International Journal of Science, Environment and Technology, Vol. 4, No 1, 2015, 264 – 272
ISSN 2278-3687 (O)

CLOUD COMPUTING CONCEPTS, DEPLOYMENT, DATA SECURITY ANALYSIS & FUTURE

Sandeep Dhawan
Director of Technology, OTTE New York, USA
E-mail: sandeepdo@gmail.com

Abstract: with a brief conceptual examination on Cloud Computing, this paper includes the deployment models, data security analysis and future of this emerging technology. Since, with the ease of access, security implication on public clouds is a great challenge considering the types of cloud computing and the services delivery.
Index Terms: Cloud Computing, Data Security, Privacy laws, IaaS, PaaS, SaaS, Encryption.

1 INTRODUCTION

Cloud computing is an appealing subject since its beginning. People, corporate group & public sectors are heading towards decreasing their operational & money related expenses of data centers support and usage of their IT assets in vital planning of activities & execution, to fasten application running for accessibility to front end client and IT assets conformity to eccentric and vacillation in stipulation of business. [1], [2], [3]. In this discernible actuality the data of the real and physical frameworks where the software is running remains completely nonfigurative & abstractive from the front end client.

The general cases of the cloud computing today are SkyDrive & Drop Box, which are in extreme utilization to distribute data by the people and associations for delicate & confidential information distribution, however real deficiency without breaking a sweat of access is absence of security and access controls when clients share their private information through open or public clouds. Since the complex virtual machines can get to the data which is unreliably streaming, there's need of an impeccable security assembled marvel that can dispense with risk of misdirecting, misusing, information seizing and deceiving the private data.

In this paper we have performed thorough investigation of information security, architectures and administrations model examination of distinctive cloud sending models. To achieve economies of scale & soundness, cloud computing primarily depends on offering of the assets

*Received Jan 21, 2015 * Published Feb 2, 2015 * www.ijset.net*

precisely like a system utility, and have the real five qualities, for example, (1) On interest organization toward oneself (2) Broad system get to (3) Resource Pooling (4) Rapid Elasticity (5) Measured Service [4]. Other fundamental attributes of the Cloud are its extraordinary spryness and agility, application programming interface, cost diminishment, empowers the gadget & area autonomy, simplicity of support, empowers multitenancy, expands the execution through profit by enhancing adaptability and dependability [5],[6],[7],[8],[9].

2. CLOUD SECURITY, ARCHITECTURE & SERVICE DELIVERY ANALYSIS

2.1 Security

Since cloud concentrates on centralization of information it can enhance the security by expanding the security resources usage however there is a consistent danger of loss of controls for classified data and confidential information as well as security needs for stored kernels [10].

2.2 Services Models & Architecture

Fundamental models of the service adopted by cloud computing service providers are: Unified Communications as a Service (UCaaS), Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (Iaas).

Fundamental segments of the cloud construction modeling are backend stages and front end stages. Back end stages are contained the servers and information stockpiling while front end stage typically involved thin client, fat client, zero client and portable peripherals. Subcomponent includes the presence of intranet, web and intra cloud, so the cloud information stockpiling and collaboration gets to be conceivable through virtual interactive sessions and applications, for example, web programs and web browsers. Thus, cloud structural engineering gives the cloud answer for diverse frameworks managing distinctive segments, for example, middleware and programming and software component, administration and services, cloud resources, and geo-locations.

