



Cloud Security And Electronic Transaction Security: Merger For Online Crime Mitigation

Abdullahi Haruna Ishola

Department of Sociology, Lagos State University, Ojo, Lagos State, Nigeria

Corresponding Author: haruna.abdullahi@lasu.edu.ng

Article Information:

Received: February 02, 2023, Accepted: May 12, 2023, Published: June 10, 2023

Abstract

The insecurity of cloud leads to loss or exposure of vital information thereby threatens online transactions. These unfortunate happenings resulted in financial loss, reduced patronage of cloud services and investment diversions. Therefore, this chapter assesses cloud security and electronic transaction security. The chapter adopts qualitative research method, data were sourced secondarily through content analysis of edited books, peer-reviewed journals and credible online resources. It was descriptive in nature and thematically analyzed. The paper anchors on routine activity theory and broken windows theory. Findings revealed that cloud activities are under internal security threats of the cloud service providers and external threats of other users of cloud services. The chapter recommends proper background checks for the staff of the cloud service providers, public enlightenment on cloud security protocols. This chapter will be useful to individuals, cloud services providers, NGOs and researchers in the field of online crimes.

Keywords: Security, Cloud, Online-crimes, Protocols, Threats, Data

1. Introduction

Security of online transactions is highly essential especially in e-commerce. In the 21st Century, most transactions are going digital to ease task of physical transaction and to save time and there is need for online transaction to be fully secured to gain trust from customers and for increase in customer patronage. security of online transactions is necessary for the sustenance of the online transaction's security for proper confidence building in the whole exercise. One reliable means of instilling confidence in online transactions is through cloud security. Cloud security is another digital storage mechanism that has resources for data storage and retrieval when it is necessary. In this era of online transaction, business are conducted online to take the advantages of globalization and international competitive advantage and public sectors are not exempted from the usage of cloud security as well. The corporate entities, public sector administrators as well as individuals are actively hooked up to cloud for safety and protection. But despite the numerous advantages of cloud security, the structure is threatened by internet crimes which may eventually result to failure



to ensure appropriate information security and privacy protection and can lead to potential loss of business. The cybercrime could come from internal and external sources.

The internal sources of criminal activities are major security challenges because without vital information on the cloud protocols, resources, processes and procedures. Whenever, this problem exists, the cloud administrators and investors are apprehensive about the security of the resources. The different mechanisms are deployed to cloud community to facilitate security of data also affects the financial security. And to instill confidence in the cloud and sustain patronage and usage. These mechanisms work synchronously to enhance financial security of online transactions. Shayini (2016), investigated enhancement of the security of Modern Information Communication Technology systems with multimodal biometric cryptosystem and continuous user authentication. Meanwhile, Haghighat (2015) investigated Cloud ID, Trustworthy Cloud-based and Cross-Enterprise Biometric Identification Expert Systems with Applications. Sadha and Lalitha (2015), examined cyber casing as challenges and taxonomy to address the problems in cloud system through GMSP. From the best knowledge of the author, no study has been conducted on cloud security and Online transaction security as means of mitigating online- crimes. On this basis of this, this study is necessary to fill the knowledge gap. The specific objectives of the study are; to verify the types of cloud system; the problems of cloud systems.

2. Literature Review

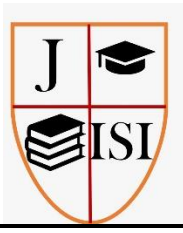
Meanings of Cloud Security. This refers to established policies, applications, high-tech and controls that are used in protecting data, software applications, online services and related infrastructures of cloud computing.

Categories of Cloud Computing. The following are the categories of cloud computing and cloud services:

Category of cloud

Private cloud: All clouds turns to private clouds when the underlying Information technology infrastructure is dedicated to a single customer with completely isolated access. Authorized users can access, utilize and store data in the private cloud from anywhere exactly the way public cloud can be assess.

Public clouds: Public clouds are cloud environments that mainly created from Information Technology infrastructures that are not owned by the end users. Examples are: IBM Cloud, Google Cloud, Alibaba Cloud, Amazon Web Service etc. It is often used for software development and collaborative projects. The essential infrastructure and operating system of public cloud remain under the full control of the cloud provider and customers are restricted to the users are restricted to the usage based on the rules and regulations of the provider which may cause difficulty to users repatriating their asset if need arise for change of provider. Customers are susceptible to security issue in the cloud architecture exposing them to risk especially when dealing with electronic transactions. Cloud environment is solely dedicated to a single user or group. Private clouds can only be expanded through addition of more hardware and storage capacity which can result to difficulty in scale operation quickly and frugally when need arise for it use for business.



