Towards Building Customer Relationship in Cloud Environment: Experimental Analysis of the Cloud Trust Label Approach.

Onawola, H.J., Longe, O.B, Ridwan, S. & Garba, A.
[1&2]Department of Information Systems
[3&4]Department of Computer Science
American University of Nigeria
School of IT& Computing
E-mails: [1]Hassan.onawola@aun.edu.ng; [2]olumide.longe@aun.edu.ng; [3]ridwan.salahudeen@aun.edu.ng; [4]garba.aliyu@aun.edu.ng
Phone: [1]+2348167730044; +2348160900893; [3]+2348065491787; [4]+2348068107088

ABSTRACT

Findings have established that Cloud computing offers ease of use for businesses with a reduction in the cost of operation for users. In building a relationship between the providers of cloud and customers, trustworthiness has been a key factor that determines the acceptability of cloud computing. The focus of this paper is on building adequate measures on how to create a good and sustainable relationship between cloud users and cloud providers for businesses to thrive in a cloud environment. Work reviewed has shown that information stored in the cloud is vulnerable to a security threat and customers have less or no access control over data and no idea of where their information is being stored. These make the data more vulnerable to be accessed by the third party, which is why many users were very mindful of adapting to the use of the cloud. This study proposed that major stakeholders, the providers, and the users must harmonize and come up with a mechanism that is capable of bringing trust, confidence, transparency, and security of data and other valuable information's in the cloud from being vulnerable to threats. Literature has shown that the cloud trust label of positive or negative information will have an impact on customer's trustworthiness (Van Der Werff et al., 2019). We developed a conceptual model involving three major stakeholders that is the cloud users, the cloud provider, and the service provider(Third Party Auditor TPA), with a secured security device to monitor information transmission.

Keywords: Cloud, Mechanism, Sustainable, Stakeholders, Trustworthiness, TPA

23rd iSTEAMS Conference Proceedings Reference Format
Onawola, H.J., Longe, O.B, Ridwan, S. & Garba, A. (2020): Towards Building Customer Relationship in Cloud Environment: Experimental Analysis of the Cloud Trust Label Approach. Proceedings of the 23rd iSTEAMS Conference, American University of Nigeria, Yola. April, 2020. Pp 89-96 www.isteams.net/yola2020

1. INTRODUCTION

Many businesses, financial institutions would have been closed or slowed down and trading activities may extremely find it difficult to operate in real-time if not because of modern cloud technologies. To build a customer relationship in Information systems is to have the capacity to bring into business very robust customer satisfaction. The providers need to create a mechanism that can open up more business opportunities for the customers in the blockchain(Soltani & Navimipour, 2016). The advent of cloud technologies has witnessed one challenge or the other by the users.

These challenges which makes some of the users not have total trust in the services of cloud technology. As a result of issues such as litigation, security threats, the mimic of information's and maliciously compromising of customer data were some of the complaints of the users of cloud computing. These have given a negative impression of using the technology. The recent transformation in the IT world has impacted on the technological development across the globe focusing towards achieving more business opportunities and providing customers satisfaction with benefits such as the reduction in the cost of operating expenses, ease of use, increased mobility, portability application, scalable and flexible, reliable, maximize utilization of servers, reduce energy consumption and conveniences of operation(Rao & Rao, 2015). The technology aimed to change the organization's attitude in the building of IT infrastructure.

For these reasons, many have closed their doors from using the traditional IT infrastructure to cloud computing. Past reviewed has shown that although cloud computing had tremendous advantages over the traditional IT but also cloud computing is been challenged with security threats to information, privacy issues, data loss, data location, data integrity, and other similar challenges, this is because the operation of cloud computing involves big data(Srinivas, Reddy, & Qyser, 2012).

Cloud computing is internet-based computing, shares resources, and data to PC and other devices (R.Kabilan1, 2017). Information stored in the cloud is vulnerable to the security threat if adequate measures are not put in place by the cloud service provider. All users of cloud need to place more priority on security and be cautious of information stored in the cloud(Huth & Cebula). Cloud computing technology comprises hardware, software, and infrastructure which enable the delivery of cloud computing services like software as a service (SaaS), Platform as a service (PaaS), and Infrastructure as a service (IaaS).

Fig.1 Rapid growing of Cloud Computing
Source:www.google.com/search

Cloud computing is a state-of-the-art internet service system which provides a reliable available and better service to customers(Wang, Kunze, Tao, & von Laszewski, 2011). The paradigm was built on existing technologies and it aims at changing organizational approach for building IT infrastructure, which has now been embraced by many establishments (Araujo et al., 2018; Gamaleldin, 2013).