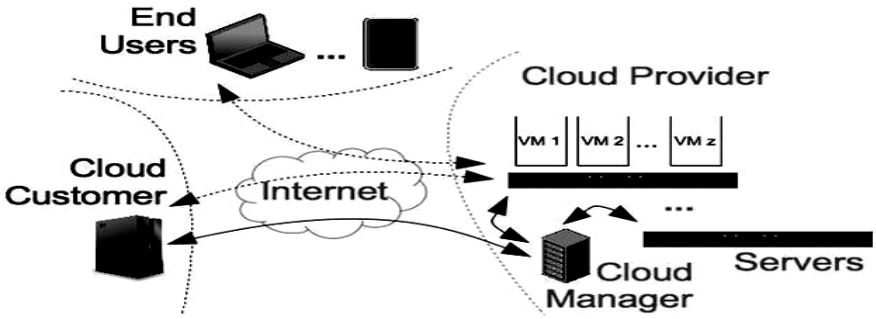

Fig.1. shows the Cloud Computing Architecture

In UCaaS, the service supplier gives the multi-stage collaboration over a system. Administrations for distinctive gadgets, for example, versatile augmentation and feature conferencing brought together unified messaging & web convention telephony. The parts incorporates multi-model communications & call control, instant and unified messaging, individual aid and speech access, conferencing and joint effort tools, portability, BPI (Business Process Integration) and programming to encourage BPI [11].

As indicated by IETF, suppliers of key model IaaS cloud offers machines and in the majority of the cases virtual machines, servers, load balancers, storage, VLANs, firewalls, software bundles and IP addresses [12].These extra resources or hypervisors might run the virtual machines as guests, for example, VMware ESX/ESXI, Xen and Oracle Virtual Box. In SaaS, programming applications by the SaaS's merchant are rented by the contracted party on the premise of pay every utilization costing strategy and administrations are accessible via web browser application. Ease of access and software can be customized and tailored to the needs and paid for.

Facilitating of SaaS suppliers can be through their own particular server farms or they can outsource it to different SaaS vendors. Consequently, the key empowering influence of SaaS is IaaS [13]. At this case, when the applications are accessed by means of web, the effort to establish safety is an indispensable need to secure the secret data of the users interacting. Different SaaS security models are connected by the application security authorities, for example, information insurance requirement through WS security, SSL usage and XML encryptions. Because of the non-accessibility of the common SaaS to the company's internal services, databases, diverse application programming interfaces and integration protocols are offered, for example, JSON, REST, HTTP and SOAP. Signally arranged, centrally hosted applications, regression tested & vendor accessible easily expedite & designed, user behavior monitoring & control and enhancement are the accelerated delivery features of SaaS applications.

PaaS, providers encourages the end users essentially developers with computing platform so as to adapt to multifaceted nature of managing and purchasing of the operating system and programming dialect with other processing devices, for example, databases, execution runtime, web servers, and additional hardware or programming layers.

In PaaS, for example, Google App Engine and Windows Azure , frameworks or systems and storage are customized consequently to meet the application run time prerequisites with the goal that the front end client don't have need to perform it physically.

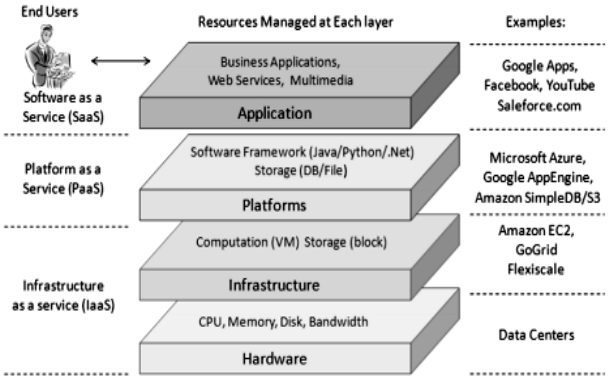

Fig.2. shows the Cloud Services Models

To encourage constant in cloud environment, PaaS has likewise been proposed by another structural modeling [14]. Since, the utilization of virtual machines utilized as a part of distributed computing precisely like an impetus to accelerate the procedure, along these lines the malevolent or malicious assault at PaaS layer ought to be secured through the requirement of exact validation check over the whole network system, particularly when the information is being exchanged, in this way the application integrity is likewise a thumping point to be dealt with while arranging the efforts to establish safety of cloud computing frameworks.

2.3 Analysis of Cloud Deployment Models:

S. Dhawan, 2014 urges that with progression in computing and technology the client security & privacy arrangements, laws and principles are a subject to be as often as possible and consistently overhauled [15]. For the examination and implementation of security suggestions it is critical to have sufficient investigation of cloud models. Since, it is a significant choice which sort of cloud is to be executed for which sort of association. Operation models of the clouds are largely public, private & hybrid.

