Texila International Journal of Academic Research
Special Edition Apr 2019

Cloud Computing Environment Security Issues

Article by Khanyisile Patience Dlamini- Shabangu
Nursing, Texila American University
E-mail: patiencedlam@gmail.com kshabangu@texilaconnect.com

Abstract

Cloud Computing is a technology that provides on-demand computing services such as applications, storage, and processing to consumers over the internet (cloud). It is centered on the pay-per-use model meaning that a user has to pay only for the services utilized. This technology is based on the virtualization perception. Such services allow the companies/establishments to scale-up or scale-down their in-house grounds. Cloud computing has numerous advantages such as flexibility, efficiency, scalability, integration, and capital reduction (upfront fixed cost), and shared resources. Moreover, it offers an advanced virtual space for companies to deploy their applications or run their operations. However, companies which consider embracing cloud based services must also appreciate that regardless of its benefits, the transition to this computing paradigm raises security concerns which are subject of several researchers. The goal of this article is to identify the main security issues and to draw the attention of both decision makers and users to the potential risks of moving data into "the cloud".

Keywords*: cloud computing, cloud service, data security, infrastructure data confidentiality.*

Introduction

The term "cloud" is used as an icon of the Internet and other communications systems as well as an idea of the underlying infrastructures involved. Cloud computing usually refers as the result of a progression of the widespread acceptance of virtualization, service-oriented architecture, autonomic, and utility computing. The specifics of site of infrastructure or component devices are not known to most of the end-users, user do not require to comprehensively appreciate or control the technology infrastructure that supports their computing activities and the users do not necessarily have their own resources.[17].

Cloud Computing is Innovative Information System architecture. It is a driving force challenging its observers to rethink their understanding on operating systems, client-server architecture and browsers. Cloud Computing is an enticing technology which is a combination of many existing technologies such as parallel computing, grid computing, distributed computing, etc. It offers services like data storage, power supply, low cost to its consumers over the internet at anytime from anywhere. The pricing model is centered on pay as you go method. Millions of individuals and companies are depending on cloud for their data.

Although cloud computing is realizing increased popularity, concerns are being voiced about the security issues introduced through the adoption of this model. Data security issue is the major challenge which is hindering the progression of cloud computing. It needs to be resolved in order to make it widely acceptable and to accelerate its growth.

National Institute of Standards and Technology (NIST) describe cloud computing as a model for allowing ubiquitous, convenient, on demand network access to shared pool of resources (e.g. networks, servers, storage, applications and services) that can be promptly provisioned and released with insignificant management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models and four deployment models [5].

DOI: 10.21522/TIJAR.2014.SE.19.01.Art009
ISSN: 2520-3088

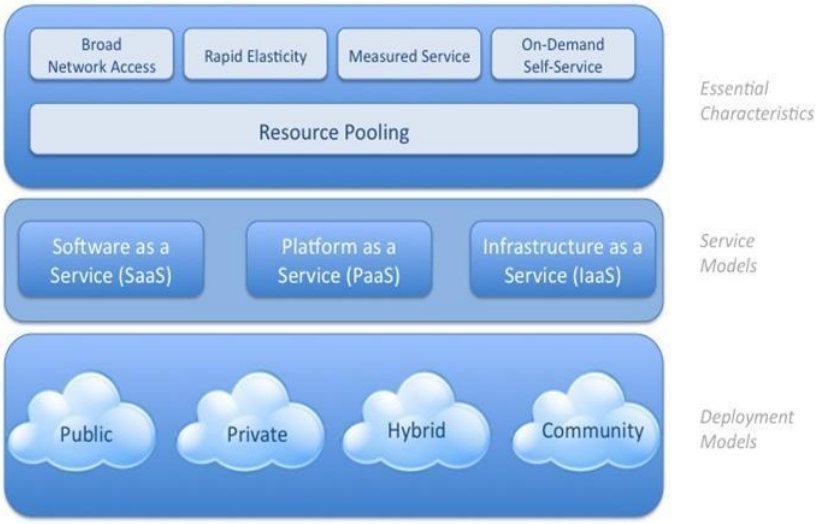

Figure 1. NIST- Visual model of cloud computing

In cloud computing the available service models are: [5, 8]

A. ***Infrastructure as a Service (IaaS):*** Focuses on hardware and IT infrastructure management. The facility provided to the client is to lease processing, storage and other computing resources. The client does not manage or control the basic cloud infrastructure but has control over the operating systems, storage, deployed applications and possibly limited control of select network components.

