloud specialist organization in its migration. There is the Cloud Security Cooperation in the U.S.A. and the Government Office for Data Security (BSI) in Germany that help in mitigating trust issues. Both help in an activity called EuroCloud Star Review that gives a seal of value to Programming-as-an-Administration and is one of the three subdomains of distributed computing [28]. From the core papers examined for this analysis, about 54% of the authors examined these issues.

F. Data and Service Migration

One essential concern of cloud users is the potential absence of long haul benefits assurances and the failure to get the required information, once an organisation's data is deployed to the cloud, because of information security issues with CSPs. Therefore, the clients would be compelled to remain with only one CSP, who may ask for premium costs and along these lines demoralize potential clients from utilizing the cloud benefits. Users would just utilize cloud services, in the event that it becomes essential or because they were guaranteed that their information could certainly be moved to other cloud service provider if the need arises. Hao, Yen and Thuraisingham considers the issue of administration choice and movement in a cloud and built a system that enhances portability. It likewise incorporates a cost factor and a choice calculation to examine trade-offs issues and locate the ideal administration migration choices [29].

There are limitations found in the various trust frameworks reviewed in this paper. In the Service level agreement trust framework, privacy and safety is not taken into consideration and cloud consumers are not able to assess the cloud services on their own. This requires the help of a third party either trust authority or a broker. In addition, there is lack of a standardization frameworks or models for a selection process provided by the cloud providers that are suitable to be recommended. In reputation trust framework, reputation is the basis for choosing the required service provider in the first instance but subsequently the service provider may not render satisfactory services. The complication is very high because a large number of customers have to rate the services for it to be considered to have a good reputation. To overcome these problem, it is possible to combine recommended and reputation trust framework with high degree of privacy and safety to improve the efficiency.

As shown in Table 1, the major areas of focus are accessibility/consistency, identifying the quality cloud providers, security/reputation trust model, credibility/privacy, scalability and applicability, standardized SLAs audit, application of encipherment in cloud computing, auditability/transparency. Generally, none of the papers examined covered all the areas under consideration, while [15][16][17][18][22][32] only discussed the core security areas being considered. Application of encipherment in cloud computing was not sufficiently discussed. Criteria for identifying quality cloud providers received less than 30% attention. Mechanisms for auditability and transparency was expected to have over 50% consideration but only received less than 20%. Therefore, more work needs to be done in terms of security and transparency considerations in cloud trust management. Clearly there is a lot of research being done in the area of trust in cloud computing, however it is obvious that cloud users are very much concerned about the

ISBN: 978-988-14048-1-7
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

confidence levels across the various deployment platforms and the services provided.

VII. CONCLUSION

Cloud computing provides scalable elastic, on-demand and vital services to users. User can take advantage of applications provided by cloud providers or use the cloud to deploy and also perform various services. The cloud user is concerned about security and privacy of data hence the issue of trust. The issue of trust is aggravated because the cloud user does not know where data is located and who has access to it. Several efforts are ongoing to build trust between the CSP and cloud users. Various security strategy and confidence building measures using technology are evolving regularly to ensure trust in cloud computing.

ACKNOWLEDGMENTS

We acknowledge the support and sponsorship provided by Covenant University through the Centre for Research, Innovation and Discovery (CUCRID).