1.1 Cloud Providers, Subscription and types

Three types of service providers can be subscribed to namely the Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). The services being provided vary in prices depending on the topology of the business. Cloud subscription can be Public, Private, Community or Hybrid types of cloud computing, which combine both private and public together or at least two combinational clouds(Huth & Cebula).

1.2 Data Security Protection by Stakeholders

The diagram below depicts Data Security Protection by Stakeholders

Fig. 2: The Conceptual Model Involving Three Stakeholders for Data Security Protection
Source: Razaque & Rizvi, 2017

1.2.1Cloud Security

Cloud computing is a ubiquitous platform and business-friendly enable connections everywhere, therefore the cloud users require higher assurance of adequate security protection. The interest of customers must be considered very important and be factored into the design of the cloud security network. The deployment of cloud computing needs to come with policies that can protect, controls the cloud users, and safe guide data, information, application, and other vital infrastructure from being vulnerable to threats by cyber-crime. Building a good relationship between the users of cloud and cloud provider requires putting in place a monitorable security management system(Lin, Su, Meng, Liu, & Liu, 2013) and formulating terms of agreement about the trustworthiness of data, information, storage security and security architecture with other items relevant for cloud standardization in the network, for the smooth operation by the users using the cloud (Lee, 2012; Okuhara, Shiozaki, & Suzuki, 2010). Authentication measure is essential to check the pessimism of the major stakeholders involved in the blockchain (Razaque & Rizvi, 2017).

1.2.2 Cloud user

Cloud computing has been an emerging paradigm that provides a good innovative way to engage in business. Findings show that major impediment in the cloud is the lack of adequate security agreements between cloud users and providers in cloud business(Almorsy, Grundy, & Müller, 2016), this has drawn a setback to cloud computing. The stakeholders that are the two providers and the end-users need to come together and discuss and agreed on the modalities and applicable security network standard that is best suitable for their businesses that cannot compromise the security of data, data storage, other vital items from not been vulnerable to threats or attack.

1.2.3 Third-Party Auditor (TPA)

Cloud environment comprises the cloud two providers, the cloud and service usually referred to as the third party auditor (TPA) and cloud users, these shareholders do communicate through infrastructure and other communication tools provided by these two providers on the cloud. The two providers and the users' needs to come together and negotiate on agreed and applicable security standard suitable for the business and good enough to protect data and information's from its vulnerability to security threats. The service provider delegated by the cloud to provide support by proxy also access and share information on the internet to the host and cloud users, in this way it will be improbable to the belief that service provider (TPA) can be trusted and as such data and other valuable information available on the internet can be compromised by TPA and this has been a contentious and security issues surrounding the involvement of a third party for infrastructural support in the cloud environment. Therefore, TPA can be vulnerable and a potential threat to the user's information. To guide against this is to device a means to use a well trusted TPA, protect data integrity, authentication, and provide data confidentiality.

1.2.4 Cloud providers

The activities of the service provider better still the third party cannot be ignored in the supports offered to both the users and cloud providers. Exposing sensitive information's into the hands of the third party in the business blockchain can be risky, inadequately managed and that information's can be vulnerable most especially if the cloud service provider is not trusted (Tang & Liu, 2015) thereby compromising the information. Reviews have shown that trustworthiness has been the concern factors by customers in accepting the deployment of the cloud for businesses, this is imperative for the sustainability of relationship, therefore this has necessitated the need to address this issue.

1.3 Tools Mechanisms for Customer Relationship Management (CRM)

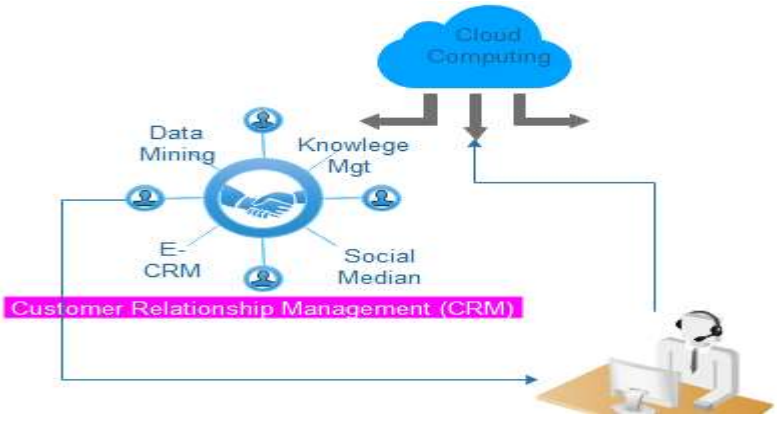

Fig.3 Conceptual idea for frame work for CRM mechanism

1.3.1 Social Media

Engaging in a relationship requires that cloud providers are to constantly engage the cloud users in video chatting, iCloud, sending emails, and interacting with users on information about their business environment, flaws in the business, and other relevant information that can boost users' business.