Hybrid clouds: this category of cloud combines public cloud with private and are designed to allow seamless interaction of two platforms. Though, combination of two clouds may result to high cost

Multiclouds: Multicloud combines a private cloud with multiple public cloud services in order to meet organizations computing needs. All hybrid clouds are multiclouds but not all multiclouds are hybrid cloud. Multiclouds become hybrid clouds when multiple clouds are connected by some form of integration or orchestration. Multi-cloud infrastructure provides flexible enterprises needed to innovate at speed yet it has management issue due to wide range of cloud services an enterprise use. Inability in the part of the system management can increase cost and thereby, affect business agility. Also, deployment of multi-cloud could be a bit complex to configure.

Communities: Communities do have data that required storage, there are different association at the communities' level that needs better storage. This could come in terms of community development associations data, monetary contributions, flood, agricultural out and government intervention.

Category of cloud services

Cloud services are the tools, platforms and/or software that are hosted by third party

SaaS: This denotes Software as a service, is a software licensing and delivery structures. It has a license as a subscription with absolute central control. The software design to facilitate power host and ensure availability to customers at all times. Examples are: Microsoft office 365, Cisco WebEx, Salesforce, GoogleApps etc.

PaaS: This stands for Platforms-as-a-Service; it is a type of cloud computing structure. In this type of cloud computing, cloud service provider delivers reliable and closed-monitored protocols for customers, for onward development, administration, business applications and maintenance of the infrastructure such as software development processes.

IaaS: This is an abbreviation for Infrastructures as a service. This type cloud computing is a type in which virtualized computing services are provided across the internet. It is a cheaper than other resources provided.

General Architecture of Cloud Computing

The architectural design of cloud computing can be classified into three: the infrastructure-as-a-service (IaaS) is the lowest layer and it serves as the background layer over which other layers are built. Platform-as-a-Service (PaaS) layer is the middle layer that deals with development and hosting of users' application while software-as-a-service (SaaS) is the most upper layer of the architecture which provides an application that works as a service on demand. The architecture is as shown in Fig. 1.

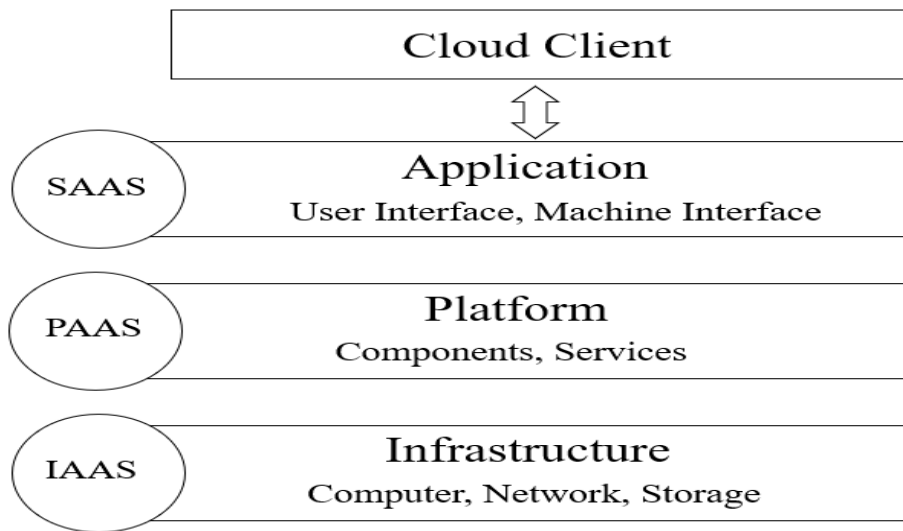


Fig. 1: Service model in cloud architecture (Lubna *et al.*, 2019)

Duality Of Responsibilities For Security In Cloud Computing

Transaction through cloud need very robust cloud security due to constant security threat for effectiveness of security in cloud computing. The responsibilities fall on the two major stakeholders. These are as follows,

The Cloud Service Providers: It is the responsibilities of service providers to infrastructures that will guarantee the security of data and applications of the various categories of client. This will sustain the credibility and confidence various users imposes on the cloud service providers, and also ensure competitiveness and business continuity of cloud service providers.

Cloud Users: When cloud service providers satisfy their roles in ensuring safety and protection of the cloud platforms. The users should also reciprocate the gesture, by ensuring strengthening of security processes through strong passwords and reliable authentication processes.

