International Journal of Advanced Trends in Computer Applications
www.ijatca.com

STORAGE SECURITY IN CLOUD COMPUTING CHALLENGES AND SOLUTIONS

[1]Folorunso Olufemi Ayinde *Ph.D*, [2]Alebiosu Omobolade B.
[1]Folorunso Olufemi Ayinde *Ph.D*
Wellspring University, Benin City, Edo State, Nigeria
[2]Alebiosu Omobolade B.
National Open University of Nigeria
[1]dict@wellspringuni.edu.ng, [2]boladealeb@gmail.com

ABSTRACT: *Cloud Computing (CC) is a model that allows shared and configurable computing resources positioned in the cloud with little management effort from the CloudServicesProviders (CSP). However, security, reliability, cost, virtualization, need, on demand service, maintenance, integration, user friendliness legislation and regulations are top priority in the adoption of cloud computing concepts with security being the most important. This paper highlights the challenges of adoption of cloud computing paradigm, examines threats in cloud computing as highlighted by several authors with proposed solutions. The burdens on Cloud Services Providers and the future of this technological shift are also discussed.*

Keywords: Cloud, Computer Security, Data Storage Security, Cloud Solution.

I. INTRODUCTION

The last decade saw tremendous deployment of cloud computing platforms by individuals, small and medium scale enterprises as well as large corporations, this shows a shift from the traditional on-premise Information Technology (IT) infrastructures. Whereas, the concept of cloud computing was first introduced in the 1960s by John McCarthy when he stated that the organization of computation as a public utility will come to fruition someday and he equally explained how this might occur [1]. Hence, in order to properly identify the challenges militating against cloud computing deployment and evaluate each cloud service provider's security architecture with a view of making recommendations. It becomes imperative to evaluate the security of cloud computing.

Markus et al. defined cloud computing as an IT deployment model which is based on virtualization, where services, resources, storage, infrastructure, applications and data are deployed via the internet as a distributed service which could be scalable on demand, provided by one or several service providers and can be priced on a pay-as-you-use basis. He also opined that most of the definition of cloud computing by several authors spans around the features service, hardware, software, scalability, internet, usage-bound payment models as well as virtualization were frequently mentioned [2].

II. LITERATURE REVIEW

2.1 Factors Affecting the Adoption of Cloud Computing

Ezgi and Sona in their study explained and evaluated the factors having effects on the adoption of cloud computing and to predict casual relationships between the factors. Security, reliability, cost, virtualization, need, on demand service, maintenance, integration and user friendliness as explained in the characteristics of cloud computing are the factors discussed by Ezgi and Sona [3]. Additionally, legislation and regulations also play an important role in the adoption of cloud computing paradigm, as legal factors are needed to help predict whether the satisfactory level of legal protections in solving conflicts between cloud services providers and cloud in case problem arises due to natural disaster or hacks.

Radhika and Burkhard described cloud computing as a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or services provider interaction with one of its major benefits of CC as the pay-as-you-go model. Furthermore, their study iterated that to successfully adopt Cloud computing in organizations, it was imperative to evaluate the value and impact of incorporating it into businesses, as taking a decision on whether to adopt cloud computing or not is highly important, it is important to identify factors such as requirements of the cloud-customer, type of service model, and deployment model from a technical, economic and organizational viewpoint [4].

2.2 Advantages of the Adoption of Cloud Computing

Xue and Xin listed the following as the benefits of cloud computing in business:

Flexibility - It allows every employee to be more flexible in or out of their workplace. Thus, businessescan now spend time on other businesses in different locations and are not restricted due to the traditional on-premise computing. Since data and files are stored virtually on the Internet, it allows the employees to access the same resources simultaneously. Cost Reduction - organizations only pay for the services that they use, when they access cloud services. Automatic Software/Hardware Upgrades - when an information technology (IT) solution has been implemented in organizations, it creates a problem that is unable to have an appropriate financing due to the high cost of purchasing and maintaining hardware and software. This will give a negative effect[5]. Consequently, these problems can be solved by adopting cloud computing.

Agility - Due to the availability of the Internet, cloud computing is around the clock; this helps organizations to deliver services in the shortest time. Cloud computing increases agility by offering three types of low-level administrations from cloud providers: System Infrastructure – machines and spare parts maintenances, Backup Policy – backup management, Application – software management (upgrade software/application support). Scalability – It allows users to adjust their resources based on the changes of business needs. It helps to solve problems and increase customer satisfaction. Cloud computing is able to make resources quickly available, and allows users to analyse a huge amount of data in just a few minutes due to its processing power [5].