An open or public cloud empowers the clients with availability of interfaces through standard web programs. Interest for cloud augmentation is catered through an adaptable pay-per-use model. IT cost to an operational level can be analyzed and compared by the cloud customers by means of diminishing its capital cost on the base of IT [16].

Public clouds are less secure mostly because of element of managing other information & applications running and don't subject to any security weakness. Security concerns are ubiquitous while managing public clouds particularly with cloud Services Level Agreements (SLAs). Whether the security controls are placed in the spot, it can be guaranteed by the key administration of SLAs. For the implementation of cloud check and validation over their

frameworks both vendor and customer commonly go ahead the same page of agreement and offer a joint obligation, in order to deal with cloud security they can further isolate the individual role for each party.

Private clouds are managed on association's internal adjusted enterprise datacenters, alongside ease of access, control over organization it can be solely adjusted to administrative, consistence and security necessities. Virtual applications and offer of pool resources are given by the dealer of private clouds to be utilized by cloud customers, it is managed by the organization like an intranet in this way cloud resources and applications are managed there. Private clouds are a great deal more secure then open clouds mostly because of the confined access and private particular & internal exposure and may be just accessed by the assigned and authorized stakeholders to maintain the security of confidential data.

In hybrid cloud computing environment some well defined resources are provided by the services providers externally while the others are managed and centralized by the organization itself. Thus hybrid model is a mixture of private and public cloud models with open architecture which enables the interface with a system management. Therefore, a holistically assessed security consideration tailored to the requirement of the organization help in adopting the suitable cloud model along with an advantage of scalability and cutting edge cost-effectiveness through this technology. Enterprise's architectural settings and information security are the key points to be considered while adopting any cloud deployment model.

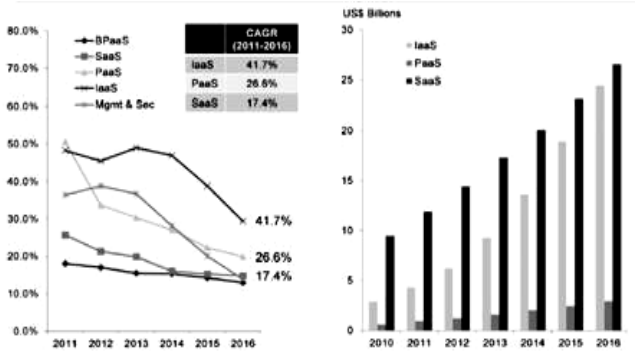

Fig.3. Public Cloud Services Forecast (Gartner) 2012.

Now the question arises, when we analyze the data storage on public clouds, it is a greatest concern of the corporate and individuals looking to transform their business through IT solutions and cloud computing convergence mainly for cutting the costs of maintenance

related to IT infrastructures. Major concern for the organizations adopting the cloud computing is to secure the sending and receiving of their confidential information. We must assume that as with data traffic through Wide Area Network (WAN), can be modified & intercepted. Therefore it is a matter of fact that data stored off the premises and traffic to cloud services providers must be encrypted. And data protecting mechanism must be ensured not only to protect the passwords and IDs but the other data which may be coming along while users are interacting through Clouds.

2.4 Key Security Mechanisms

First key mechanism is identification & authentication process, which targets to verify & validate the cloud users by their user names and passwords according to their cloud profiles. Users of cloud must be given permissions and supplementary access priorities. In private clouds mainly system administrators maintain the authorization in private cloud and helps sustaining the referential integrity, controls and privileges. Robust implementation of security protocols to enhance the user's confidentiality also plays major role to maintain the organizational data security across the multiple distributed databases. Different layers of cloud application may need enforcement of different security protocols.

