International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-3 Issue-12, May 2014

Cloud Computing and its Security Concerns A Survey

Shikha Dogra, Sahil

Abstract*— Cloud Computing is evolving into the most desirous computing technology especially because of its low cost & resource independence but also incurs some of the most threatening concerns to the future of this technology i.e. its security. This paper presents a brief introduction to Cloud Computing with a comprehensive review of the most discussed security concerns to Cloud Systems.

Keywords*— Grid Computing, Distributed Computing, Parallel Computing, Virtualization, Utility Computing, Image optimization, Image portability, Fault tolerance, Multitenancy, Virtual Appliance, OS Kernel, Cloud migration, DDoS, Virus, Data location, Data Recovery, Data Control, Data privacy, Data Availability, Data Transmission, Data Security, Data Reminisce, Data Disposal, Virtual Servers, Virtual Networks, Hypervisors, APIs, VM Portability, Uptime.

I.CLOUD COMPUTING

The concept of cloud computing has been defined formally at the end of 2006 by Eric Schmidt, the CEO of Google proposed the Google 101 plan. By NIST, cloud computing is defined as a model for enabling convenient, on demand network access to a shared pool of configurable resources (e.g. networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management efforts or cloud provider interaction[1].

Cloud Computing is a new computing model which comes from Grid computing, Distributed computing, Parallel computing, Virtualization technology, utility computing and other computing technologies [2]. Cloud refers to a network of provided resources, in which all resources are infinitely scalable and used as a utility [3] means; user can get services according to his needs.

NIST suggested a system architecture of cloud computing, which consists of three basic layers from bottom to the top including infrastructure layer, platform layer and application layer. These layers have different functions and provide different services respectively including IaaS (Infrastructure as a Service), PaaS (Platform as a Service), SaaS (Software as a Service) [4].

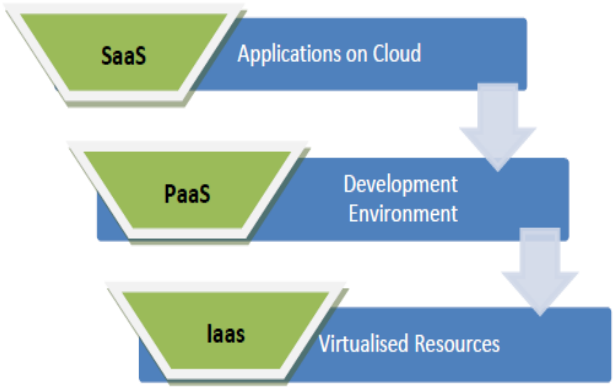

Fig.1. Layered Architecture of Cloud

IaaS (Infrastructure as a Service) is the basis of other two layers comprised of hardware resources abstracted by virtualization technology and distributed technology to provide a pool of unlimited virtual resources in the form of infrastructure as a service. Users subscribe to such services to utilize virtual infrastructure resources provided by cloud service provider. PaaS (Platform as a service) builds upon IaaS to provide development environment, runtime environment and management environment on cloud without depending upon end users hardware constraints. SaaS (Software as a service) works upon PaaS to provide applications run on clouds to fulfill users need without any constraints of application specific environment and save cost of software licenses. On the other hand, architecture of cloud computing can also be defined upon its deployment: public cloud, private cloud, hybrid cloud and community cloud. In public cloud, cloud services are available to general public or to a large section, owned and sold by cloud service providers. In private cloud, cloud services are purely used by an organization and managed by that organization or third party. In community cloud, a community of several organizations share services which are maintained by organizations or third party. Sometimes, there is need to deploy cloud in more than one of the above models to fulfill specific needs called hybrid cloud, where those clouds are bounded by standardized and proprietary technologies to maintain its integrity. Cloud can be viewed as a pool of resources where service providers provide services to users through internet [5]. Users only need to subscribe to required services without any consideration of hardware constraints and one-time payments for licenses because in cloud computing, users only need to use services according to their needs like pay as you go like utility models.

Manuscript published on 30 May 2014.
***Correspondence Author(s)**
Shikha Dogra, Department of Computer Science Engineering, Punjab Institute of Technology (Punjab Technical University Main Campus), Kapurthala, PB India.
Sahil, Department of Computer Science Engineering, Punjab Institute of Technology (Punjab Technical University Main Campus), Kapurthala, PB India.

