Data Security in Decentralized Cloud Systems: A Case for the Deployment of Blockchain Technology

Abdul, M.M. & Longe, O.B. Phd
School of IT & Computing, American University of Nigeria, Yola
Academic City University College, Accra, Ghana
E-mails: abdul.m@aun.edu.ng; Olumide.longe@acity.edu.gh

ABSTRACT

The technological advancement and growth of the cloud computing technologies is changing network service provisioning and operation. Cloud based services represented as XaaS where X refers to service offering such as Platform, Software and Infrastructure as a service, provides flexible on-demand provisioning along with its security concerns that goes with the adoption of the cloud computing. Despite all the advantages of adopting the cloud computing option, the security and privacy of the clients' data cannot be overlooked. Understanding these security concerns is a fundamental requirement to choosing the cloud solution. This paper focuses on the use of Blockchain technology to mitigate the security challenges of the cloud computing. Literature reviews have discussed other security options for the cloud, but little discussions have centered on the adoption of the Block Chain technology to secure the cloud and open doors for future research of cloud computing using smart contract.

Keywords: Blockchain, Distributed Database Systems, Data Integrity, cryptography, Cloud Infrastructure Security, Confidentiality, Distributed Ledger

Proceedings ReferenceFormat
Murtala, M.M. & Longe, O.B. Phd (2021): Data Security in Decentralized Cloud Systems:
A Case for the Deployment of Blockchain Technology. Proceedings of the 27th iSTEAMS Multidisciplinary Innovations & Technology Transfer (MINTT) Conference.Academic City University College, Accra, Ghana. June, 2021. Pp 135-142 www.isteams.net/ghana2021. DOI - https://doi.org/ 10.22624/AIMS/iSTEAMS-2021/V27P13

1. INTRODUCTION

The evolution of Cloud computing over the years has changed the way Information Technology infrastructure is being deployed across the globe, utilizing a network of interconnected remote servers and storage hosted on the internet and distributed at different regions of the world to store, manage and process data rather than limiting ourselves to the available onsite computing resources. Unlike the old days when operating system is married to the physical hardware and a hardware component failure can bring down the whole machine, the cloud computing service model has Software as a Service(SaaS) at the top of the layered stack, Infrastructure as a Service(IaaS) and Platform as a service(PaaS) at the base. With the cloud computing technology, IT resources can be allocated based on the needs and can be upgraded as the need arises. Security and management of the cloud remains the function of the service provider. Bharadwaj, Bhattacharya, and Chakkaravarthy (2018) predict that 92 percent of world data will be managed on the cloud by 2020 and that cloud workload will increase 3.2 times in the same period.

As more organizations migrate to the cloud, the security experts need to work more on security strategies on how to secure the data and applications hosted on the cloud as most businesses that would have wanted to migrate to the cloud are skeptical of the security and integrity of the cloud infrastructure (Müller, Ludwig, & Franczyk, 2017). The German privacy laws make provision for data security applicable to private individuals and not very suitable for reliable protection of business data (Müller et al., 2017). The security in a distributed cloud architecture has become a major challenge in the infrastructure development and design of Distributed cloud architecture. However, little studies or none have been carried out in the integration of Blockchain Technology to secure the Distributed Cloud computing system. In this study, we contend that it is important to understand how the Blockchain Technology can be deployed to salvage the security challenges in the Distributed cloud computing system.

This study is motivated by the quest to answer the question: "How must a cloud-based computing infrastructure be designed and integrated in a decentralized information system and be built to guarantee cloud user their privacy laws and data integrity?" (Müller et al., 2017).

1.1 Problem statement

A major challenge of decentralized cloud computing is the security implementation with the growing dependence of organization data to the cloud. Maintaining confidentiality, integrity, authentication, privacy and access control, authorization to data must be maintained and hence, the need for security infrastructure that protects the Integrity and security of the data needs to be researched. Most studies have discussed security challenges in the cloud computing environment, but little or no studies have discussed the protection of the cloud data using the Blockchain technology with increased transparency in the security architecture of the cloud.

