Cloud Computing: Security Issues and Challenges

Sheetal Mavi*

Abstract

Cloud computing is an architecture which provides computing services over the internet on demands and pay per use access to shared resources namely networks, storages, servers, services and applications, without physically acquirance. So it saves managing cost and time for organizations. Many industries like banking, healthcare sectors and education sectors are moving towards the cloud computing due to the efficiency of services and resources like using processing power, transaction carried out, bandwidth consuming, data transformation, or storage space occupying etc which is provided to users on basis of pay per use pattern. Cloud computing is fully internet dependent technology where client data is stored and maintained in the data center of a cloud provider like Google, Amazon, Salesforce.som and Microsoft etc.

Keywords: Cloud computing, security, privacy, encryption, Security Management Model.

I. Introduction

Cloud Computing has emerged as a scalable services consumption and carriage platform in the area of Services now. The main enabling technology of Cloud Computing includes Virtualizations and Service-Oriented Architecture (SOA) of hardware and software. The aim of Cloud Computing is to provide environment for the collaboration and share the resources among the cloud service consumers, cloud partners, cloud vendors and stakeholders in the cloud value chain. The resources shared at different levels result in various cloud offerings framework as infrastructure cloud (e.g. hardware, IT infrastructure management), Software cloud (SAAS focuses on middleware as a service, or classic Consumer Relationship Management as a service), application cloud (e.g. Application as a Service, UML (Unified Modelling Tools) modelling tools as a service, social network as a service), and business cloud (e.g. business processing as a service). "Cloud computing" is the natural step in the emerging scenario of on-demand technology services and products. To a large extent, cloud computing is based on virtualized envision resources. Cloud computing forerunners have been around for some time now [1, 12, 15, 17, 18, 24, 29, 30, 35, 40], but the term became "favoured" sometime in October 2007 when IBM and Google announced a collaboration in that domain [27, 22]. It was followed by IBM's announcement of the "Blue Cloud" effort [23]. Since then, everyone is talking about "Cloud Computing". Of course, there also is an unavoidable Wikipedia entry [45]. VCL has been in production use at NC State University since 2004, and is a suitable vehicle for dynamic implementation of almost any current "cloud" computing solution. This discusses "cloud"-related research and engineering challenges and summarizes and concludes the paper.

Cloud Computing -A key differentiating element of a successful information technology is its ability to become reliable, valuable, economical and true contributor to digital infrastructure [4]. "Cloud" computing embraces digital infrastructure, and builds upon decades of research in virtualization, "grid computing", utility computing, distributed computing, and, more recently, networking, web and software services. It provides service as oriented architecture, reduced information technology to head for the end-user, greater flexibility, reduced total cost of ownership for users. This paper discusses the concept of security issues and challenges in "cloud" computing, it tries to address, related research challenges, and a "cloud" implementation available today.

Sheetal Mavi*
Management of Educational and Research Institute
Guru Gobind Singh Indraprastha University

II. Issues in Cloud

Security is the important aspect in the field of computing, as it an obvious expectation for users. The security issues are crucial for cloud environment too. As the cloud computing approach can be associated with the user's sensitive data stored both at client's end as well as in cloud servers, identity management and

authentication are much prioritized in cloud computing (Kim & Hong, 2012; Emam, 2013; Han, Susilo & Mu, 2013; Yassin, Jin, Ibrahim, Qiang & Zou, 2012). Verification of eligible users' credentials and protecting such credentials are the part of the main security issues in the cloud – violation. In these, areas could lead to undetected security breach (Kumar, 2012) at least to some extent for some period. We are residing everything as in providers' premises which makes the information highly unsecured .It is the main barrier in adoption of cloud computing. Some security concerns are mention below

#1: Company has breach the law (risk of data seizure by (foreign) government).

#2: Storage services provided by one cloud seller may be incompatible with another seller's services if user decides to move from one to the other (e.g. Microsoft cloud is incompatible with Google cloud).

#3: Who controls the encryption/decryption keys? Logically it should be the customer who controls these keys.

#4: Ensuring the integrity of the data like transfer, storage, and retrieval means that it changes only in response to authorized transactions. A common standard to ensure data integrity does not yet exist.

#5: Some government regulations have some strict limits on the data for its citizens that can be stored and for how long, and some banking regulators require that customer's financial data remain in their home country

#6: Customers may be able to sue cloud service providers if their privacy rights are breach or violated, and in any case the cloud service providers may face harm to their reputation. Concerns arise when it is not clear to the individuals why their personal information is requested or how it will be used or send to other parties.

#7: With the cloud model the control physical security is lost as because of shared computing resources with other companies, No knowledge or control of the resources to run.