B. ***Platform as a Service (PaaS):*** Concentrates on middleware and design tools as a service. Clients obtain access to the platforms by enabling them to organize their own software and applications in the cloud.

C. ***Software as a Service (SaaS):*** Clients obtain the facility to access and use the application or service that is hosted in the cloud. The applications are designed for end users and it is delivered over the web. Deals with traditional software applications such as customer relationship management or social networking as a service, and business process as a service (business cloud) offers value added services.

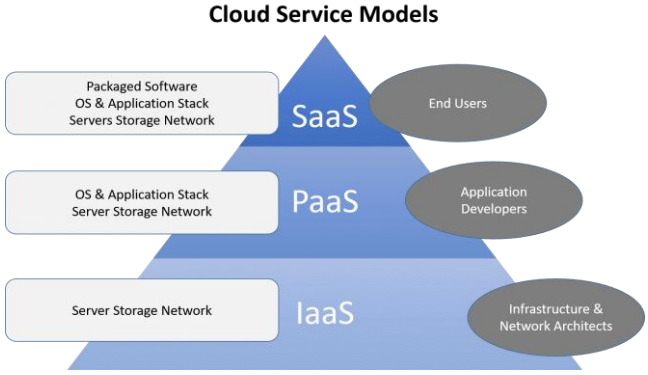

Figure 2. Cloud service model [3]

The four deployment models for cloud architecture solutions are: [2,4]

A. ***Private Cloud:*** Clients have complete control over how data is managed and what security measures are in place while data processing in cloud. Clients are considered to be trusted (employees, contractors, and business partners).

B. ***Community Cloud***: The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g. security requirements, compliance consideration, policy, etc.). It may be managed by the organizations or third party, may exist on premise or off premise.

C. ***Public Cloud:*** Services and infrastructure are provided to different clients. The clients access the application (web) or services over the internet. The clients do not know how the cloud is managed or what infrastructure is available. The clients of this service are considered to be untrusted.
D. ***Hybrid Cloud:*** It is a combination of two or more clouds (private, community, or public) that remains unique entities, but are bound together by standardized or proprietary technology that enables data and applications portability (e.g. cloud bursting for load balancing between clouds).

The essential qualities of cloud computing are: [5, 18]

A. ***Shared Infrastructure:*** Cloud environment uses an effective software model that allows sharing of physical services, storage and networking capabilities among users.
B. ***Network Access:*** Cloud services are accessed over a network from a wide range of devices such as PCs, laptops, and mobile devices by using standards based APIs.
C. ***Scalability of Infrastructure:*** New nodes can be added or dropped from the network as can physical servers, with limited modifications of infrastructure set up and software. Cloud architecture can scale horizontally, or vertically, according to demand.
D. ***Reliability:*** Improves through the use of multiple redundant sites, which makes cloud computing suitable for business continuity and disaster recovery.
E. ***Location Independence****:* There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources, but may be able to specify location at a higher level of abstraction.

Some of the Cloud Domains that should be addressed by service contracts are: [5]

A. Architecture Framework
B. Governance, Enterprise Risk Management
C. Legal, e-Discovery
D. Compliance & Audit
E. Security, Business Continuity, Disaster Recovery
F. Incident Response Issues

A number of standard bodies are creating standards for cloud environment. Clients have a liberty to move between cloud providers. This may be due to different reasons. E.g. other service providers offer better prices; relationship with a vendor may not be working, etc. The community of cloud computing has already developed numerous standards by several forums. These standards are developed to offer interoperability between clouds and to develop an excellent environment in cloud computing industry [2, 18]. Some cloud security standard organizations are:

A. National Institute of Standards and Technology (NIST)
B. Open Cloud Consortium (OCC)
C. Open Grid Forum (OGF)
D. Cloud Security Alliance (CSA)
E. Cloud Computing Interoperability Forum (CCIF)

Methods

A number of researches have been performed in the literature for cloud computing and its security issues. Here I present the review of some of the researches.