Within the cloud domain application of due diligence process requires the integrity. Therefore, a robust implementation of ACID (atomicity, consistency, isolation and durability) for cloud data must be ensured. Additionally, the appliance of non-repudiation can be adopted in cloud computing with conventional e-commerce security protocols and provisioning of token can be adopted such as obtaining the signatures and time stamps. Availability of information security is most crucial in cloud computing when deciding a deployment model or choosing among the public, hybrid or private clouds. The SLAs are the most decisive & vital documentation that must be available to segregate the level of resources and services between client and cloud services provider.

Another security mechanism is adoption of Third Party Auditor (TPA), which can enable the Cloud Services Provider (CSP) with information to improve their p services platforms and Cloud User (CU) to evaluate the risk embedded with subscription of their cloud data [17].

With the popularity of this technological emergence, business and corporate people are striving hard to transform their IT infrastructure smoothly to cloud technology. Whereas to control the CU and sustain an effective technological business policy, it urges for the security concerns of cloud computing. Total security of information on the clouds is a serious concern of buyers for this technology, such as security models adopted by the cloud users. S. Dhawan

emphasized that technological advancement needs the organizations to ensure the security of their information & data through implementation of industry wide security standards, yet the standards are also subject to be upgraded accordingly [15]. Therefore, security algorithms, adoption of TPA [17] and other security mechanisms are subject to be on a continuous improvement to achieve the public cloud user's information security at receiving and sending ends.

4 Related Work

F. Gens shows with a survey results new IDC IT cloud services and explained the top benefits and challenges cloud services may encounter with. Associated challenges and different security issues were presented in the survey details, such as costing model, security, charging model, SLA's, migration and issue of interoperability for cloud [18]. Cloud security is evolving and emerging end of computer's network and information security. Associated infrastructure is referred to secure via internal and external controls, technologies and set of well defined adopted policies. Cloud security controls mainly deterrent, prevention, detection and corrective controls must be put in the place to defend against unseen system weakness and security threats especially for the public clouds users [19].

Morsy et al, 2010 discussed the cloud computing and related issues regarding cloud services models, stakeholders, offered characteristics and cloud architecture [20].

Gartner identified and presented the seven main ends such as confidential user access, authoritarian compliance, data locality, data isolation, revival, exploratory support and long term practicality [21]. On the other hand the Cloud Computing Use Case Discussion Group focuses on scenarios and related requirements such as security engineers, developers and customers, for different Use Case in the cloud model [22]. Balachandra et al, 2009 focused on the security SLA's objectives and specifications regarding data recovery, segregation and data locations [23]. Kresimir et al, 2010 elaborated the top level security concerns in the Cloud, like sensitive information privacy in payment and integrity of data [24]. Cloud Security Alliance (CSA) classified the cloud security concern areas into fourteen. The recent survey of CSA & IEEE urges that wide scale and accelerated adoption of Cloud Computing is hindered by the lack of security & response of regulatory & authoritarian drivers [25].

5 Conclusion

The paper emphasis on the cloud computing concepts, deployment models, data security analysis & future of this technology and urges the need of development for new security mechanisms and Cloud user's data privacy laws, as the additional data security concerns will

be required especially around the data jurisdiction because the tenant data or customer may not only stay alongside the same system, data center or same cloud service provider. It suggests the implementation of well-built encryption implementation on the sending & receiving ends in order to secure the data transmission on Cloud. It is also concluded that once the security & regulatory concerns are met, a smooth, wide scale and enterprise level transition to a secure, cost-effectively viable cloud system will be possible in near future.

REFERENCES

[1] Amazon Web Services, “What is cloud computing”, 19 MAR 2013.

[2] Baburajan, Rajani, "The Rising Cloud Storage Market Opportunity Strengthens Vendors," info TECH, August 24, 2011". It.tmcnet.com. 24 AUG 2011

[3] Oestreich, Ken, "Converged Infrastructure", CTO Forum. Thectoforum.com. 15 NOV 2010

[4] National Institute of Standards and Technology, "The NIST Definition of Cloud Computing", Retrieved 07 OCT 2014

[5] Farber, Dan, "The new geek chic: Data centers". CNET News. 25 June 2008

[6] He. Sijin; L. Guo, Y. Guo, M. Ghanem, "Improving Resource Utilisation in the Cloud Environment Using Multivariate Probabilistic Models", 2012 (2012 IEEE 5th International Conference on Cloud Computing (CLOUD). pp. 574–581. doi:10.1109/CLOUD.2012.66. ISBN 978-1-4673-2892-0.)