#8: The dynamic and fluid nature of virtual machines will make it difficult to maintain the consistency of security and ensure the audit ability of records.

#9: In case of Payment Card Industry Data Security Standard (PCI DSS) data logs must be provided to security managers and regulators.

#10: Security concern #10: Users must keep up to date with application improvements to be sure they are protected.

Cloud computing enters with various possibilities and challenges simultaneously. Of the major challenges, security is appraised to be a critical obstacle for cloud computing in its track to success (Khorshed, Ali & Wasimi, 2012). The security challenges for cloud computing approach are somewhat strong and huge. Data location is an important factor in cloud computing security (Teneyuca, 2011). Location transparency is one of the well known workable flexibilities for cloud computing, which is also a security threat at the same time – without knowing the specific location of data storage, the provision of data protection act for some region might be severely affected and violated and could be damaged. Cloud users' personal data security is thus a crucial concern in a cloud computing environment (Joint, Baker & Eccles, 2009; Ismail, 2011; King & Raja, 2012). In terms of customers' personal or business data security, the strategic policies of the cloud providers are of the highest significance (Joint & Baker, 2011) as the technical security alone is not adequate to address the problem. Trust is one of the another problem which raises security concerns to use cloud service (Ryan & Falvy, 2012) for the reason that it is directly related to the authority and authenticity of the cloud service providers. Trust establishment might become the key to create a successful cloud computing environment. The provision of trust model is crucial in cloud computing as this is a common interest area for all stakeholders or vendors for any given cloud computing scenario. Trust in cloud can be depend on a number of factors among which some are automation management, human factors areas, processes and policies (Abbadi & Martin, 2011). Trust in cloud is not a technical security issue, but it is the most influential soft factor that is driven by security issues inherent in cloud computing to a great extent.

III. Some Solution For Security Issues In Cloud Computing

Following given approaches can be helpful to secure the cloud computing

- Investigation Support: Analysis tools are provided to the users to observe how the data gets stored, used and protected, and verify the policy of enforcement. But the investigation of illegal action is very difficult because data for multiple customers may be collocated and it may also be geographically spread across set of hosts and data centers. To solve this audit tools must be contractually committed along with the evidence.
- Network Security: A user can contradict the access of any Internet based service by using IP Spoofing which can be a cause of security harm [6]. To solve this problem we can use Digital Signature technique. SSL (Secure Socket Layer) Protocol used for managing security of message transmission on The Internet which also avoids resource hacking problem.
- Encryption Algorithm: Obviously cloud service providers encrypt the user's information using strong encryption algorithm. But problem is that encryption accident can make data totally unusable and encryption also complicates the availability [6]. To solve this problem the cloud provider must provide evidence or proof that encryption scheme were designed and tested by experienced specialists.
- Backup: The physical devices can be damaged by the natural disasters that may cause the loss of data. To avoid this problem, the key of assurance of service is backup of information provided by vendor.
- Customer satisfaction: It seems quite hard for the customer to verify the recently implemented security practices and an initiative of a cloud computing provided by the service provider because the customers generally has no access Rajesh et al , International Journal of Advanced Research in Computer Science and Software Engineering 2 (9), September- 2012, pp. 115-120 © 2012, IJARCSSE All Rights Reserved Page | 118 to the provider's facility which can be comprised of multiple facilities spread around the globe [8]. Solution for this Provider should get some standard certificate from some governing or standardized institution that ensures users that provider has established adequate internal control and these control are operating efficiently.

IV. Security Management Model (SMM)

This section contains twenty recommended models of security management and their requirements for cloud computing service providers should definitely consider as they evolve their compliance programs

1) Security management (People): It is very important to develop a formal charter for the security organization and agenda. The charter should be ally with the strategic plan of the organization or company the security team works for. Lack of responsibilities and clear define roles and agreement on expectations, can result in a confusion and loss among the team of security about what is expected of them, how their experience and skills can be edged, and meeting their performance goals.

2) Security governance: A security guiding committee should be evolved whose main aim is to focus on guidance on security initiatives and alignment with business and the IT strategies. This committee should clearly define the roles and responsibilities of the security management team and other groups involved in performing information security functions.