Nasarul highlighted ten major benefits of cloud computing in his research work, he stressed that these benefits are important in the adoption of cloud computing. However, he concluded that despite the attendant benefits of cloud computing, cloud computing services adoption should only be implemented after analyzing all the major security issues. The benefits the research highlighted are: Cost Savings, Time Saving, Scalability and Flexibility, Backup and Recovery, Resource Maximization, Mobile Access, Multi-sharing, Customization, Collaboration, Deliver new services [6].

2.3 Myths of Cloud Computing

Microsoftopined that most companies that choose to move to the cloud do so because they have decided they need it for business agility and want the cost savings that come with it. To help in your migration to the cloud, their study evaluated myths generally believed about cloud computing and presented a myth-busting guide, this would help organizations look at the cloud computing myths so as to separate the facts from fiction[7]. However, Business White Paper believed that Cloud concepts can mean different things to different people, hence a look at the myth of cloud computing concept in order to distinguish facts and fallacies became essential [8].

Myth: Control over technology becomes difficult when the organisation's data is moved to the cloud. Moving to the cloud significantly reduces time spent maintaining hardware and upgrading software. Instead of spending more and more portions of your capital budget on servers for email storage and workloads, you can think strategically and support business managers in a much more agile fashion, quickly responding to their needs [7].

Myth: The public cloud is the most inexpensive way to procure IT services - A characteristic of the public cloud is a relatively inexpensive "pay-as-you-use" model. In the cloud, cost can be leveraged by enterprise using other cloud models, such as shared resources delivered via a private cloud to access resources that are needed constantly. In cases like this, the private cloud actually is more cost-efficient than even the pay-as-you-use public cloud model [8].

2.4 Threats in Cloud Computing

Suryatejain his research defined a threat as a potential cause of an incident that may result in harm to a system or an organization. Vulnerability is a weakness in the asset or system which is exploited by a threat. A threat agent carries out threats by exploiting one or more vulnerabilities. Various threats and vulnerabilities for cloud computing are identified. Security in cloud computing is still evolving, new threats and vulnerabilities are being uncovered. Due to this, the adoption of cloud computing for business processes is slowing down. However, it is opined that classifying threats in cloud computing along with their cloud service delivery model and the possibility of simulating some of the threats with various cloud simulators could be the future [9].

Kacha and Zitouni are of the opinion that data security is a common concern to all technologies that becomes a major challenge when applied to an uncontrolled environment like Cloud Computing. Data outsourced to Cloud infrastructure is more vulnerable than that stored on a traditional infrastructure, mainly for three reasons namely: data is stored on the service provider's infrastructure; data of different users shares the same physical infrastructure; data is accessible via internet [10].

Listed below are several threats in cloud computing as highlighted by several authors listed below:

Data Breaches: A data breach is a security incident in which sensitive, private, or confidential data related to a person or organization has been accessed, copied, or transmitted by an unauthorized party. Targeted attacks, any form of human error, application vulnerabilities, and poor security practices can be can lead to data breaches.

Data Loss: This is simple human errors like when a cloud administrator accidentally deletes files, hard drive failure, power failure, or due to malware infection. The most efficient strategy to data loss is to backup data to multiple locations so that even when data gets corrupted or lost at one location, it can be replaced with a copy available at another location.

Malicious Insiders: An insider threat can be a former employee, system administrator, third-party contractor, or a business partner. A malicious insider which could either be a system administrator or a user, could cause a data breach, because he can access confidential or

restricted information and equally gain orincrease access levels to more critical systems.

Denial of Service: Denial of Service(DoS) attacks are designed to prevent legitimate users of a service from being able to access their data or applications. In a DoS attack, there is only one source machine from which the attack originates and it is susceptible to mitigate. A DDoS (Distributed Denial of Service) attack on the other hand, employs several systems to attack a cloud service.

Vulnerable Systems and APIs: Cloud APIs (Application Programming Interfaces) represent an open door for public to your cloud application. Considerable access to cloud resources can be granted to an attacker by exploiting cloud APIs. For more considerable security, cloud APIs should be accessed via encrypted keys, which are used to authenticate the API user.

However, Malar & Prabhucategorized threats in cloud computing according to cloud computing service model [12], as shown in the table below:

Table 1: Security Issues in Cloud Computing According to Service Model

Service models	**Description**	**Examples**	**Securityissues**
Software as a service (SaaS)	Both the user and end user interfaces impart the software services.	Google docs, Gmail, Yahoo, Salesforce.com etc.	Data privacy, security of network and vicinity, reliability and access of data, verification, Backup, accessibility etc.
Platform as a service (PaaS)	PaaS provides the deployment of apps without buying and managing it. This provides to make and exist the web apps which is required what they needed.	App Engine by Google, SQL Microsoft Azure etc.	The provideris having the full control to build the apps by the user. The security is maintained by the provider. The code of an app is more likely to attacked, if hackers are trying to attack the infrastructure of an app.
Infrastructure as a service (IaaS)	The computer framework is treated like a service and the consumer or tenants does not pay for the resources as an alternative they buy them.	Amazon web services, Windows Azure etc.	The security challenges are created by taking the virtual machines off. Safety measures issues in operating systems are encountered in IaaS.

