Journal of Advances and Scholarly Researches in Allied Education
Vol. 16, Issue No. 6, May-2019, ISSN 2230-7540

Data Protection of Big Data in Cloud Environment and Its Security Measures for Super Marketing

Dibakar Panigrahi*

Research Scholar, Pacific University, Udaipur

Abstract – Cloud computing is an internet based computing platform which is shared information, hardware and software resources, is provided to computers and devices on-demand, like the power grid. It is a great idea to make many standard computers together to get a super computer where it can do a lot of things powerfully. It aims to construct a perfect system with powerful computing capability through a large number of relatively low-cost computing unit, and using the innovative business models like SaaS, PaaS, and IaaS to distribute the powerful computing capacity to end user's hands. This paper provides a snapshot of cloud computing background, classifications, service model, existing security issues and typical security measures.

Keywords – Cloud Computing, Classifications, Services, Security issues and Typical Security Measures

----------X----------

INTRODUCTION

Cloud computing continues to be boasted as a major breakthrough in IT management. Cloud computing is a model for enabling appropriate, on request network access to a shared group of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction. The direct definition is not available, but it can be expressed in general as the following statement:" Cloud computing is a kind of computing environment, where corporate owners get the service for their computing needs including application software services to a third party and when they need to use the computation or personnel need to use the application resources like database, emails etc., they access the resource via internet [1].

A small business needs a few small servers for database, emails, applications etc. The servers need higher power of computing. Also the pcs or laptop needs lower power of computing are much cheaper than servers. Most of the customers decide to avoid need of purchasing servers and thus cut-off the need of keeping an operation and maintenance team. Cloud computing is the next natural step in the evolution of on-demand ICT services and products. Cloud computing refers to a wide field which includes applications ready to use, web-based client services, and a scattered, platform-independent server design. The user can pay the money on monthly basis and use the IT infrastructure of a third party IT managed service data center.

Cloud is a virtualized pool of computing resources. It can manage a variety of dissimilar loads, including the group of back end operations and user oriented shared applications. The main advantage of using Cloud computing facility is that customers do not have to pay for infrastructure installation and maintenance charge. As a user of cloud computing you have to pay the service charges according to your usage of computing power and other networking resources. Moreover, users are free from care about software updating, installations, maintaining of server for email , anti-virus updating , follow up the backups, caring of web servers and both physical and logical security of your data.

Figure 1 - The Cloud

CLASSIFICATIONS OF CLOUD

Cloud computing is usually classified in two based on the behavior:

Based on the Location

Services offered by the cloud

Classification based on the Location

Cloud computing is usually classified as follows based on the location where it is available [9]:

Public cloud

Public cloud is the computing infrastructure hosted by the cloud vendor at the vendor premises. The customer has no visibility and mechanism over where the computing infrastructure is hosted. The computing infrastructure is common between any organizations.

Private cloud

Private cloud is the computing infrastructure dedicated to a particular organization and not shared with other organization. Some experts consider that private clouds are not real examples of cloud computing. Private clouds are more costly and more secure than public clouds. Again the private clouds are classified into two as follows:

On-premise private clouds

On-premise private clouds are constructed and maintained by the organization itself. They feel this type of cloud is more secure and economical than the other.

Externally hosted private clouds

Externally hosted private clouds are also exclusively used by one organization, but are hosted by the professional from a CSP. Externally hosted private clouds are economical than On-premise private clouds.

Hybrid cloud

The usage of both private and public clouds together is called hybrid cloud. Organizations may host risky applications on private clouds and applications with relatively less security concerns on the public cloud. Cloud bursting is the processes of organization use their own computing infrastructure for normal usage, but accessing the cloud using services for high/peak load requirements. This ensures that an unexpected increase in computing requirement is controlled smartly.

Community cloud

Community cloud is sharing of computing infrastructure in between organizations of the same community.

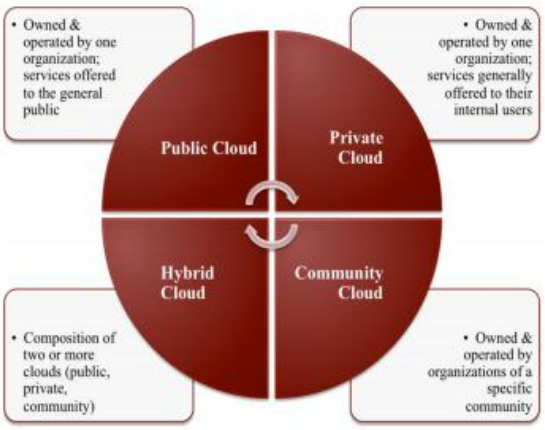

Figure 2 - Cloud Types

Classification based on Service Provided

Cloud services are generally divided in the three main types, Software-as-a-Service (SaaS), Platformas-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS).