© The Authors. Published by Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP). This is an open access article under the CC-BY-NC-ND license http://creativecommons.org/licenses/by-nc-nd/4.0/

For hardware constraints, all the physical resources required for demanding services is on cloud side, so a user only need to have a system with internet connection and a simple system configuration.

II.IMPETUS FOR CLOUD COMPUTING IN MARKET

The reason, why today's computing paradigm is transforming into cloud computing is the number of issues addressed by cloud computing and attain those solutions as its characteristics [6][7]:

A. Flexibility and Scalability

The characteristic of flexibility/elasticity which provisions and de-provisions resources according to demand to scale horizontally by increasing or decreasing number of systems and vertically by increasing and decreasing hardware configurations.

B. Scope of Network Access

Cloud Computing provides the standardized mechanism to access network by different platforms i.e. mobile phones, laptops and PDAs.

C. Location Independence

Cloud Computing abstracts the physical resources to provide virtualized resources, results in, users have the sense of location independence. But can specify location at a higher level of abstraction i.e. Country, State.

D. Economy of Scale

With the help of virtualization technology, a resource is further virtualized into many small resources results in better utilization of resources.

E. Reliability

Cloud Computing provides mechanisms to use redundant resources to provide higher degree of reliability and uptime.

F. Cost Effectiveness

As the sole idea of cloud computing is utility computing, where users only charged according to its usage irrespective of the one-time ownership cost of resources like in conventional computing. Hence provide cost effectiveness.

G. Sustainability

Cloud computing as because of improved utilization of resources, less carbon emission and results in efficient system, proves its sustainability.

Because of these facts, many agencies those study this technology assess its upcoming importance. In a press release, Gartner says, cloud computing will become the bulk of new IT spend by 2016[8].

III.CLOUD COMPUTING SECURITY CONCERNS

As cloud computing is comprised of various hardcore technologies like networking, virtualization, software development, it has a vivid scope of research in different directions. Image (OS kernel/Virtual Appliance) Optimization [9], Fault tolerance [10], Multitenancy [11], Cloud Migration [11], Virtualization [12], Security etc. But security concerns are the most prioritized one for end user to feel comfortable with cloud for software, data and processes, he uses in terms of its privacy, integrity etc [9].

As shown in Figure 3, a report of IDC (International Data Corporation) enterprise panel in August 2008 [13] states the problems facing during Cloud Computing Platform development shows how Cloud Computing Security dominates all other problems with the highest percentage of 87.5% . That's why this paper focuses on a comprehensive review of Cloud Computing Security concerns. The very basic view of Cloud Computing Security is based on the composition structure of Cloud Computing platform [14]. Cloud Computing platform has composed of three layers: Core resources layer, Centralized management layer & Foreign Services interface layer. Foreign Services Interface layer faces users, so security of this layer concerns with the user data protection. Hence need to use application layer encryptions, identity authentication, and SSL like security protections. Centralized Management interface layer is responsible for receiving, processing & managing scheduling system of user request. The security of this layer deals with software system security, data audit security & access management. The core layer deals with Physical resources & its management. The safety of this layer deals with network layer access security. So, this layer is the key to Cloud Computing platform Security. So, during the Cloud Computing Platform construction, need to consider some non-avoidable issues at different layers:

At Foreign Service layer [15],

- Interface Security: Interface of Cloud Systems should be rigid enough to resist injection, overflow vulnerability, cross-site attacks.
- Data Encryption: Need to use high strength encryption algorithms.
- Channel Safety: As because of the threat of data stealing by third party, need to secure channels using stronger authentications.

At Centralized Management Interface layer [15],

- Filter: Filter checks the data in terms of its validity & prevents illegal data entering into system. Also authenticate users to accessing using blacklists to prevent illegitimate user. So need to concern the security & integrity of filter.
- Audit: Auditing of data, authorization of users prevent internal problems.

At Core Resources layer [15],

- Firewall: Firewall protects resources from attacks.
- IDS/IPS: IDS/IPS provides flexible defensive strategies to protect systems.

Cloud Computing Security Concerns can also be defined from two perspectives [16]: One, from Traditional system security, where need to deal with virus, DDoS etc. Second, from cloud computing systems, where these concerns brought by cloud computing systems itself, where privacy, resource availability, data encryption etc. emerges as security concerns. Security concerns in cloud computing can also be divided at five different levels including clients, applications, platform, infrastructure and server [18]. Also the deployment models of cloud: Private, Public, Community and Hybrid have their own security concerns associated with them based on the user-domain in which it exists [19].