1.3.2 Knowledge Management (KM)

Today decision-maker faces pressure to make better and faster decisions in an environment characterized by a high domain complexity and market instability of which the outcome of such decision may have positive or negative impacts on the business environment, cloud technologies facilitate the speed at which knowledge and ideas thrive, therefore KM is a vital part and constituent for business to thrive
(Rafiq, Bashar, & Shaikh, 2014).

1.3.3 Data Mining

The extraction of Knowledge from a large amount of database or other repositories Working (Sowmya & Suneetha, 2017).According to R.Kabilan1 (2017) the organization with huge data storage in the cloud will have a large amount of data to mine cloud computing is crucial in the business domain in that, its provide business model and other relevant information's extracted from big data which can follow subscription types such as Analytic as a Service(AasS) and Big data as Service(BdaaS) critical for CRM (Manikyam & Kumar, 2017).

1.3.4 Electronic -Customer Relationship Management (E-CRM)

E-CRM incorporates all forms of net environment use in achieving results that can be used as a model in managing customer relationships via information technology. CRM is a business strategy used in establishing and sustenance of long-standing relationship with customers in a business environment, the integration of cloud will further add more impetus to the business thereby creating more customers loyalty, minimize customer's negativity and create more vibrant interactions with the customers, the cloud has been employed in CRM to further maximize information technology used for constant interaction with customers(Faed, Wu, & Chang, 2010).

This study seeks to build customer relationship in a cloud environment, therefore the cloud computing providers need to be more responsive for provision of reliable service delivery and built a sustainability factor into service being rendered to their various customers across the globe to enhance better performance and establishing a good relationship with customers who subscribed to the platform.

2. RELATED LITERATURE

In developing country the scalability and the low cost of cloud computing makes it more attractive to many establishments especially (Srinivas et al., 2012). Adoption of cloud technology was resisted by some cloud users due to transparency (Van Der Werff et al., 2019).The technology of cloud affects users inability to build a trusted relationship with the service provider(Van Der Werff et al., 2019). Cloud provider couldn't offer customer enough tools to verify the originality of their information, in some cases, they single-handedly manipulate, controlled and executes customers information (Moussa, Ithnin, & Zainal, 2018). In ligation, the information in the cloud can be compromised or manipulated by cloud service provider either to be in favour of plaintiffs or defendant (Alenezi, Atlam, & Wills, 2019; Simou, Kalloniatis, Mouratidis, & Gritzalis, 2015; Zawoad, Hasan, & Grimes, 2015).Soltani and Navimipour (2016) Establishing a customer link paves way for a lasting relationship and successful management of customer relationships is driven by technology. Badwan, Al Shobaki, Naser, and Amuna (2017) the application of the electronic method can enhance customer loyalty, satisfaction good service delivery, and retention. Aggressiveness in business in terms of market strategy can be amplified using big data to send information via communication devices to target client(Anshari, Almunawar, Lim, & Al-Mudimigh, 2018).The complaint and concerns of users in the acceptance of cloud technology were hinder due to security threats and lack of trust in cloud computing(Ferrer & i Montanera, 2015).

Cloud technology does not provide users of the cloud means of verifying and checking that their information's are not tainted(Moussa et al., 2018).Müller, Ludwig, and Franczyk (2017); (Razaque & Rizvi, 2017). Literature has shown that many organization avoids using cloud computing due to data security challenge. To protect the integrity of data and to satisfy customers on the cloud platform, some mechanisms needed to be put in place, the inclusion of TPA can also be a threat to cloud users(Razaque & Rizvi, 2017). The deployment of cloud system in the building of customer relationship has an advantage but resolving issues such as trust and security have a major challenge in cloud environment (Simou et al., 2015). Fernandez, Monge, and Hashizume (2016). One factor of concern to establish good customer relationships is for the vendors to provide adequate security reference architectures (SRAs).In personalization and customization of services for CRM a big data is required to enable the business environment to be more aggressive, competitiveness and coming up with marketing strategy through the adoption a social media(Anshari et al., 2018). Adoption of cloud and subsequent deployment of cloud computing in CRM has potential in improving service delivery making service available and reliable(Ferrer & i Montanera, 2015).The emerging of cloud technologies has assisted many organizations to restructure their business strategies(Rafiq et al., 2014). Making trust an ultimate factor in the cloud environment can inform decision-making for its deployment in an organization (Adjei, 2015)