Software as a Service (SaaS)

Software as a service (SaaS) includes a complete software offering on the cloud. Clients can access a software application hosted by the cloud vendor on the basis of their usage. The applications normally exist to the clients via the Internet and are managed completely by the Cloud provider. That means that the management of these services such as updating and patching are in the provider's concern. One big advantage of SaaS is that all clients are running the same software version and new functionality can be easily integrated by the provider and is therefore available to all clients. Good example for SaaS offered CSP is Salesforce.com, they offering in the online Customer Relationship Management (CRM) space. Other examples are Google, Gmail, Google docs, Microsoft's hotmail, and Microsoft's other online services.

Platform-as-a-Service (PaaS)

Platform as a Service (PaaS) involves offering a development platform on the cloud. This type of service used by the developer community and was likely started with the introduction and popularity of Linux open source code. This cloud computing model offers a platform for developers to coding, testing and experimenting new software without the complexity of setting up the kinds of server for maintenance, development and production. Platforms delivered by different vendors are usually not compatible. Typical players in PaaS are Google's Application Engine, Microsoft's Azure, and Salesforce.com.

Infrastructure-as-a-Service (IaaS)

This is hardware related services using the principles of cloud computing. It delivers hardware resources such as CPU, disk space or network components as a service. These resources are usually delivered as a virtualization platform by the Cloud provider and can be accessed across the Internet by the client. Primary vendors that provide IaaS are Amazon EC2, Amazon S3, Rackspace Cloud Servers and Flexiscale.

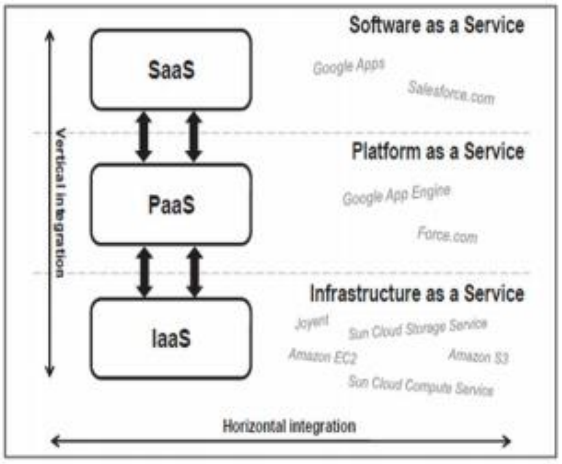

Figure 3 - Cloud Services

NECESSITIES OF CLOUD SECURITY

There is a number of security issues/concerns associated with cloud computing but these issues fall into two broad categories: Security issues faced by cloud providers (organizations providing software-, platform-, or infrastructure-as-a-service via the cloud) and security issues faced by their customers. In most cases, the provider must confirm that their infrastructure is secure and that their client's data and applications are protected while the customer must ensure that the provider has taken the proper security measures to protect their information.

Data Protection

Cloud providers have systems in place to prevent data leaks or access by third parties. Suitable split-up of duties should confirm that auditing and /or monitoring cannot be defeated, even by priority users at the cloud provider. Identity management every enterprise will have its own identity management system to control access to information and computing resources. Cloud providers either integrated the customer's identity management system into their own infrastructure, using alliance or SSO technology, or provide a uniqueness management solution of their own.

Physical and Personnel Security

Providers ensure that physical machines are satisfactorily secure and thus access to these machines as well as relevant customer data is not only restricted but that access is documented.

Availability

Cloud providers assure that they will have regular and predictable access to their data and applications.

Application Data

Cloud providers ensure that applications available as a service via the cloud are secure by applying, testing and approval procedures for outsourced or packaged application code. It also wants an application security measures are in place in the production.

Privacy

Privacy ensures that all critical data are concealed and that only authorized users have access to data in its whole. Moreover, digital personalities and passports must be protected as should any data that the provider collects or produces about customer activity in the cloud.

TYPICAL BIG DATA CLOUD SECURITY MEASURES

Cloud computing is causing a seismic change in the business models of companies as well as in the everyday computing habits of the general public. Cloud computing reduces expenses, saves storage space, provides remote access, affords extendable, and improves efficiency. Cloud security is the growing day by day for make sure the security of the resources available in the cloud.

Since that time, significant steps have been made. Cloud service providers (CSPs) have become increasingly active in implementing aggressive measures to address the issues raised by the Gartner report as well as other related security concerns. The following are some of the creativities that CSPs have undertaken to enhance cloud security.

IDS - Intrusion Detection Systems

Several kinds of IDS systems have been implemented and used successfully on high-volume networks to monitor and record activities in order to detect possible intrusions, hateful activities, or policy destructions. Some of these systems also take actions to stifle intrusion attempts but just about all of them are effective in identifying and reporting potential incidents.

In a cloud paradigm, the stakes are higher and so are the challenges.

Interference attempts are potentially more impactful and the complexity of the cloud can stretch the

limitations of a traditional IDS. Deployment of IDS sensors on separate cloud layers managed by a multi-threaded queue and couched within a coordinated communication mechanism over a single platform can significantly mitigate the complexities inherent within the cloud environment.