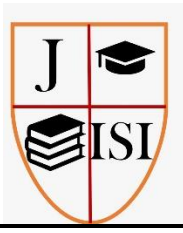
Data Security By Cloud Service Providers

To further strengthening data and application security of clients, the cloud service providers offer the following services.

Data Isolation. This is a process that involves giving unique identity for a particular. It limits unauthorized access to another client's data.

Logical

Validity of Data. This takes the shape of verification of data that will be stored on cloud platform to prevent storage of data may compromise the integrity of the cloud system. It enhances the security of the entire platforms.



Background Checks. The background checks of every employee of the cloud security company is essential to avert tampering with the data and other resources handled by cloud service providers. To do this, cloud companies may contract the background checks to security companies or they may do it by themselves. The criminal history or records of employees will be investigated. The kind of character they exhibit in the community and family will also be examined.

Virtualisation: This changes the interaction between Operation System and physical hardware. It enhances security of hardware and other resources. It covers computing, storage and networking processes.

Dimensions of Cloud Defensive Mechanisms

Deterrent Protection. In cloud security this type of protection gives warnings to prospective intruders and inform them of the dire consequences of unlawful or unauthorized consequences of trespass.

Detective Protection. If an intruder escapes the first security hurdles by ignoring warnings and eventually penetrated into cloud security structures. The detective mechanisms inbuilt security systems that points out unacceptable compromise of the cloud security system. This mechanism exposes staff who have compromised the standard.

Preventive Mechanism. This guides against the activities of intruders are prevented through robust defensive mechanisms. This takes the shape of passwords, two-way authentication and others.

Corrective Mechanisms. This type of defensive mechanism rectifies the anomalies created by intruders by reinstalling normalcy in the system. It prevents the possibility of destabilizing the cloud computing system.

Various Cloud Computing Attacks And Possible Solution

Despite the fact that Cloud Computing (CC) has defensive mechanism has discussed above, there are still some attacks that occur on each of the service deliveries like PaaS, IaaS and SaaS. The likely attacks are as discussed below:

1. **Security attack on SaaS layer:** The SaaS layer is well known for security measures and is well managed remotely by one or more providers and it is most susceptible to data related security problems like data backup, data management, data locality, data authentication as well as data identity management. Among likely security attacks on SaaS cloud layer are:
 - (a) Denial-of-Service attack (DOS) which is a pronounced attack in cloud computing. It operates by sending thousands of requests to victims over the internet and thereby exhausts all the resources of the victim. It has the capability of reducing users' bandwidth, disturbing service to a specific system as well as prevention of the user from being able to access or use the cloud service. DOS attack can be prevented by using strong authentication and authorization as well as using filter-based approach.
 - (b) Structured Query Language Injection attacks: Database and web servers are important aspect within the cloud environment. Structured Query Language is mainly programming and management of data in relational database. This kind of attack usually steals

information like username and password from web application by introducing malicious code into the web application as a user input. Upon successful acceptance, the attacker gain unauthorized access and have the capability to adjust the database design to suit their aim. Usage of appropriate filtration method to sanitize user input among other is a way to protect this attack.

- (c) Authentication attack: this kind of attack is basically used to gain access to cloud applications. Authentication is majorly to avoid unauthorized access to cloud services and in this kind of attack, the attackers target the mechanisms used to authenticate the system by adopting various encryption and decryption methods of bridging the confidential manner of transferring data. Usage of strong passwords and better authentication mechanism as well as encryption of communication channels to secure authentication tokens are possible solution to the problem.

2. Security Attacks on PaaS cloud layer: In PaaS, the user controls the applications that run in a cloud environment and the cloud environment is in charge of the hardware, network substructure and operating systems. Among various issues in PaaS is lack of validation, anonymous signs, and service fraud. Below are parts of the security attacks on PaaS cloud layer:

- (a) Phishing attacks: This type of attack usually affects both providers and users in PaaS cloud model. Phishing attacks operate by manipulating retrieved personal information from a legitimate user and redirecting the user to a spoofed link. All the three layers IaaS, PaaS and SaaS are usually affected by this type of attack. It can be solved by the use of browser collaboration and active content filtering.
- (b) Metadata spoofing attacks: Metadata can be defined as data about data which usually contains confidential and sensitive information. Metadata spoofing attack usually affects SaaS and PaaS and the attack could be solved by encrypting information about service functionality and other details.