Blockchain: as the name implies, is a growing linked-list of digital events of transactions verified by majority of consensus of participants in the network, with a timestamp, and transaction data making blockchain resistant to data modification (Crosby et al., 2016). The data in a blockchain is immutable, once written, the committed data cannot be changed without changing all the subsequent block in the list making the technology more secured, considering the nature of the distributed design with very high Byzantine fault tolerance. It is a decentralized database infrastructure which stores data as transactions.

1.2 Research Thrust

The aim and objective of this study is to explore the suitability of a decentralized and distributed security approach to cloud computing compared to the centralized security approach with its featured single point of failure, redundancy, availability and to achieve self-healing capabilities for the cloud infrastructures. The current security approach to cloud computing is not immune to attacks such as distributed denial of services (DDOS) attack resulting in reliability and availability as a major concern. (Ahmed, 2018). Distributed approach to computing will require distributed security architecture to address its security challenges as obtainable in the blockchain distributed security architecture. Cloud computing architecture is distributed, but the security architecture is not fully distributed as currently deployed in the block chain distributed networks. (Ahmed, 2018) The security architecture to the cloud computing must be fully decentralized with no central that can result in a single point of failure should the core be compromised. (Ahmed, 2018).

Also, self-healing is another important security architecture that needs to be extensively researched. Whereby should any part of the system be compromised, the system should be able to recover from the compromise and heal itself. The advancement in deep learning algorithm aspect of machine learning in the field of Artificial Intelligence would be a good solution approach to self-healing.

1.3 The Four Pillars of Blockchain Technology

The Blockchain Technology has gained widespread acceptability due to four main properties of the technologies (Memon, Hussain, Bajwa, & Ikhlas, 2018).

- **Decentralization:** in which systems have no central core of authority to dictate other participants in the network. Every participant in the network can access and confirm any new transactions in the network.
- **Transparency**: individual identity is hidden via a complex cryptographic and represented only by their public address while the person's real identity remains secured increasing the level of transparency and accountability of the transactions.
- **Immutability**: once transaction is committed into the blockchain, it cannot be changed.
- **Trustless**: which is one of the greatest appeals of blockchain is in its decentralized nature, no third party to be relied upon in order to keep fund safe.

A consensus mechanism to achieve validity of transaction in Blockchain includes:

1. **Proof of work**: the most common consensus mechanism used to synchronize millions of decentralized nodes rely on computing power to solve complex mathematical puzzle ensuring that funds are always safe, preventing arbitrary dilution of the transactions (Memon, Hussain, Bajwa, & Ikhlas, 2018).
2. **Proof of stake**: There has been a tremendous shift from Proof of work to Proof of stake as it requires a user or a forger to show ownership to a certain level to qualify him to earn the mining power and the forger will have to stake his investment in order to be in a position to forge and validate transactions and creating new blocks in the chain (Memon, Hussain, Bajwa, & Ikhlas, 2018).

1.4 Basic Terms

The term 'decentralized information systems' defines an interconnected information system technology whereby no single entity is the sole authority (www.computerhope.com/jargon/d/decentral.htm) and decentralization of infrastructure described is externalized across geographical locations/region of the world (Müller et al., 2017). The term 'cloud computing' describes an on-demand availability of networked computer systems resources such as storage (cloud storage) computing power where the people do not need to own the resources and without having to worry about the management of the resources. This includes data centers available to individuals and corporate entities over the internet(Wikipedia).

1.5 The difference between Cloud and Traditional computing

The traditional multi-layered architecture consists of the presentation tier, application logic tier, and the database tier and each tier runs on a dedicated server in a static perimeter fixed at a particular location. While the cloud on Information Technology paradigm provides scalability, dynamic provisioning, fault tolerance and geo availability.