3) Software-as-a-Service (SaaS) security: SaaS is the major cloud service model for the computable future and the area where the most critical need for security practices and oversight will reside. Just as with a managed service provider, corporations or end users will need to research vendors' policies on data security before using vendor services to avoid losing or not being able to access their data. The technology analyst and consulting firm Gartner lists [14] seven security risks which one should discuss with a cloud-computing vendor: Privileged user access: Get as much information as you can about the people who manage your data. Ask providers to supply specific information on the hiring and oversight of privileged administrators, and the controls over their access. Regulatory compliance: Make sure that the vendor is willing to undergo external audits and/or security certifications. Data location: When you use the cloud, you probably won't know exactly where your data is hosted. In fact, you might not

even know what country it will be stored in. Ask providers if they will commit to storing and processing data in specific jurisdictions, and whether they will make a contractual commitment to obey local privacy requirements on behalf of their customers.

Data segregation: Make sure that encryption should available at all stages, and that these encryption schemes were tested, designed and maintained by experienced professionals. Recovery: Even if you don't know where your data is, a cloud provider should tell you what will happen to your data and service in case of a disaster. Any offering that does not replicate the data and application infrastructure across multiple sites is vulnerable to a total failure. Ask your provider if it has "the ability to do a complete restoration, and how long it will take." Investigative support: Investigating inappropriate or illegal activity may be impossible in cloud computing. Cloud services are especially difficult to investigate, because logging and data for multiple customers may be co-located and may also be spread across an ever-changing set of hosts and data centers. If you cannot get a allowable commitment to support specific forms of investigation, along with proof that the vendor has already successfully supported such activities, then only safe assumption is that investigation and discovery requests will be impossible. Long-term viability: Ideally, the cloud computing provider will never go broke or get acquired and tolerated up by a larger company. But you must be sure that your data should remain available even after such an event. Ask potential providers how you would get your data back and if it would be in a format that you could import into a replacement application. To address the security issues listed above, SaaS providers will need to incorporate and enhance security practices used by the managed service providers and develop new ones as the cloud computing environment evolves.

4) Risk management: Risk management entails identification of technology assets [15]; identification of data and its links to business processes, applications, and data stores; and assignment of ownership and custodial responsibilities. Actions should also include maintaining a repository of information assets. Owners have authority and accountability for information assets including protection requirements, and custodians implement confidentiality, integrity, availability, and privacy controls.

5) Risk Evaluation: Security risk assessment is critical to helping the information security organization make informed decisions when balancing the duelling priorities of business utility and protection of assets [16][17]. A formal information security risk management process should proactively assess information security risks as well as plan and manage them on a periodic or as -needed basis. More detailed and technical security risk assessments in the form of threat modelling should also be applied to applications and infrastructure.

6) Data governance: This framework should describe that who can take what actions with what information, and when, under what circumstances, and using what methods.

7) Virtual machine security: In the cloud environment, physical servers are stabilized to multiple virtual machine instances on virtualized servers. Not only data center security teams can replicate typical security controls for the data center at large scale to secure the virtual machines, they can also advise their customers or vendors on how to prepare these machines for migration to a cloud environment when suitable.

8) Disaster recovery: In the SaaS environment, customers can depend heavily on access to their services and any intervention in access can be disastrous. With the help of virtualization software virtual server can be backed up, moved and copied just like a file (live migration). Benefit is quickly reallocating computing resources without any downtime

   Ability to deliver on service-level agreements and provide high-quality service

9) Third party risk management: Lack of a third-party risk management program may result in

damage to the provider's reputation, revenue losses, and legal actions should the provider be found not to have performed due diligence on its third-party vendors.

10) Vulnerability assessment: Classifies network assets to more efficiently prioritize vulnerability-mitigation programs, such as patching and system upgrading.

11) Security image testing: Virtualization-based cloud computing provides the ability to create "Test image" VM secure builds and to clone multiple copies. Gold image Virtual machines also provide the ability to keep security up to date and reduce exposure by patching offline. Offline virtual machines can be patched off-network, providing an easier, more cost-effective, and less production-threatening way to test the impact of security changes.

12) Security awareness: People are the weakest link for security. Knowledge, culture and awareness are among the few effective tools to manage risks related to people. Not providing proper awareness and training to the people who may need them can expose the company.