A. Data Integrity, Data Location, Data Confidentiality, Data Leakage, Investigation, Data Availability, Third Party Control, Privacy & Legal Issues and Backup are the key issues related to data security in cloud computing identified by the researchers [16, 1, 7, 11, 12, 17, 4, 15]. Data Availability, the unavailability of data may lead to outages which may have cost implications to the company. For Data location, cloud clients usually wish their data may reside in their specific country based on the policies, standards and legislation of the country. They usually feel cross border storage may pose risk in terms of data confidentiality, data leakage and privacy and legal issues and the regulatory legislation framework of another country. Therefore, with this the data security becomes the main concern.
B. In the recent years, cloud computing has developed from being a promising business concept to one of the fast-growing sectors of the IT industry. Security is the key issue, as it has lot of loose

DOI: 10.21522/TIJAR.2014.SE.19.01.Art009
ISSN: 2520-3088

ends which worries a number of cloud users and prospective users. Cloud service users require being attentive in comprehending the risks of data breaches in this new environment.

C. Open Foundation have revealed that more than 2000 cloud related data breach incidents globally have been reported since 2012, which still calls for security concern.

D. The International Journal of Computer Science & Networks revealed/publicized some well-known outages of leading cloud providers, unavailability lead to service outages. Availability is one of the most critical information security requirements in Cloud computing because it is a key decision factor when deciding among private, public or hybrid cloud vendors as well as in the delivery models.

Results

A. According to study [6] security has always been the key issue for Information Technology Executives when it comes to cloud acceptance. They state that in two surveys conducted by International Data Corporation (IDC) in 2008 and 2009 respectively, security came top on the list. Refer to fig.3/4