1.6 Cloud Security

Public Cloud security is a shared responsibility between the customer and cloud service providers. While in the private cloud, the customer is solely responsible for all aspects of security. The cloud service provider is responsible for the security of the shared infrastructures such switches, hypervisors, network storage, firewalls, routers, load balancers etc. (Kumaraswamy, 2011)

1.6 Identity security at the cloud

The technologies for managing and certifying customers' identity in the cloud is mostly based on a centralized architecture from third party service providers and trusted authorities' operators (Goodell & Aste, 2019).

1.7 Effect of threats and vulnerabilities on the cloud

Any event, accidental or intentional, that could yield desirable consequences to a person, organization or resources is referred to as a threat. (Ahmed, 2018). Barriers to cloud computing are security issues and loss of integrity (Ahmed, 2018). Security is one of the biggest challenges for cloud architecture (Ahmed, 2018), virtualization introduces security challenges that can affect the whole cloud architecture (Ahmed, 2018). In the cloud deployment architecture model, the functionality of the infrastructure at a particular level e.g Security as a service (SaaS) and security depends on the reliability of the level (e.g Platform as a Service (PaaS). The cloud service dependency model makes cloud security an important point to look at.

A lower layer model may have little or no control over the security architecture of a higher layer, for example, the Infrastructure as a service has little control security architecture beyond its own layer, which exposes the system to security breaches(Ahmed, 2018). Security perceptions are linked to trust, risks and threat which imply the sensitivity of data security. The cloud computing resources are under a third party management and ownership, outsourcing such resources exposes the cloud computing to threat and vulnerability as the data exist outside the scope and control of organization firewall (Ahmed, 2018).

1.8 Importance of cloud security

The most important aspect of the cloud is the security architecture of the cloud as it covers the integrity of the cloud architecture. (Ahmed, 2018). In cloud computing, resources and service provisioning are based on a distributed approach where resources and data are distributed among different servers interconnected via the cloud at different locations or regions. This approach of resource distribution in the cloud makes the system complex to administer and manage, also making the cloud a target for attackers. (Ahmed, 2018)

2. LITERATURE REVIEW

This Literature review section reveals facts based on the analysis of many authors' work as indicated below:

Sharma, Ahuja, and Goyal (2018) present Blockchain ability to enhance security and compare the various platforms on which it can be deployed or implemented for secure infrastructure of cloud computing. Wang, Dong, Wang, and Yin (2019) discuss the analysis of past work on providing data security in a network involving data brokers via Blockchain and Artificial Intelligence. It evaluates past methodologies and introduces newer version of maintaining the integrity of data in a network environment. Sun (2018) discusses cloud computing from the dimension of computer security, network security and information security to highlight the vulnerabilities of cloud architecture model. Kumar and Goyal (2019) discusses cloud security requirements, vulnerabilities and threats in cloud computing and counter measures to mitigate these known threats and highlights security challenges in related fields such as Software defined Network, Network Function Virtualization, Internet of things and trust-based security model.

Kumar (2018) discusses ways to adjust blockchain safety to distributed calculating and its data protecting arrangement feature intended to incapacitate discretional altering of stored data and avert hacking amidst data exchanges including virtual money. Kirti, Gupta, Biswas, and Turlapati (2017) discuss the techniques for cloud security monitoring, threats intelligence and remediating the security threats using a first portion of activity data, identifying a threat using the second portion activity data and selecting a security policy to mitigate identified threats. Choo, Rana, and Rajarajan (2017) discuss cloud security engineering, theoretical foundation and practice that enable security to be engineered and practice in cloud system and services. Memon, Hussain, Bajwa, & Ikhlas, (2018) enlighten the use of Blockchain technology beyond bitcoin and also reveal the evolution, concept, mechanisms and challenges of implementing blockchain technologies in the real world application. Basu et al., (2018) discusses a survey on cloud security challenges and countermeasures to mitigate the identified threats and the lack of common framework that generalize the concept of cloud security and its requirement.