V. Conclusions

Cloud computing has various prospects, but the security threats embedded in cloud computing approach are directly proportional to its proposed advantages. Cloud computing is a great opportunity and profitable option both to the businesses and the attackers – either parties can have their own advantages from cloud computing. The huge possibilities of cloud computing cannot be ignored simply for the security issues reason – the ongoing investigation and research for robust, consistent and integrated security models for cloud computing could be the only path of motivation. The security issues could severely affect infrastructures. Security itself is conceptualized in cloud computing infrastructure as a distinct layer (Dukaric & Juric, 2013). Security for cloud computing environment is a non-compromising requirement. Cloud computing is inevitable to become the ideal (and possibly the ultimate) approach to business computing though the security barriers along with other issues need to be solved for cloud computing to International Journal of Network Security & Its Applications (IJNSA), Vol.6, No.1, January 2014 33 make it more viable (Marston, Li, Bandyopadhyay, Zhang & Ghalsasi, 2011) ., Given its total benefits and dynamism provided that it is deployed with in an integrated and secure infrastructural framework, cloud computing can offer virtual ownership and access to 'super computers' without achieving them physically. Perhaps this is what inspired the term SCC (Scientific Cloud Computing). Research effort has been contributed to develop faster yet secured SCC tools (Jorissen, Villa & Rehr, 2012) which will greatly inspire the era of research and motivation in various fields of clouding computing itself. The social conclusion of cloud computing approaches can emerge with severe impact if robust security models for cloud computing does not exist. The issues in security for cloud computing are not related to direct security and technical aperture only; a number of social deviation may be resulted even when there is no 'hard' security breach taken place. The dispersive processing like transmission and storage features is behind reason. One of the examples is the obtaining of digital clues. The evolution of cloud computing might significantly affect the collection and retention of digital evidence (Mason & George, 2011). The vastness and potentiality of cloud computing cannot be overlooked, subsequently robust security models for cloud computing scenarios is the most prioritized factor for a successful cloud based infrastructure development and deployment. With the goal of secured exploitation of a Service Oriented Architecture, the security aspects and issues of cloud computing are inherent not only with the elements that from the cloud infrastructure but also with all associated services as well as the ways computing is done both at the users' and the cloud service providers' ends. The security issues in cloud computing are somewhat sensitive and crucial on the basis of sociological and technological viewpoints – the technological inconsistency that results in security breach in cloud computing might lead to significant sociological impacts. As a result, when dealing with cloud computing and its security issues, technical as well as epistemological factors are equally important to take into consideration. Based on the fact that the

impact of cloud computing can include both the technical and social settings, the research on cloud computing and its related concerns are not related only with computing aspects. Service oriented architecture and other characteristics of cloud computing suggests that the concept of cloud computing would require to analyze the practicality in line with social, business, technical and legal perspectives – all these facets will incorporate security issues either in technical or strategic form. Even if not considering the nature of security issues, it can be doubtless concluded that the acute unfavorable effects as a result of security in cloud computing, the classification of any form of cloud computing should deal with the security concerns corresponding to those of the safety critical systems.

References

1. Abbadi, I.M. and Martin, A. (2011). Trust in the Cloud. Information Security Technical Report, 16, 108-114. doi:10.1016/j.istr.2011.08.006
2. Agarwal, A. and Agarwal, A. (2011). The Security Risks Associated with Cloud Computing. International Journal of Computer Applications in Engineering Sciences, 1 (Special Issue on CNS), 257-259.
3. Arshad, J, Townsend, P. and Xu, J. (2013).A novel intrusion severity analysis approach for Clouds. Future Generation Computer Systems, 29, 416–428. doi:10.1016/j.future.2011.08.009
4. Atayero, A.A. and Feyisetan, O. (2011). Security Issues in Cloud Computing: The Potentials of Homomorphic Encryption. Journal of Emerging Trends in Computing and Information Sciences, 2(10), 546-552.
5. Bisong, A. and Rahman, S.S.M. (2011). An Overview of the Security Concerns in Enterprise Cloud Computing. International Journal of Network Security & Its Applications, 3(1), 30-45. doi:10.5121/ijnsa.2011.3103
6. Buyya, R., Yeo, C.S., Venugopal, S., Broberg, J. and Brandic, I. (2009). Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. Future Generation Computer Systems, 25, 599–616
7. Amazon Elastic Compute Cloud (EC2): http://www.amazon.com/gp/browse.html? node=201590011, accessed Dec 2008.
8. ILKAY ALTINTAS, BERTRAM LUDAESCHER, SCOTT KLASKY, MLADEN A. VOUK. "Introduction to scientific workflow management and the Kepler system", Tutorial, in Proceedings of the 2006 ACM/IEEE Conference on Supercomputing, Tampa, Florida, TUTORIAL SESSION, Article No. 205, 2006, ISBN:0-7695-2700-0, also given at Supercomputing 2007 by Altintas, Vouk, Klasky, Podhorszki, and Crawl, tutorial session S07, 11 Nov 07.
9. ILKAY ALTINTAS, GEORGE CHIN, DANIEL CRAWL, TERENCE CRITCHLOW, DAVID KOOP, JEFF LIGON, BERTRAM LUDAESCHER, PIERRE MOUALLEM1, MEIYAPPAN NAGAPPAN, NORBERT PODHORSZKI, CLAUDIO SILVA, MLADEN VOUK, "Provenance in Kepler-based Scientific Workflow Systems", Poster # 41, at Microsoft eScience Workshop Friday Center, University of North Carolina, Chapell Hill, NC, October 13 – 15, 2007, pp. 82.
10. D.E. ATKINS ET AL., "Revolutionizing Science and Engineering Through Cyber infrastructure: Report of the National Science Foundation Blue-ribbon Advisory Panel on Cyber infrastructure", NSF, Report of the National Science Foundation Blue-ribbon Advisory Panel on Cyberinfra structure, January 2003, http://www.nsf.gov/od/oci/ reports/atkins.pdf [5] Ditto, Appendix A (http://www.nsf.gov/od/ oci/reports/APXA.pdf). [6] SAM AVERITT, MICHALE BUGAEV, AARON PEELER, HENRY SCHAFFER, ERIC SILLS, SARAH STEIN, JOSH THOMPSON, MLADEN VOUK, "The Virtual Computing Laboratory", Proceedings of the International Conference on Virtual Computing Initiative, May 7-8, 2007, IBM Corp., Research Triangle Park, NC, pp. 1–16.