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)
© Copyright: All rights reserved.

In cloud computing, Identity and Access Management plays one of the most important parts for its security [10], which features how to authorize, authenticate and audit users who are accessing cloud services.

Concerns of account and service hijacking which involves phishing, fraud and other vulnerabilities where credentials are stolen and used to gain an unauthorized access to cloud threat the integrity, confidentiality and availability of data services [20].

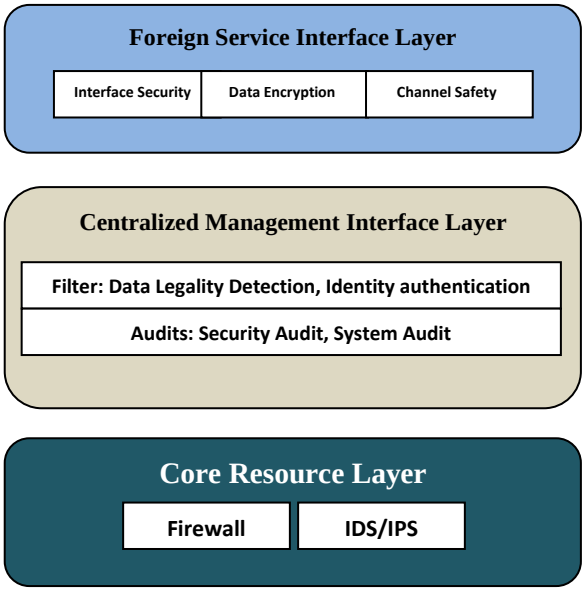

Fig.2. Security Issues at different layers of Cloud Computing Platform [15]

Even malicious insiders can severely impact the organization in terms of brand damage, financial and productivity losses. In cloud, there is need to have strong authentication mechanism [21].

Regulations for privacy of information vary across the world, which needs to comply with those ones. Concerns regarding compliance risk are because of lack of governance for audits [20]. There is not any provision for audits of Cloud Service Providers [22]. If, Cloud Service Providers outsource services to 3_{rd} party not in fully transparent manner, a user must have to inspect the process [23][24]. In case of data loss, user has no right to claim on Service Provider.

The concerns of securing data in transmission [25] introduce the concept of encryption to secure data and access by authorized user only. User Identity [25] concerns emerges because cloud services are metered and should be only used by authenticated user.

Protection of data in storage [25] is another challenge in Cloud Computing environment. Data location, Data Recovery, Data Control, Data privacy, Data Availability, Data Transmission, Data Security, Data Reminisce issues and Data Disposal are some common and important concerns regarding data in cloud environment requires to be properly encrypted, transmitted, protected, controlled and available in timely manner [26][27][24][21][28][29][30].

Protection of Virtual Servers and Virtual Networks are as important as its non virtual counterparts. Network attacks present a bigger concern in cloud environment [25]. Misconfiguration of network firewalls and inadequate security configuration in cloud environment and on-network emerges as security holes for illegitimate users [24].

Virtualization Technology presents new challenges in security like virtual traffic analysis, integrity of virtual machines etc.[31].VM level vulnerabilities occur because of faulty implementation of VM Hypervisors[20][32]. Insecure APIs expose organizations to risks like unauthorized access, reusable token, logging capabilities and content transmission [20].

Reputation Fate Sharing[33], which transfer errors from one server to each virtual machine by that corrupted server also need to be addressed using best practices[21]. Quality of Services also required to be focused as Cloud Service Providers are only focusing on fast performance and low cost [22]. Issues of Multitenancy present the threat of information leakage and exploitation when sharing applications and hardware in virtualization [27].

Virtual Machine portability needs to be secured for cloud migration as residual data of ported Virtual machine on former cloud presents threats to security of Virtual Machines[20][34].

Migrating computing to cloud computing increases Internet dependencies, which presents concerns of Internet reliability.

IV.CONCLUSION

Although whatsoever the concerns regarding security of Cloud Computing, yet there is need to do an extensive research in the field of Cloud Computing Security, because the emergence of new technology totally depends upon the trust it builds upon with its users. That's why this paper is drafted so can provide a one stop purview of the Cloud Computing Security concerns & motivate new researchers in this field.