The cloud computing concept, as well as the deployment approaches including cloud service architecture, were explored during the literature review. One of the major reviews are the security architecture in cloud and distributed computing with regards to its existing security models. (Ahmed, 2018). Cloud computing have recently become very popular computing approach as it offers a significant cost reduction using highly scalable software and hardware solutions bringing flexibilities to its users. (Ahmed, 2018). A good cloud computing model is considered to be a very important component of cloud computing requirements and deployment. (Ahmed, 2018). All the above mentioned benefits come with their shortcomings especially from the security perspective e.g the apple iCloud security breach (apple, 24; PCWorld, 2014). The security breach on Sony cloud (Bloomberg, 2011a), JPMorgan cloud server breach (CNN,2014; Computerworld, 2014). The distributed and open structure of the cloud computing opens it up for attack. New security architecture has been suggested to sustain its acceptability (Ahmed, 2018).

2.1 The Cloud Service Architecture

The cloud deployment service model defines anything providers offer as services (XaaS). It represents layered high-levels of abstraction that enables multiple cloud users. (Wikipedia). The cloud service models include:

Infrastructure as a service (IaaS) enables computing resources and storages to be delivered as a service. Clients are provided resources to provide access to the virtual servers, these computing resources are used by the clients to deploy any software set-up. In this model, only the infrastructure is provided to the customer, the operating system and the supporting license that will run on the platform remains under the ownership of the clients. Hence, the client has full control over whatever they choose to deploy on the platform. Clients can exploit the benefit of the platform but do not have control over the platform. (Kavis, 2014)

Platform as a service (PaaS) offers the clients the facilities for deploying application without the complexity of owning the underlying computing infrastructure such as the operating systems and its hardware, but control over the client's application and setup requirement for the application hosting environment (Kavis, 2014).

Software as a Service (SaaS) is a cloud service model which is a complete service provider software application delivered as a service including all the underlying computing resources such as the operating systems and the hardware infrastructures. The clients only configure some application specific settings and manage the users of the application. (Kavis, 2014)

2.2 The Cloud computing model

The most important step to take for a successful cloud computing deployment is the choice of a suitable cloud computing model, and organization needs to examine their date precisely before deciding on the best option of cloud computing in order to avoid failure of implementation. There are 4 adopted models in cloud computing deployment based on the physical location and distribution:

1. **The Private cloud**: this deployment model resides with the organization and the cloud computing service is not accessible to the public. It is the most secured deployment model as the organization data processes are controlled and managed by the organization internally. The cloud infrastructure owned and managed locally by the organization to flavour of private cloud include on-the-premise private cloud and externally hosted-private cloud. Some characteristics of private cloud include:

i. Enhanced security measure.
ii. Dedicated resources and
iii. Better customizations (Diaby & Rad, 2017)

2. **The public cloud**: this model comes with various featured services based on pay-as-you-go or on-demand basis. This model is designed to provide boundless computing resources to organizations via the internet of interconnected nodes. It is hosted and owned by a third party service provider. Basic characteristics of a public cloud architecture are:

i. Flexibility and elastic environment.
ii. freedom of configuration settings and self-service.
iii. on-demand service and
iv. Reliability and availability. (Diaby & Rad, 2017)

3. **The hybrid cloud model**: this model combines the best of private and public cloud models which is shared among different organizations with similar requirements and interests. It can be managed by a third-party service provider or internally managed. Characteristics of this model include:

i. Optimal use of resources.
ii. data center consolidation and
iii. Availability (Diaby & Rad, 2017)

4. **The community cloud model**: this model infrastructure is supervised and used by different organizations with similar core businesses, shareable infrastructure such as hardware and software to reduce the overall running cost. Academic cloud is a very good example of this model (Diaby & Rad, 2017)

3. VIRTUALIZATION

Virtualization is a technology that enables the creation and deployment of virtual machines that can be referred to as the guest while the physical machine from which the virtual machine is created is referred to as the host. A core characteristic of virtualization is the multi-tenancy model that enables sharing of computing resources among multiple clients. It enables a single computer machine to provide a platform for multiple clients.