2.1 Gaps in Liteture

One thing that can be done to establish build relationship between the users of cloud and cloud providers is to have a mutual understanding of nature, topology of the service being provided and develop a mechanism that is capable of establishing trust, confidence, transparency of security of data in the cloud. Kumar and Pradhan (2018) Instituting trust between the users and service providers can stimulate long-term business relations. In Fig.3&2 we developed a conceptual idea for a framework for CRM mechanism and also modified a conceptual model for authenticating and verifying the trustworthiness for the originality of the user's information. If a third party auditor (TPA) is used, a program can be developed to checkmate the activities of TPA and to save guide the integrity of the data. TPA can also be vulnerable and a potential threat to users information(Razaque & Rizvi, 2017).

3. CONCLUDING REMARKS

Building a customer relationship in the cloud environment cannot be overemphasized in this digitalization era. The deployment of cloud technologies has the capacity to enhance business efficiency and promote effective performance. Building customer relationships is a way of given satisfaction and value to cloud users while maintaining cordial relationships, however, in doing these it is necessary for the stakeholders to harmonize and fashion-out mechanisms that could guarantee user's data and information's on the cloud. Additionally, insourcing for provider's support trusted service provider is sought for. The conceptual model in Fig.2 was proposed to detect information transmissions and to detect the characteristics behavior of the stakeholders secondly, the model was designed to curtail the activities of the service provider (TPA) considered a potential threat to the system and protect the integrity of the information being transmitted via the cloud. The study also proposed a conceptual idea for the framework for the CRM mechanism in Fig.3 this is aim at establishing a good synergy relationship between the stakeholders and injecting KM into the management of the business to fast-track better decisions. We hope our efforts in this study will help remodel building CRM in cloud environment of today's emerging technologies towards solving future challenges.

4. FUTURE RESEARCH DIRECTION

We intend to develop methods and techniques capable of curbing the activities of potential threats to user's data and information. The objective is to provide a secure environment and to attract more users into embracing cloud technologies in the business environment. Our efforts will lead to the development of a system that can achieve the following:

- The integration of power sensors that can prohibit unauthorized users from accessing other user's information.
- Providers should provide a well-secured network to guide against malicious intent from accessing user's information.
- Trusted TPA with certified credentials should be outsourced to take responsibility for support services rendered to the customer.
- The providers must be able to provide adequate security measures and assure the users of the protection of data and other information in their custody.
- Adherence to transparency is very key for the stakeholders in the business blockchain.

REFERENCES

1. Adjei, J. K. (2015). Explaining the role of trust in cloud computing services. *info*.
2. Alenezi, A., Atlam, H. F., & Wills, G. B. (2019). Experts reviews of a cloud forensic readiness framework for organizations. *Journal of Cloud Computing, 8*(1), 11.
3. Almorsy, M., Grundy, J., & Müller, I. (2016). An analysis of the cloud computing security problem. *arXiv preprint arXiv:1609.01107*.
4. Anshari, M., Almunawar, M. N., Lim, S. A., & Al-Mudimigh, A. (2018). Customer relationship management and big data enabled: Personalization & customization of services. *Applied Computing and Informatics*.
5. Araujo, J., Maciel, P., Andrade, E., Callou, G., Alves, V., & Cunha, P. (2018). Decision making in cloud environments: an approach based on multiple-criteria decision analysis and stochastic models. *Journal of Cloud Computing, 7*(1), 7.
6. Badwan, J. J., Al Shobaki, M. J., Naser, S. S. A., & Amuna, Y. M. A. (2017). Adopting technology for customer relationship management in higher educational institutions.
7. Faed, A., Wu, C., & Chang, E. (2010). *Intelligent CRM on the Cloud.* Paper presented at the 2010 13th International Conference on Network-Based Information Systems.
8. Fernandez, E. B., Monge, R., & Hashizume, K. (2016). Building a security reference architecture for cloud systems. *Requirements Engineering, 21*(2), 225-249.
9. Ferrer, A. J., & i Montanera, E. P. (2015). *The role of SLAs in building a trusted cloud for Europe.* Paper presented at the IFIP International Conference on Trust Management.
10. Gamaleldin, A. M. (2013). An Introduction to Cloud Computing Concepts. *Software Engineering Competence Center*, 2.
11. Huth, A., & Cebula, J. The basics of cloud computing (2011): carnegie Mellon University. Produced for USCERT, a government organiztion.
12. Kumar, V., & Pradhan, P. (2018). Comprehensive three-layer trust management model for public cloud environment. *International Journal of Business Information Systems, 28*(3), 371-391.
13. Lee, K. (2012). Security threats in cloud computing environments. *International journal of security and its applications, 6*(4), 25-32.