3. Security attacks on IaaS cloud layer: Security concerns at the virtualized level are major security threats to IaaS computing environment. Some major security attacks on IaaS are:

- (a) Cross-virtual-machine (side-channel) attacks: Within the cloud environment, Virtual machines are easily accessible by tenant users and are the most vulnerable part of the virtualized system. VM attacks are solely meant to get confidential and important information from a victim VM by acquiring side-channel information such as time, cache, heat and power. The attack can be prevented using virtual firewall as well as encryption and decryption.
- (b) VM escape attack: It breaks isolation layer by interacting with the hypervisor. The attacker always make attempt to break down guest operating system or gain to the memory to gain access to the hypervisor or penetrate the functionalities in order to read, write or execute its contents (Lubna *et al.*, 2019). The VM escape attack can be solved by the use of a secure hypervisor and strong configuration of the host-guest interaction.

Challenges Of Dua Service Providers

Published by:

One of the greatest challenges of cloud service providers is maintenance of the security of data and applications of multiple clients at the same time. Once, a cloud service provider has been selected to maintain a client data. Other clients may have access to the data, it is then the core responsibilities of cloud service providers to further strengthening each client's identity. The major challenge of cloud security provider is internal compromise. The staff of cloud service providers' compromise to breach data integrity and warranted the need for cloud service providers to improve on security of data across their platforms.

Online Transactions

The world is going digital, most business and private activities are conducted online. Business organizations, educational institutions, insurance services are conducted online. These enterprises rely on online transactions for their survival and continuity and such trust will be bridged if their data and information is susceptible to cloud computing and online attacks as discussed above.

Table 1: Regions Internet Users by Regions from 2009 to 2019

Year /Regions	Asia	Europe	North America	Latin America	Africa	Middle East	Oceania Australia	Total
2009	764	426	260	187	86	58	21	1,802
Percentage	42.38	23.64	14.43	10.38	4.77	3.22	1.17	100%
2010	825	475	266	205	111	63	21	1,966
Percentage	41.96	24.16	13.53	10.43	5.65	3.20	1.07	100
2011	1,017	501	273	236	140	77	24	2,268
Percentage	44.84	22.09	12.04	10.41	6.17	3.40	1.06	100
2012	1077	519	274	255	167	90	24	2,406
Percentage	44.76	21.57	11.39	11.00	6.94	3.74	1.00	100
2013	1,265	566	300	302	240	104	25	2,802
Percentage	45.15	20.20	10.71	10.78	8.57	3.71	0.89	100
S2015	1,563	604	314	333	313	116	27	3,270
Percentage	47.80	18.47	9.60	10.18	9.57	3.55	0.83	100
2016	1,792	615	320	385	340	133	28	3,613
Percentage	49.60	17.02	8.86	10.66	9.41	3.68	0.77	100
2017	1,938	660	320	404	388	147	28	3,885
Percentage	49.88	16.99	8.24	10.40	9.99	3.78	0.72	100
2018	2,062	705	346	458	456	164	28	4,219
Percentage	48.87	16.71	8.20	10.86	10.81	3.89	0.66	100
2019	2,300	704	346	438	456	164	28	4,454
Percentage	51.64	15.81	7.77	9.83	10.24	3.68	0.63	100

Source: <https://www.statista.com/statistics/265147/number-of-worldwide-internet-users-by-region/> modified by author

From the Table 1, Asian Continent has the highest number of internet users across the years, followed by Europe. African Continent came 4th among the continents, and Oceania Australia came last. The internet penetration gives opportunities for cloud computing because there is no



way one can hook-up to cloud system without internet services. In addition to that, online transactions are integral parts of internet penetration.

Theoretical Framework

To shed more lights on cloud computing and online banking transactions, routine activity theory by Marcus Felson and broken windows theory by George Kelling, routine activity theory states that for crimes to be perpetrated three things are necessary these are motivated offenders, target and reliable guardianship. In this regard, unscrupulous person both internal and external are the motivated offenders, the clients' data are their targets and viable security or defensive mechanisms put in place to defend are the guidance against motivated offenders. Broken windows theory by George Kelling states that in society where minor crimes are not checked; it will leads to major crimes that might consume the whole society. If the activities of online crimes are not regulated. The online criminals may progress to cloud data attacks. There are instances of attacks on cloud data resources by online criminals or fraudsters.