4. CONCLUSION AND FUTURE WORK

Data Security in a cloud computing setting should be fully distributed and decentralized as identity management can be carried out with the help of a Blockchain technology which relies upon network consensus among participants instead of platform operators which relies on third party operators and trusted authorities. The Blockchain system will provide participants a common view of the transaction, ensuring transparency of the transaction history with no single authority or trusted authority in control. In this paper, there have been some related works that have discussed the use of blockchain in securing distributed computing system and identifies their flaws especially the Scalability issue with the blockchain technology which executes on average, 10 transactions per seconds due to its consensus mechanism. This major setback of the blockchain technology in securing distributing computing system will be an area for future research work. Also, we believe that continued integration of Blockchain in cloud computing system for enhancing security and integrity of the infrastructure is yet to be fully explored.

REFERENCES

1. Ahmed, M. (2018). Ki-Ngā-Kōpuku: a Decentralised, Distributed Security Model for Cloud Computing. Auckland University of Technology
2. Basu, S., Bardhan, A., Gupta, K., Saha, P., Pal, M., Bose, M., Sarkar, P. (2018). Cloud computing security challenges & solutions-A survey. Paper presented at the 2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC).
3. Bharadwaj, D. R., Bhattacharya, A., & Chakkaravarthy, M. (2018). Cloud threat defense–A threat protection and security compliance solution. Paper presented at the 2018 IEEE International Conference on Cloud Computing in Emerging Markets (CCEM).
4. Choo, K.-K. R., Rana, O. F., & Rajarajan, M. (2017). Cloud Security Engineering: theory, practice and future research. IEEE transactions on cloud computing, 5(3), 372-374.
5. Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain technology: Beyond bitcoin. Applied Innovation, 2(6-10), 71.
6. Diaby, T., & Rad, B. B. (2017). Cloud computing: a review of the concepts and deployment models. International Journal of Information Technology and Computer Science, 9(6), 50-58.
7. Goodell, G., & Aste, T. (2019). A decentralised digital identity architecture. Frontiers in Blockchain.
8. Kavis, M. J. (2014). Architecting the cloud: design decisions for cloud computing service models (SaaS, PaaS, and IaaS): John Wiley & Sons.
9. Kirti, G., Gupta, R., Biswas, K., & Turlapati, R. R. S. (2017). Techniques for cloud security monitoring and threat intelligence. In: Google Patents.
10. Kumar, R. (2018). Security in Cloud Computing Using Blockchain Technology. AIJR Proceedings, 422-439.
11. Kumar, R., & Goyal, R. (2019). On cloud security requirements, threats, vulnerabilities and countermeasures: A survey. Computer Science Review, 33, 1-48.
12. Kumaraswamy, S. (2011). Introduction to Cloud Security Architecture from a Cloud Consumer's Perspective. InfoQ. Dec, 7.
13. Memon, M., Hussain, S. S., Bajwa, U. A., & Ikhlas, A. (2018). Blockchain beyond bitcoin: Blockchain technology challenges and real-world applications. Paper presented at the 2018 International Conference on Computing, Electronics & Communications Engineering (iCCECE).

14. 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), 1-9.
15. Sharma, S. G., Ahuja, L., & Goyal, D. (2018). Building secure infrastructure for cloud computing using blockchain. Paper presented at the 2018 Second International Conference on Intelligent Computing and Control Systems (ICICCS).
16. Sun, X. (2018). Critical security issues in cloud computing: a survey. Paper presented at the 2018 IEEE 4th International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing,(HPSC) and IEEE International Conference on Intelligent Data and Security (IDS).
17. Wang, K., Dong, J., Wang, Y., & Yin, H. (2019). Securing data with blockchain and AI. IEEE Access, 7, 77981-77989.