11. ROSELYNE BARRETO, TERENCE CRITCHLOW, AYLA KHAN, SCOTT KLASKY, LEENA KORA, JEFFREY LIGON, PIERRE MOUALLEM, MEIYAPPAN NAGAP- PAN, NORBERT PODHORSZKI, MLADEN VOUK, "Managing and Monitoring Scientific Workflows through Dashboards", Poster # 93, at Microsoft eScience Workshop Friday Center, University of North Carolina, Chapell Hill, NC, October 13 – 15, 2007, pp. 108.
12. D.A. BATCHELOR, M. BECK, A. BECOULET, R.V. BUDNY, C. S. CHANG, P. H. DIAMOND, J. Q. DONG, G. Y. FU, A. FUKUYAMA, T. S. HAHM, D. E. KEYES, Y. KISHIMOTO, S. KLASKY, L. L. LAO1, K. LI1, Z. LIND 1, B. LUDAESCHER, J. MANICKAM, N. NAKA- JIMA1, T. OZEKI1, N. PODHORSZKI, W. M. TANG, M. A. VOUK, R. E. WALTZ, S. J. WANG, H. R. WIL- SON, X. Q. XU, M. YAGI, F. ZONCA, "Simulation of Fusion Plasmas: Current Status and Future Direction", Plasma Science and Technology, Vol. 9, No. 3, Jun. 2007, pp. 312–387, doi:10.1088/1009- 0630/9/3/13.
13. MICHAEL BELL, "Introduction to Service-oriented Modeling", Service-oriented Modeling: Service Analysis, Design, and Architecture. Wiley & Sons, 3. ISBN 978-0-470-14111-3, 2008.
14. W. M. BULKELEY, "IBM, Google, Universities Combine 'Cloud' Foces", Wall Street Journal, October 8, 2007, http://online.wsj.com/public/article print/SB119180611310551864.html
15. http://www.cca-forum.org/, accessed February 2006.
16. CONDOR: http://www.cs.wisc.edu/condor/, accessed May 2008.
17. CRNKOVIC AND M. LARSSON (EDITORS), Building Reliable Component-based Software Systems, Artech House Publishers, ISBN 1-58053-327-2, 2002, http://www.idt.mdh.se/cbse-book/ [14] R. L. DENNIS, D. W. BYUN, J. H. NOVAK, K. J. GALLUPPI, C. C. COATS, M. A. VOUK, "The Next Generation of Integrated Air Quality Modeling: EPA's Models-3", Atmospheric Environment, Vol. 30 (12), pp. 1925–1938, 1996.
18. http://www.thecloudcomputing.org/2013/research.html
19. GLOBUS: http://www.globus.org/, accessed May 2008.
20. HADOOP: http://hadoop.apache.org/core/, accessed May 2008.
21. ELIAS N. HOUSTIS, JOHN R. RICE, EFSTRATIOS GAL- LOPOULOS, RANDALL BRAMLEY (EDITORS), Enabling Technologies for Computational Science Frameworks, Middleware and Environments, Kluwer-Academic Publishers, Hardbound, ISBN 0-7923-7809-1, 2000.
22. M. HSU (ED.), "Special Issue on Workflow and Extended Transaction Systems", IEEE Data Engineering, Vol. 16(2), June 1993. [21] IBM, "IBM Launches New System x Servers and Software Targeting Large Scale x86 Virtualization, http://www-03.ibm.com/press/us/en/ press release/19545.wss, 21 Apr 2006.