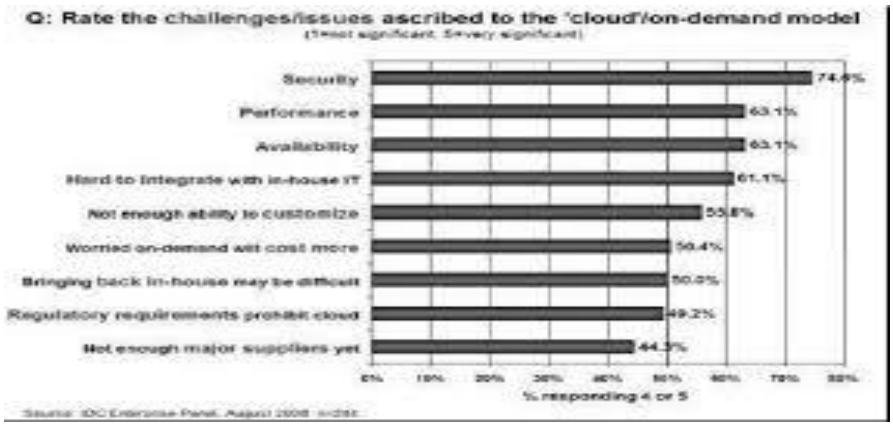

Figure 3. Source: IDC Enterprise portal, 2008

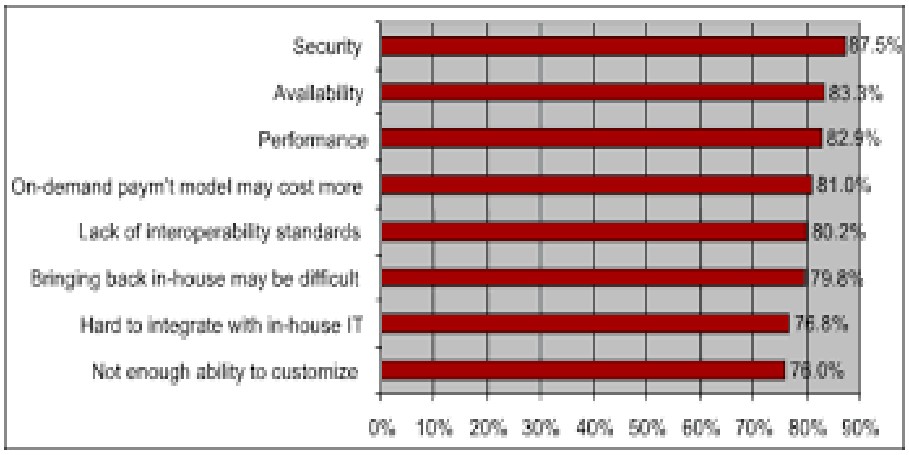

Figure 4. Source: IDC Enterprise portal, 2009

B. In another survey conducted by IDC [3] shows the importance of the challenges for those considering cloud computing as an option. It is shown in Figure 5 that security is the utmost concern. It is no surprise that data security tops the list of concerns that hold institutions back from cloud acceptance. 73% of survey respondents indicated this is a big red flag for them. Cloud service providers are targets data breaches.

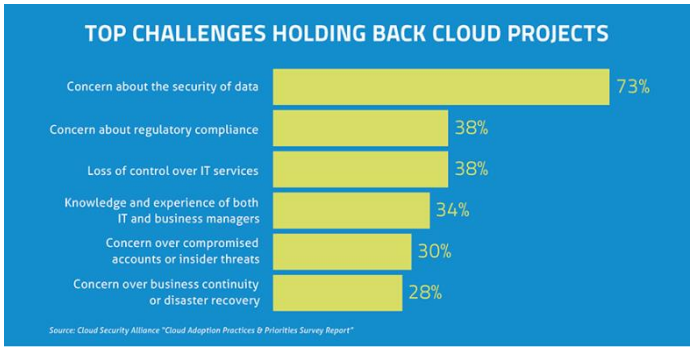

Figure 5. – International Data Corporation (IDC)

C. The 2017 Annual Cybersecurity Report revealed the possible financial bearing of attacks on enterprises, from small medium enterprise (SMEs) to large companies/enterprises. More than 50% of companies encountered public scrutiny after a security breach. Operations and finance systems were the most affected, followed by brand status and client retention. For companies that experienced an attack, the consequence was significant: [2]

i. 22% of breached companies lost their clients, with 40% of them lost more than 20% of their client base.
ii. 29% lost income, with 38% of that group losing more than 20% of income/revenue.
iii. 23% of breached companies lost business chances/opportunities, with 42% of them losing more than 20%.

D. There have been many instances where the Data Centers of the Cloud Service Providers have slowed down or have stopped working altogether. In June 2012, a big storm in North Virginia affected the Amazon's Data Center. The effect was that, websites like Netflix, Instagram, Pinterest, and Heroku were down for few hours because they dependent on Amazon's cloud service [13].

E. In another instance, a flawed storage software update over Google prompted an unpredicted bug in March 2011. Around 150,000 Gmail accounts were affected and all their messages were erased in the wake of that software bug. [13].

F. In April 2012 there was a Gmail interruption that made Gmail services inaccessible for almost 1 hour. The company initially reported that it affected less than 2 % of their clients, then they updated to 10 %, which added to around 35 million clients of a total of 350 million users. These occurrences are not unusual and indicate the client lack of control over their information. [10].

G. According to a study by Open Security Foundation, there were more than 2000 cloud related data breach incidents globally since 2012. Studies done on some randomly selected enterprises show that 82% of those enterprises saved money moving to cloud while only 14% downsized their IT after cloud adoption. [13].

Discussion

Cloud computing provides efficient, flexible and cost-effective services. However, this model is not 100% safe. The major concerns in cloud computing are privacy and security. There are various security issues in cloud computing. Of many security issues, data security seems to be the major obstacle towards the adaption of cloud computing. Data security in cloud is must, in order to ensure that the data has not been accessed by any unauthorized person.

According to a number of researchers [16, 1, 7, 11, 12, 17, 4, 15], the different key data security issues of cloud computing are discussed as follows.

A. **Data Integrity**: It is one of the most critical issues in cloud security. Data integrity describes the wholeness or completeness of data. It can easily be achieved in standalone system by using atomicity, consistency, isolation, durability (ACID) properties. But it is not easy to achieve data integrity in cloud environment because transaction management is the biggest problem with web services. [1].

DOI: 10.21522/TIJAR.2014.SE.19.01.Art009
ISSN: 2520-3088

B. **Data Location:** Clients keep their data on cloud without any clue about the location of their stored data, therefore requiring the service provider commitment to comply with privacy restrictions. Data locality is of utmost significance because some companies do not want data stored outside the country borders. Cloud model should ensure security and reliability of the location of the data. Location of data stored in cloud can be prioritized according to client's users wish or requirement. [7].