This paper firstly briefs about the Cloud Computing then presents various security concerns regarding Cloud Computing from different perspectives i.e. from the perspective of Cloud Computing Construction, from the perspective of its service layered architecture, from the perspective of tradition system, Clouds system, Server-Client computing etc. to ensure the reader to get maximum from this comprehensive review study.

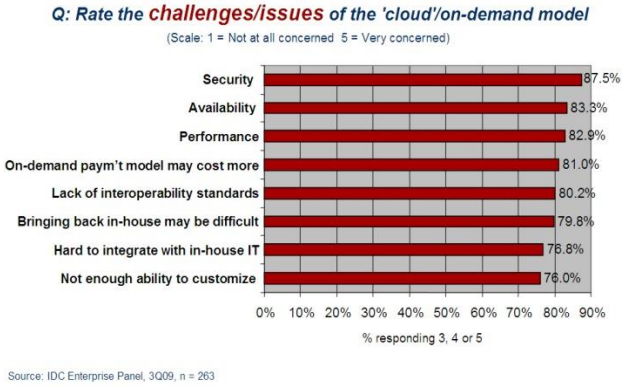

Fig.3. Ranking of facing problems during Cloud Computing platform construction

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)
© Copyright: All rights reserved.

REFERENCES

1. Mell, Peter, and Tim Grance. "The NIST definition of cloud computing." National Institute of Standards and Technology 53, no. 6 (2009): 50.
2. Liu, Wentao. "Research on cloud computing security problem and strategy." In Consumer Electronics, Communications and Networks (CECNet), 2012 2nd International Conference on, pp. 1216-1219. IEEE, 2012.
3. Lin, Guoman. "Research on electronic data security strategy based on cloud computing." In Consumer Electronics, Communications and Networks (CECNet), 2012 2nd International Conference on, pp. 1228-1231. IEEE, 2012.
4. Jamil, Danish, and Hassan Zaki. "CLOUD COMPUTING SECURITY." International Journal of Engineering Science & Technology 3, no. 4 (2011).
5. Panneerselvam, John, Lu Liu, Richard Hill, Yongzhao Zhan, and Weining Liu. "An investigation of the effect of cloud computing on network management." In High Performance Computing and Communication & 2012 IEEE 9th International Conference on Embedded Software and Systems (HPCC-ICESS), 2012 IEEE 14th International Conference on, pp. 1794-1799. IEEE, 2012.
6. Reese, George. Cloud application architectures: building applications and infrastructure in the cloud. " O'Reilly Media, Inc.", 2009.
7. Buyya, Rajkumar, Chee Shin Yeo, Srikumar Venugopal, James Broberg, and Ivona Brandic. "Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility." Future Generation computer systems 25, no. 6 (2009): 599-616.
8. Gartner, "Gartner Says Cloud Computing Will Become the Bulk of New IT Spend by 2016," [Online]. 2013.Available: http://www.gartner.com/newsroom/id/2613015
9. A Vouk, Mladen. "Cloud computing–issues, research and implementations." CIT. Journal of Computing and Information Technology 16, no. 4 (2008): 235-246..
10. Bala, Anju, and Inderveer Chana. "Fault Tolerance-Challenges, Techniques and Implementation in Cloud Computing." International Journal of Computer Science Issues (IJCSI) 9, no. 1 (2012).
11. Schubert, Lutz, and Keith Jeffery. "Advances in clouds." Report of the Cloud Computing Expert Working Group. European Commission (2012).
12. Arora, Pankaj, Rubal Chaudhry Wadhawan, and Er Satinder Pal Ahuja. "Cloud computing security issues in infrastructure as a service." International Journal of Advanced Research in Computer Science and Software Engineering 2, no. 1 (2012).
13. Gens, Frank. "Problems facing during Cloud Computing Platform Construction." [Online]. December 2009. Available: http://blogs.idc.com/ie/?p=730
14. Wanyun, L. "Cloud computing: Enterprise information construction strategy and practice." in Tsinghua University Press, 20 I 0 (In Chinese).
15. Yuel, He, and Che Mingl. "Cloud Computing Security Infrastructure Based on the Isolation Concept."
16. Zhijun, Wang, and Zhang Ni. "A Survey on Cloud Computing Security."
17. Mell, P., and T. Grance. "The NIST Definition of Cloud Computing, Version 15, National Institute of Standards and Technology, October 7, 2009." (2009).