14. Lin, C., Su, W.-B., Meng, K., Liu, Q., & Liu, W.-D. (2013). Cloud computing security: architecture, mechanism and modeling. *Chinese journal of computers, 36*(9), 1765-1784.
15. Manikyam, N. R. H., & Kumar, D. S. M. (2017). Methods and techniques to deal with big data analytics and challenges in cloud computing environment. *International Journal of Civil Engineering and Technology, 8*(4).
16. Moussa, A. N., Ithnin, N., & Zainal, A. (2018). CFaaS: bilaterally agreed evidence collection. *Journal of Cloud Computing, 7*(1), 1-19.
17. Müller, A., Ludwig, A., & Franczyk, B. (2017). Data security in decentralized cloud systems–system comparison, requirements analysis and organizational levels. *Journal of Cloud Computing, 6*(1), 15.
18. Okuhara, M., Shiozaki, T., & Suzuki, T. (2010). Security architecture for cloud computing. *Fujitsu Sci. Tech. J, 46*(4), 397-402.
19. R.Kabilan1, D. N. J. (2017). Data Mining withBig Data under Cloud Environment –Opportunities, Issues and Challenges. *International journal of advanced research in computer and communication engineering, Vol. 6*(Issue 2), 179-182. doi:DOI 10.17148/IJARCCE.2017.624
20. Rafiq, M., Bashar, A., & Shaikh, A. (2014). *Innovative trends in knowledge management: A cloud computing perspective.* Paper presented at the Proceedings of the First Middle East Conference on Global Business, Economics, Finance and Banking.
21. Rao, V. V., & Rao, M. V. (2015). A survey on performance metrics in server virtualization with cloud environment. *Journal of Cloud Computing, 2015*(2015).
22. Razaque, A., & Rizvi, S. S. (2017). Privacy preserving model: a new scheme for auditing cloud stakeholders. *Journal of Cloud Computing, 6*(1), 7.
23. Simou, S., Kalloniatis, C., Mouratidis, H., & Gritzalis, S. (2015). *Towards the development of a cloud forensics methodology: a conceptual model.* Paper presented at the International Conference on Advanced Information Systems Engineering.
24. Soltani, Z., & Navimipour, N. J. (2016). Customer relationship management mechanisms: A systematic review of the state of the art literature and recommendations for future research. *Computers in Human Behavior, 61*, 667-688.
25. Sowmya, R., & Suneetha, K. (2017). *Data mining with big data.* Paper presented at the 2017 11th International Conference on Intelligent Systems and Control (ISCO).
26. Srinivas, J., Reddy, K. V. S., & Qyser, A. M. (2012). Cloud computing basics. *International journal of advanced research in computer and communication engineering, 1*(5), 343-347.
27. Tang, C., & Liu, J. (2015). Selecting a trusted cloud service provider for your SaaS program. *Computers & Security, 50*, 60-73.
28. Van Der Werff, L., Fox, G., Masevic, I., Emeakaroha, V. C., Morrison, J. P., & Lynn, T. (2019). Building consumer trust in the cloud: an experimental analysis of the cloud trust label approach. *Journal of Cloud Computing, 8*(1), 6.
29. Wang, L., Kunze, M., Tao, J., & von Laszewski, G. (2011). Towards building a cloud for scientific applications. *Advances in Engineering software, 42*(9), 714-722.
30. Zawoad, S., Hasan, R., & Grimes, J. (2015). LINCS: Towards building a trustworthy litigation hold enabled cloud storage system. *Digital Investigation, 14*, S55-S67.
31. https://www.google.com/search?client=firefox-b-d&q=what+is+E-CRM