Source: Malar and Prabhu (2019)

2.5 Solutions to Cloud Threat

Protection from Data Breaches: Various security measures and techniques have been proposed to avoid the data breach in cloud. One of these is to encrypt data before storage on cloud, and in the network. Implementing proper isolation among VMs to prevent information leakage, implement proper access controls to prevent unauthorized access, and to make a risk assessment of the cloud environment to know the storage of sensitive data and its transmission between

various services and networks are some of the measures necessary to avoid data breaches in the cloud [13].

Protection from Data Loss: One of the most important measures is to maintain backup of all data in cloud which can be accessed in case of data loss. However, to maintain the security properties of data such as integrity and confidentiality, data backup must also be protected.

Protection from Malicious Insiders: The protection from these threats can be achieved by limiting the hardware and infrastructure access only to the authorized personnel. To prevent data from malicious insider encryption can also be implemented in storage, and public networks.

Protection from Denial of Service: To avoid DOS attacks it is important to identify and implement all the basic security requirements of cloud network, applications, databases, and other services. The DDOS attacks can be prevented by having extra network bandwidth, using IDS that verify network requests before reaching cloud server, and maintaining a backup of IP pools for urgent cases.

Protection from Insecure Interfaces and APIs: To protect the cloud from insecure API threats it is important for the developers to design these APIs by following the principles of trusted computing. Cloud providers must also ensure that all the all the APIs implemented in cloud are designed securely, and check them before deployment for possible flaws. Strong authentication mechanisms and access controls must also be implemented to secure data and services from insecure interfaces and APIs[14].

III. CONCLUSION

Cloud computing generally poses great data security challenge. However, its benefits are enormous especially in its ubiquity, scalability and elasticity of the technology abilities. These security challenges and threats inherent in this technology raises a concern especially for organizations with extremely sensitive data and makes it expedient to analyse the security strategies emplaced by Cloud Services Providers. A probe to the security state of Cloud Services Providers while using well defined parameters is definite future direction of this paper.

REFERENCES

[1] Frank da Cruz – Herman Hollerith - Columbia University Computing History, Retrieved 18th March 2020.
[2] Markus et al. (2011), Cloud Computing and Computing Evolution. Cloud Computing Technologies, Business Models, Opportunities and Challenges.
[3] Ezgi Ari and Sona Mardikyan (2012), Factors Affecting the Adoption of Cloud Computing.
[4] Radhika Garg and Burkhard Stiller (2015), Factors Affecting Cloud Adoption and Their Interrelations, 5th International Conference on Cloud Computing and Services Science (CLOSER-2015), pages 87-94
[5] Colin Ting Si Xue and Felicia Tiong Wee Xin (2016), Benefits and Challenges of the Adoption of Cloud Computing in Business, International Journal on Cloud Computing: Services and Architecture (IJCCSA) Vol. 6, No. 6.
[6] Nasarul Islam K.V (2017), Review on Benefits and Security Challenges of Cloud Computing, International Journal of Computer Science and Information Technologies, Vol. 8 (2), 224-228.
[7] Microsoft (2018), 10 Myths About Moving to the Cloud
[8] Business White Paper (2011), Five myths of cloud computing, Hewlett-Packard Development Company, L.P.
[9] Suryateja P.S. (2018), Threats and Vulnerabilities of Cloud Computing: A Review, International Journal of Computer Sciences and Engineering, Volume-6, Issue-3, 297-302.
[10] Lynda Kacha and Abdelhafid Zitouni (2018), An Overview on Data Security in Cloud Computing.
[11] Abhinay B. Angadi, Akshata B. Angadi, Karuna C. Gull (2013), Security Issues with Possible Solutions in Cloud Computing-A Survey, International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, Issue 2, pp.652-661.
[12] M B Benjula Anbu Malar and Dr.J.Prabhu (2019), International Journal of Civil Engineering and Technology (IJCIET) Volume 10, Issue 2, February 2019, pp.2138–2153.
[13] Muhammad Kazim and Shao Ying Zhu (2015), A survey on top security threats in cloud computing, (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 6, No. 3, pp.109-113.
[14] Luigi Coppolino, Salvatore D'Antonio, Giovanni Mazzeo, Luigi Romano (2016), Cloud Security: Emerging Threats and Current Solutions, Computers & Electrical Engineering.