SIEM - Security Information and Event Management Systems

Traditional SIEM systems address key security essentials at various levels: observing, warning, report generation, trend study, and security compliance. SIEM systems do is to continuously collect system data and generate reports, which are then correlated and analysed. They also react automatically to resolve security incidents. The big breakthrough in recent years has been the ability to deploy SIEMs in cloud environments. This will be done by technological advances in speed and volume. This will create the new service in cloud environment, many CSPs are now able to offer log report generation and management as common services within the cloud.

ISO/IEC 27001 Certification

ISO/IEC 27001 certification which is specifies standards that a management system needs to meet in order to ensure that a measurable and sufficient level of security and risk management of records is in place. The ISO/IEC 27001 is an information security management system (ISMS) standard published in October 2005 by the International Organization for Standardization (ISO) and the International Electro technical Commission (IEC). While not cloud specific, this standard has been adopted as a cloud industry staple and a benchmark of security agreement by CSPs. In order to become certified, vendors are required to satisfy a three-stage audit process undertaken by independent auditors and checked on a regular basis thereafter.

Registration with CSA STAR

In 2011, the Cloud Security Alliance (CSA) launched a new initiative to encourage transparency of security practices within cloud providers. STAR (Security, Trust, & Assurance registry) is a free and publicly accessible registry that documents the specific security controls provided by various CSPs. The office is always open to get the self-assessment report from the cloud providers. STAR is easily reachable and searchable, making it a great source for cloud customers to review the security observes of different providers. In many ways, it is a major rise forward in industry clearness and in the inspiration of CSPs to exercise extreme carefulness and thoroughness in their cloud security measures.

The Cloud Control Matrix

The Cloud Control Matrix (CCM) is a baseline set of security controls created by the CSA. Organized by categories, the matrix is comprised of a large list of security controls mapped to a variety of well recognized industry security standards. The CCM is another appreciated tool and it will assist prospective cloud customers in assessing the security risk associated with a cloud computing provider. The commonly-held belief that a site-specific infrastructure is inherently more secure than an infrastructure managed by a service provider in the cloud can now be safely classified as a error. Although cloud security has continuously posed great encounters, these encounters are being met and the security beast is slowly being tamed.

There is no question that security continues to be among the top concerns that potential customers have about cloud computing, and rightly so. The huge steps made in this area in recent years are real and determinate. And it will increasingly clear that security threats in the cloud environment are today not that much bigger, and in many cases less prevalent, than those handled by on-site systems.

CONCLUSION

This paper discusses about cloud computing technology, describes its definition, its types, its service models, existing security issues and typical measures of cloud security. There is no doubt that the cloud computing is the development trend in the prospect. Cloud computing carries us the about endless computing proficiency, good scalability, ondemand service, payment based on usage and so on, also challenge at security privacy, legal issues and so on. Cloud computing offers many benefits, but it is vulnerable to threats. There should be a oath of belief and confidentiality between the service provider and the client. Security must be viewed as a endless process to meet the changing needs of a highly unstable computing atmosphere. Holistic approach being needed for cloud computing safety procedures, which can be used in common, in any service model, at any phase till the client is using the service. The client should be aware of their own security. To help mitigate the threat, cloud computing participants should capitalize heavily in risk assessment to ensure that the system encrypts to protect data; establishes trusted foundation to secure the platform and infrastructure; and builds higher assurance into auditing to strengthen compliance.

REFERENCES

[1] K. Valli Madhavi, et. al. (2012). Cloud Computing : Security Measures Threats and Counter International Journal of

Research in Computer and Communication technology, IJRCCT, ISSN 2278- 5841, Vol. 1, Issue 4.

[2] Jennifer Marsh software programmer with Rackspace Hosting,, Effective Measures to Deal with Cloud Security, Sep 14, 2012.

[3] Mohamed Ashik M. and Sankara Narayanan A. (2012). An Overview of Cloud Computing and its Security Issues.

[4] Jianfeng Yang IEEE 3rd international conference on cloud computing, “cloud computing research and security issues”, 2010.

[5] Philip Wik (2011). Service Technology Magazine. 2011-10. www.servicetechmag.com/I55/1011-1. Retrieved “Thunderclouds: Managing SOA-Cloud Risk", 2011-21-21.

[6] B. Grobauer, T. Walloschek and E. Stöcker (2010). IEEE Security and Privacy, vol. 99, "Understanding Cloud Computing Vulnerabilities”.

[7] Chris Harding (2010). Service Oriented Architecture and the Cloud.

[8] Ko, Ryan K. L. Ko; Kirchberg, Markus; Lee, Bu Sung (2011). “From System-Centric Logging to Data-Centric Logging - accountability, Trust and Security in Cloud Computing". Proceedings of the 1st Defence, Science and Research Conference 2011 - Symposium on Cyber Terrorism, IEEE Computer Society, 3–4 August 2011,Singapore. http://www.hpl.hp.com/people/ryan_ko/RKo-DSR2011- Data_Centric_Logging.pdf.

Corresponding Author

Dibakar Panigrahi*

Research Scholar, Pacific University, Udaipur