3. Findings and discussions

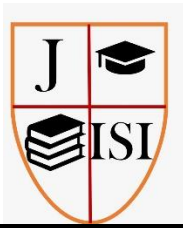
From findings there are a number of people that hooked-up to cloud security structures which includes private, public and hybrid entities. The cloud data service providers are duty-bound to ensure security of data at cloud services (SaaS, PaaS and IaaS) that are being attacked at every level of the cloud model. The online transactions are veritable means of conducting businesses and public transactions online. The cloud security platforms offer deterrent protection as a result of attacks on cloud computing environment and consequences of unauthorized access into users'/ client data. The preventive mechanism will offer the necessary security measures to discourage the activities of online fraudsters who may be making attempt to steal peoples' sensitive data. The corrective control rectifies any danger that intruders might have caused to cloud data centre.

4. Conclusion

The cloud data is a veritable mean of data and applications security in online environment and the security of data on cloud security platforms rebuilds confidence in online transactions. Each country endeavors to increase of its internet penetration.

References

- Sahayini, T (2016). "Enhancing the security of modern ICT systems with multimodal biometric cryptosystem and continuous user authentication". *International Journal of Information and Computer Security*. **8** (1): 55
- Haghighat, M. (2015). "CloudID: Trustworthy Cloud-based and Cross-Enterprise Biometric Identification". *Expert Systems with Applications*. **42** (21): 7905–7916.
- Haghighat, M.; Zonouz, S.; Abdel-Mottaleb, M. (2015). "CloudID: Trustworthy Cloud-based and Cross-Enterprise Biometric Identification". *Expert Systems with Applications*. **42** (21): 7905–7916
- Sudha, K.R., Lalitha, B., and Cyber Casing: Challenges and Taxonomy to Address the Problems in Cloud System Through GMSP. *International Journal of Computer Science and Information Security*. 18(8), 1—10



- Hamid, S., Mahdi, Alsutant ,Qusay, Kanaan K, Robiah, Y., and Rahayu, S., (2018). The Cloud Security and Contemporary World. Journal of Physics Conference Series, 1018(10),
- Alex M.k.(2011).Opportunities and Challenges of Cloud Computing to Improve Health Care ServicesJ Med Internet Res 2011;13(3):e67Journal of Medical Health Research
- Sun, Y., Zhang, J., and Xiong, Y.(2017). Data Security and Privacy in Cloud Computing. International Journal of DistributedSensor Networks: Data Security and Privacy in Cloud Computing, 110, 465—472
- Mamidisetti, G., and Makala, R. (2020). A Novel Data Sharing Model for Cloud Environment using dual key Authentication. International Journal of Cloud Computing, 9(2—3), 295—310
- Morris, K. (2016). Infrastructure as Code: Managing Servers in the Cloud. O`Relly Media, Boston, United State of America
- Ko, R., and Chao, R.(2015). The Cloud Security Ecosystems Technical, Lega, Business and Management Issue, Elsevier Science, Amsterdam, New York
- Erl, T. Cape, R., and Naserpair, A .(2015). Cloud Computing Design Patterns; Prentice Hall, New Jersey, United State
- Summery, M. (2015). The Financial Security Bible. How to Build Wealth and Be Happy, Gildan MediaCorporation, New York City
- Dotson, C.(2019). Practical Cloud Security: A Guide for Secure Design and Development, O`Relly Media, United State, California
- Krutz, R.L ,& Vines , R. D. (2010). Cloud Security and Convenience: Efficiency set Data Protection and Privacy Principles, Packt Publishing, Birmingham, United Sate
- Vacca, J.R.(2020). Cloud Computing Security Foundation and Challenges, CRC Press, Boka Raton Florida
- Gary, M.L. and Victoria, K.K.(2013). Three Steps to Wealth and Financial Security: All that Gitters Isn`t Gold. CreateSpace Independently Publishing
- Herborne, B.Dorotinsky, W., and Bisca, M.P.(2017). Securing=g Development: Public Finance and the Security Sector, World Bank Publishing
- He, D.(2016). Financial Security in China: Situational Analysis and System Design, Springer, United State of America
- vacca, J.R.(2016). Security in the Private Cloud. CRC Press
- Trocata, M.Zhu, S, Y. and Hill, R. (2016). Guide to Security Assurance for Cloud Computing, Springer
- Lubna Alhenaki, Alaa Alwatban, Bashaer Alahmri and Noof Alarifi (2019), Security in Cloud Computing: A Survey, International Journal of Computer Science and Information Security (IJCSIS),Vol. 17, No. 4, April 2019



Copyrights

Copyright for this article is retained by the author(s), with first publication rights granted to the journal.

This is an open-access article distributed under the terms and conditions of the Creative Commons Attribution license (<http://creativecommons.org/licenses/by/4>).