REFERENCES

[1] Peter Mell, Timothy Grance, (2011) "The NIST Definition of Cloud Computing", NIST Special Publication 800-145.
[2] Kai Hwang, Deyi Li, (2010), "Trusted Cloud Computing with Secure Resources and Data Coloring", IEEE Internet Computing, September/October 2010.
[3] Imad M. Abbadi, Andrew Martin (2011), "Trust in the Cloud", Information and Security Technical Report (2011), doi:10.1016/j.istr.2011.08.006.
[4] Syed Rizvi, Kelsey Karpinski, Brennen Kelly, Taryn Walker, (2015), "Utilizing Third Party Auditing to Manage Trust in the Cloud", Complex Adaptive Systems, Publication 5, Procedia Computer Science 61 (2015) 191 – 197.
[5] Sheikh Mahbub Habib, Sebastian Ries, Max M¨uhlh¨auser, (2011), "Towards a Trust Management System for Cloud Computing", Technische Universit¨at Darmstadt, Accessed on 24 January 2018
[6] Mohamed Firdhous, Osman Ghazali and Suhaidi Hassan, (2011), "Trust Management in Cloud Computing: A Critical Review", International Journal on Advances in ICT for Emerging Regions 2011 04 (02): 24 – 36.
[7] Khaled M. Khan and Qutaibah Malluhi, (2010), "Establishing Trust in Cloud Computing", IT Pro September /October 2010 Published by the IEEE Computer Society 1520-9202/10.
[8] Rizwana Shaikh, Dr. M. Sasikumar, (2015), "Trust Model for Measuring Security Strength of Cloud Computing Service", International Conference on Advanced Computing Technologies and Applications (ICACTA2015). Procedia Computer Science 45 (2015) 380 – 389.
[9] Patrick Ryan, Sarah Falvey, (2012), "Trust in the clouds", Computer Law & Security Review 28 (2012) 513-521.
[10] Soon-Keow Chong, Jemal Abawajy, Masitah Ahmad, Isredza Rahmi A. Hamid, (2014), "Enhancing Trust Management in Cloud Environment", International Conference on Innovation, Management and Technology Research, Procedia - Social and Behavioral Sciences 129 (2014) 314 – 321.
[11] Issam Kouatli, (2016), "Managing Cloud Computing Environment: Gaining Customer Trust with Security and Ethical Management", Information Technology and Quantitative Management (ITQM 2016). Procedia Computer Science 91 (2016) 412 – 421.
[12] Wenjuan Fan, Harry Perros, (2014), "A novel trust management framework for multi-cloud environments based on trust service providers", Knowledge-Based Systems 70 (2014) 392–40.
[13] Xiaonian Wu, Runlian Zhang, Bing Zeng, Shengyuan Zhou, (2013), "A trust evaluation model for cloud computing", Information Technology and Quantitative Management (ITQM2013). Procedia Computer Science 17 (2013) 1170 – 1177.
[14] Ahmed E. Y.: Exploring Cloud Computing Services and Applications. Journal of Emerging Trends in Computing and Information Sciences, VOL. 3, NO. 6, July 2012 ISSN 2079-8407 (2012)
[15] Talal H Noor, Quan Z Sheng, Sherali Zea dally and Jian Yu, Trust management of services in cloud environments: Obstacles and solutions in Journal of ACM Computing Surveys, 46(1), pp.1- 35(2013 a).
[16] Habib, S.M., Ries, S. and Muhlhauser, M, Towards a Trust Management System for Cloud Computing', in International Conference on Trust, Security and Privacy in Computing and Communications, pp.933-939 (2011).
[17] Abawajy, Establishing Trust in Hybrid Cloud Computing Environment, in 10th International Conference on Trust, Security and Privacy in Computing and Communications), IEEE, pp.118- 125. (2011).
[18] Grandison, T. and Sloman, M,A survey of trust in Internet Applications in Communications Surveys and Tutorials, IEEE ,3(4),pp.2-16(2000).
[19] Qiang Guo, Dawei Sun, Guiran Chang, Lina Sun and Xingwei Wang, Modelling and evaluation of trust in cloud computing environments in International Conference on Advanced Computer Control ,pp.112-116(2011).
[20] D.Marudhadevi,V.Neelaya Dhatchayani and V.S Shankar Sriram,A ,Trust evaluation model for cloud Computing using Service level Agreement ,Security in Computer Systems and Networks, The Computer Journal,58(10),pp.2225-2232 (2014).
[21] W. Hao, I. Yen, and B. Thuraisingham, "Dynamic service and data migration in the clouds," in Computer Software and Applications Conference, COMPSAC '09. 33rd Annual IEEE International, pp. 134–139, 2009.
[22] S. Pearson and A. Benameur, "Privacy, Security and Trust Issues Arising from Cloud Computing," *2010 IEEE Second Int. Conf. Cloud Comput. Technol. Sci.*, pp. 693–702, 2010.
[23] S. Bhattacharya and C. R. S. Kumar, "From threats subverting cloud security to a secure trust paradigm," *Proc. Int. Conf. Inven. Commun. Comput. Technol. ICICCT 2017*, no. Icicct, pp. 510–515, 2017.
[24] M. Alouane and H. E. L. Bakkali, "Security , Privacy and Trust in Cloud Computing : A Comparative Study," *Cloud Technol. Appl. (CloudTech), 2015 Int. Conf.*, pp. 1–8, 2015.
[25] Meryeme, A., Hanan, E., "Secutity, Privacy And Trust In Cloud Computing: A Comparative Study", 2015 International Conference on Cloud Technologies and Applications (CloudTech), 2015
[26]
[27] Abassi, R; El Fatmi, S.G, Towards a generic trust management model, in 19th International Conference on Telecommunications, Jounieh pp.1-6 (2012) .
[28] Jingwei Huang and David M Nicol, Trust mechanisms for cloud computing, Journal of Cloud computing, 2(1), pp.2-9(2013).
[29] Flavio Corradini, Francesco De Angelis, Fabrizio Ippoliti and Fausto Marcantoni, A Survey of Trust management models for cloud computing in 5th International Conference on Cloud Computing and Services Science, Lisbon, Portugal, pp.155-162 (2015).
[30] Zhu, H Bao and Deng, Computing of Trust in Distributed Networks in International Association for Cryptologic Research (2003).
[31] Singh, S. and Chand, D, Trust evaluation in cloud based on friends and third party's recommendations, Recent Advances (RAECS) in Engineering and Computational Sciences,pp.1-6(2014).
[32] Dehua Kong and Yuqing Zhai, Trust Based Recommendation System in Service-oriented Cloud Computing in Cloud and Service Computing International Conference ,Shanghai,pp.176-179(2012).
[33] Kerschbaum, "Secure and sustainable benchmarking in clouds," Business & Information Systems Engineering, vol. 3, no. 3, pp. 135–143, 2011.
[34] R. Giebichenstein and A. Weiss, "Zertifizierte Cloud durch das EuroCloud Star Audit SaaS," Datenschutz und Datensicherheit, vol. 35, no. 5, pp. 338–342, 2011.