18. Jain, Pritesh, Dheeraj Rane, and Shyam Patidar. "A survey and analysis of cloud model-based security for computing secure cloud bursting and aggregation in renal environment." In Information and Communication Technologies (WICT), 2011 World Congress on, pp. 456-461. IEEE, 2011.
19. Gowrigolla, Bhagyaraj, Sathyalakshmi Sivaji, and M. Roberts Masillamani. "Design and auditing of cloud computing security." In Information and Automation for Sustainability (ICIAFs), 2010 5th International Conference on, pp. 292-297. IEEE, 2010.
20. Tripathi, Alok, and Abhinav Mishra. "Cloud computing security considerations." In Signal Processing, Communications and Computing (ICSPCC), 2011 IEEE International Conference on, pp. 1-5. IEEE, 2011.
21. Lv, Haoyong, and Yin Hu. "Analysis and research about cloud computing security protect policy." In Intelligence Science and Information Engineering (ISIE), 2011 International Conference on, pp. 214-216. IEEE, 2011.
22. "A Survey on Cloud Computing Security, Challenges and Threats| Whitepapers | TechRepublic."[Online].Available: http://www.techrepublic.com/whitepapers/a-survey-on-cloudcomputing-security-challenges-and-threats/3483757
23. Archer, Jerry, Alan Boehme, Dave Cullinane, Paul Kurtz, Nils Puhlmann, and Jim Reavis. "Top threats to cloud computing v1. 0." Cloud Security Alliance (2010).
24. Gonzalez, Nelson, Charles Miers, Fernando Redígolo, Marcos Simplício, Tereza Carvalho, Mats Näslund, and Makan Pourzandi. "A quantitative analysis of current security concerns and solutions for cloud computing." Journal of Cloud Computing 1, no. 1 (2012): 1-18.
25. Kulkarni, Gurudatt, Jayant Gambhir, Tejswini Patil, and Amruta Dongare. "A security aspects in cloud computing." In Software Engineering and Service Science (ICSESS), 2012 IEEE 3rd International Conference on, pp. 547-550. IEEE, 2012.
26. Wang, Jun-jie, and Sen Mu. "Security issues and countermeasures in cloud computing." In Grey Systems and Intelligent Services (GSIS), 2011 IEEE International Conference on, pp. 843-846. IEEE, 2011.
27. Behl, Akhil. "Emerging security challenges in cloud computing: An insight to cloud security challenges and their mitigation." In Information and Communication Technologies (WICT), 2011 World Congress on, pp. 217-222. IEEE, 2011.
28. Bhardwaj, Aashish, and Vikas Kumar. "Cloud security assessment and identity management." In Computer and Information Technology (ICCIT), 2011 14th International Conference on, pp. 387-392. IEEE, 2011.
29. Mahmood, Zaigham. "Data Location and Security Issues in Cloud Computing." In Emerging Intelligent Data and Web Technologies (EIDWT), 2011 International Conference on, pp. 49-54. IEEE, 2011.
30. Wen, Fu, and Li Xiang. "The study on data security in Cloud Computing based on Virtualization." In IT in Medicine and Education (ITME), 2011 International Symposium on, vol. 2, pp. 257-261. IEEE, 2011.
31. Yandong, Zhang, and Zhang Yongsheng. "Cloud computing and cloud security challenges." In Information Technology in Medicine and Education (ITME), 2012 International Symposium on, vol. 2, pp. 1084-1088. IEEE, 2012.
32. Mollet, Ngongang Guy. "Cloud Computing Security." Bachelor of Engineering Degree Information Technology Thesis, Helsinki Metropolia University of Applied Sciences, Helsinki, Finland 11 (2011).
33. Roberts II, John C., and Wasim Al-Hamdani. "Who can you trust in the cloud?: A review of security issues within cloud computing." In Proceedings of the 2011 Information Security Curriculum Development Conference, pp. 15-19. ACM, 2011.
34. Mathisen, Eystein. "Security challenges and solutions in cloud computing." In Digital Ecosystems and Technologies Conference (DEST), 2011 Proceedings of the 5th IEEE International Conference on, pp. 208-212. IEEE, 2011.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)
© Copyright: All rights reserved.