C. **Data Confidentiality**: In Cloud computing, confidentiality plays a key part especially in maintaining control over enterprise's data located across multiple distributed databases. It is essential when employing a Public cloud due to public clouds accessibility nature. Unauthorized access to critical data of an enterprise can cause disaster. Therefore, it is cloud providers duty to ensure that data can be accessed only by a legitimate user. Data confidentiality is achieved by encryption. Cloud provider should implement suitable authentication and accounting mechanism to achieve confidentiality and should guarantee the client that their data is safe and confidential. [11].

D. **Data Leakage:** Although adoption of cloud computing is providing paramount advantages to an entity, but because of data leakage fear, they are holding back. Data leakage has become one of the main worries from security perspective. Cloud is an outside party where customer's data is hosted, and it has potential to access customer's data. Cloud environment provides resource sharing, so it seems to be risky to move data in hands of cloud provider. Data in cloud stored in a shared environment, so it could be hacked easily either due to malicious hacker attack or accidentally. To alleviate the effects of this problem a sensible data encryption technique should be implemented. Encryption should be done at client side and he should have control over the keys used for encryption. Furthermore, encryption should not be performed at any intermediary place before transmission to cloud. [12]

E. **Investigation**: Breach or intrusion attempts are difficult to be trailed and spotted over the cloud due to the dispersion of the data and resources. While in some cases it could be impossible because of the high complexity level. [14]

F. **Data availability:** Another significant concern of mission and safety company in the cloud computing is availability of services. Data availability is a term used by some computer storage manufacturers and storage service providers (SSPs) to describe products and services that ensure that data continues to be available at a necessary level of performance in situations ranging from normal through" disastrous." In general, data availability is realized through redundancy involving where the data is stored and how it can be reached [13]. The unavailability of data may lead to service outages. Table 1 shows some well-known outages of leading cloud providers. [16].

Table 1. Cloud service outage

Cloud Service	**Outage Duration (Hours)**	**Dates**
Amazon S3	7	**20/07/2008**
Google Gmail App	24	11/08/2008
Google Gmail	30	17/10/2008
FlexiScale	18	31/10/2008
SalesForce.com	0.667	6/01/2009
Windows Azure	22	13-14/03/2009

G. Third-Party Control: As, the value of company data is escalating the third party access can lead to a possible loss of trade secrets and intellectual property. There is also the issue of a malicious insider who misuses access rights to clients information. The fear of corporate espionage and data warfare also stems from third party control. Provider compliance with regulations such as those on auditing also raise questions on how that can be affected on site in a globally distributed multitenant environment [16].

H. Privacy and Legal Issues: Data in the cloud is usually globally distributed which raises concerns about jurisdiction, data exposure and privacy. The researchers [4] summarized the key privacy issues of cloud computing. Users are made to contribute their personal information without knowing where it is kept or what future drive it might work for. Businesses stand a risk of not conforming to government policies as would be explained further while the cloud vendors who uncover critical information risk legal obligation. Virtual co-tenancy of sensitive and no sensitive data on the same host also carries its own potential risks.

I. Backup: Cloud provider should guarantee that all of its consumer's data is backed up across multiple servers in multiple copies often to provide recovery in case of disaster like hardware failure. And to avoid accidental leakage of backed up data, a strong encryption scheme should be used. High Security Distribution and Rake Technology (HS-DRT), Parity Cloud Service Technique (PCS), and Cold and Hot Backup Service Replacement Strategy (CBSRS) are some backup and recovery techniques that have been developed in cloud domain [15].

Conclusion

In this paper I explained cloud computing and the its key security issues. By utilizing various facilities and services provided by cloud one can upsurge performance, agility and efficiency in addition to reduce cost and management responsibilities of an enterprise. Though there are a number of benefits of cloud, there are yet numerous challenges to be faced by cloud computing such as privacy issues and data security. In this paper we have tried to address most critical data security challenges of cloud. Also, it should be eminent that different standard organizations such as National Institute of Standards and Technology (NIST), Cloud Security Alliance (CSA), Cloud Computing Interoperability Forum (CCIF), etc. are trying to establish standards to correct numerous security issues of cloud. Cloud computing has the potential to provide a secure and economically viable IT solution in the future.