[7] He, Qiang, et al. "Formulating Cost-Effective Monitoring Strategies for Service-based Systems." (2013): 1-1.

[8] Mao, Ming; M. Humphrey, "A Performance Study on the VM Startup Time in the Cloud", (2012) (Proceedings of 2012 IEEE 5th International Conference on Cloud Computing (Cloud2012): 423. doi:10.1109/CLOUD.2012.103. ISBN 978-1-4673-2892-0.)

[9] King, Rachael, "Cloud Computing: Small Companies Take Flight". Bloomberg Business Week, 4 AUG 2008

[10] "Encrypted Storage and Key Management for the cloud". Cryptoclarity.com. 30 Jul 2009.

[11] Pleasant, Blair (2008-07-28). "What UC is and isn't "SearchUnifiedCommunications.com. Retrieved 2014-10-20.

[12] Amies, Alex; Sluiman, Harm; Tong, Qiang Guo; Liu, Guo Ning (July 2012). "Infrastructure as a Service Cloud Concept". Developing and Hosting Applications on the

Cloud. IBM Press. ISBN 978-0-13-306684-5.

[13] ISO. ISO 7498-2:1989. Information processing systems-Open Systems Interconnection. ISO 7498-2

[14] Boniface, M.; Nasser, B.; Papay, J.; Phillips, S.C.; Servin, A.; Xiaoyu Yang; Zlatev, Z.; Gogouvitis, S.V.; Katsaros, G.; Konstanteli, K.; Kousiouris, G.; Menychtas, A.; Kyriazis, D., "Platform-as-a-Service Architecture for Real-Time Quality of Service Management in Clouds," Internet and Web Applications and Services (ICIW), 2010 Fifth International Conference on , vol., no., pp.155,160, 9-15 May 2010 doi: 10.1109/ICIW.2010.91

[15] S. Dhawan, "Information and Data Security Concepts, Integrations, Limitations and Future," IJAIST, vol.30, no.30, pp.09-13, Sep.2014

[16] A Platform Computing Whitepaper, 'Enterprise Cloud Computing: Transforming IT', Platform Computing, pp6, 2010.

[17] M. A. Shah, R. Swaminathan and M. Baker, "Privacy-preserving audit and extraction of digital contents," Cryptology ePrint Archive, Report 2008/186, 2008, http://eprint.iacr.org/.

[18] F. Gens. (2009, Feb.). "New IDC IT Cloud Services Survey: Top Benefits and Challenges", IDC eXchange, Available: <http://blogs.idc.com/ie/?p=730>

[19] Krutz, Ronald L., and Russell Dean Vines. "Cloud Computing Security Architecture." Cloud Security: A Comprehensive Guide to Secure Cloud Computing. Indianapolis, IN: Wiley, 2010. 179-80.

[20] M.A. Morsy, J. Grundy and Müller I. "An Analysis of the Cloud Computing Security Problem" In PROC APSEC 2010 Cloud Workshop. 2010.

[21] "Gartner: Seven cloud-computing security risks". InfoWorld. 2008-07-02.

[22] Cloud Computing Use Case Discussion Group. "Cloud Computing Use Cases Version 3.0," 2010.

[23] R.K. Balachandra, P.V. Ramakrishna and A. Rakshit. "Cloud Security Issues." In PROC '09 IEEE International Conference on Services Computing, 2009, pp 517-520.

[24] P. Kresimir and H. Zeljko "Cloud computing security issues and challenges." In PROC Third International Conference on Advances in Human-oriented and Personalized Mechanisms, Technologies, and Services, 2010, pp. 344-349.

[25] "Security Guidance for Critical Areas of Focus in Cloud Computing". Cloud Security Alliance. 2011.