Reference

[1]. Cachin, C., Keidar, I., & Shraer,A. (2009). Trusting the Cloud. *Amc Sigact New,* Vol.40, No. 2, pp. 81-86.

[2]. Cisco 2017 Annual Cybersecurity Report: Chief Security officers Reveal True Cost of Breaches and the Actions Organizations are Taking. *Cisco, the Network. Cisco Technology News site*. Retrieved December 17, 2018 from https://newsroom.cisco.com/press-release-content?articleId=1818259.

[3]. F. Gens, "New IDC It Cloud Services Survey: Top Benefits and Challenges," 2009. http://blogs.idc.com/ie/?p=730.

[4]. Chow, R., Golle, P., Jakobsson, M., Shi, E., Staddon, J., Masuoka, R., & Molina, J. (2009). Controlling Data in Cloud: Outsourcing Computation without Outsourcing Control. *ACM Workshop on Cloud Computing Security*.

[5]. Hogan, M., Liu, F., Sokol, A., & Tong, J. (2011, July). NIST Cloud Computing Standards Roadmap. *National Institute of Standards & Technology*. Retrieved December 18, 2018 from https://www.nist.gov/sites/default/files/documents/itl/cloud/NIST_SP-500-291_Jul5A.pdf .

[6]. Hurwitz, J., Bloor, R., Kaufman, M., & Halper, F. (). Cloud Computing Standards Organizations Dummies. Retrieved December 18, 2018 from https://www.dummies.com/programming/networking/cloud-computing-standards-organizations/.

[7]. Kumarand, P., & Arri, H.S. (2013). Data Location in Cloud Computing. *International Journal for Science & Emerging Technologies with Latest Trends.* Vol. 5, No. 1, pp. 24-27.

[8]. Malik, A., & Nazir, M.M. (2012, March). Security Framework for Cloud Computing Environment: A Review. *Journal of Emerging Trends in Computing and Information Sciences.*

[9]. Neela, K.L., Kavitha, V., & Ramesh, R.K. (2013, August). Cloud Computing: Threats and Security Issues. *International Journal of Engineering Sciences & Research Technology*.

[10]. Ogigau-Neamtiu, F. (2012). Cloud Computing Security Issues. *Journal of Defense Resources Management,* Vol.3, Issue 2(5).

[11]. Ramgovind, S., Eloff, M.M., & Smith, E. (2010). The Management of Security in Cloud Computing. *Institute of Electrical and Electronics Engineers.*

DOI: 10.21522/TIJAR.2014.SE.19.01.Art009
ISSN: 2520-3088

[12]. Rawat, N., Srivastava, R., & Pandey, B.K. (2014, August 1). Data Security Issues in Cloud Computing. *Open Journal of Mobile Computing and Cloud Computing.*
[13]. Srivastava, H., & Kumar, S.A. (2015, January). Control Framework for Secure Cloud Computing. *Journal of Information Security.* 6,12-23.
[14]. Srivastava, H., & Kumar, S.A. (2015, January). Control Framework for Secure Cloud Computing. *Journal of Information Security.* 6,12-23.
[15]. Sharma, K., & Singh, K.R. (2012). Online Data Backup and Disaster Recovery Techniques in Cloud Computing: A Review. *International Journal of Engineering and Innovative Technology (IJEIT).* Vol. 2, No. 5, pp. 249 -254.
[16]. Ventrapragada, V.S., Ravuri, D., & Jyothi, G. (2013). A study on Cloud Computing and its Security Issues. *International Journal of Computer Science and Network.* Vol 2, Issue 1, 2013
[17]. Waseem, M., Lakhan, A., & Jamali, I.A. (2016, April 26). Data Security of Mobile Cloud Computing on Cloud Server. *Open Access Library Journal*, 3: e2377. Retrieved December 17, 2018 from http://dx.doi.org/10.4236/oalib.1102377.
[18]. Zissis, A., Lekkas, D. (2010, December 13). Addressing Cloud Computing Security Issues. *Future Generation Computer Systems.*