International Journal of Computer Networking, Wireless
and Mobile Communications (IJCNWMC)
Vol.1, Issue 2 Dec 2011 59-68
© TJPRC Pvt. Ltd.,

SECURITY ASSESSMENTS AND RESEARCH DIRECTIONS IN CLOUD COMPUTING

Mr.HIREN B. PATEL
Department of Computer Engineering, S. P. College of Engineering,
Visnagar, India – 384315 hbpatel1976@yahoo.com

Mr. DHIREN R. PATEL
Department of Computer Engineering, S. V. National Institute of Technology,
Surat, India – 395007 dhiren29p@gmail.com

ABSTRACT

Cloud computing offers abundant key benefits to business such as cost reduction, automation, resource independence, high availability, augmented elasticity etc. It also comes with some security barriers such as confidentiality, privacy, integrity etc. As Cloud computing is not just an improvement in technology but also how Information Technology (IT) is used, research challenges are vital to emphasize. Cloud Computing is one modern technology in which the research community has recently boarded. This paper discusses some security and research issues for Cloud computing.

KEYWORDS - *Cloud Computing, Security, Research.*

1. INTRODUCTION

Cloud computing can broadly be considered as a novel computing approach that permits users to temporary utilize computing infrastructure over the Internet, delivered as a service by the Cloud-provider with one or more levels of abstraction. A leading IT analyst firm, Gartner Group [gartner.com], forecasts Cloud will transform business, like e-Business on Internet did around a decade ago. Accordingly, quite a few business models quickly evolved to tie together this technology by providing software applications, programming platforms, data-storage, computing infrastructure and hardware as services.

Cloud computing systems fall into one of five layers [15]: applications, software environments, software infrastructure, software kernel, and hardware. There are security and research issues related to each of this layer. The broad objective of this paper is to accomplish a better understanding of Cloud computing, elaborate security issues and emphasize some of the research topics that need to be addressed in Cloud systems.

The rest of the paper is organized as follows. Section II describes security implications followed by security assessments and countermeasures in section III. Section IV presents research challenges in Cloud computing from various perspectives followed by conclusion in Section V. Last section illustrates references used.

2. SECURITY IMPLICATIONS

Security implications of Cloud can be classified as per above layers. Let us take a close look at them on by one. (a) *Cloud Application Layer*: The users access the services provided by Cloud application layer (normally referred to as Software as a Service - SaaS) through web interface and pays fees to use them. It reduces the hardware requirements on user's end to get better performance for resource-intensive applications. Security and availability are two deployment issues obstructing its extensive implementation. Cloud providers need to deal with end-users' concern about security and safety of confidential data, authentication and authorization, up-time and performance, backup and disaster recovery and provide reliable service level agreements (SLAs) for their Cloud applications. (b) *Cloud Software Environment Layer*: Referred as Platform as a Service - PaaS, it is used by Cloud application developers. Issues here are: automatic scaling, load balancing, integration with other service involving authentication etc. (c) *Cloud Software Infrastructure Layer*: It provides resources to higher-level layers, which construct new Cloud software environments or Cloud applications. Services offered by this layer can be categorized into: computational resources, data storage and communications. Security of the services, their availability and quality are among the most commonly addressed concerns for them. Providing other security mechanisms for service oriented architectures is a rich area of research with little focus so far from the SOA and security communities. (d) *Software Kernel*: It provides the fundamental software management for the physical servers that make the Cloud. (e) *Hardware and firmware*: It forms the backbone of the Cloud.

1. SECURITY ASSESSMENTS AND COUNTERMEASURES

Before users move from desktop to Cloud, Cloud providers require to dealing with consumers' worry about confidentiality, authentication, authorization, availability, performance, backup, disaster recovery and SLAs. Security, availability and quality are among the most commonly addressed issues. Current security approaches make use of Public Key Infrastructure (PKI) and X.509 SSL certificates for authentication and authorization. Due to the lack of Cloud computing standards that address these issues, Cloud security, data privacy and ownership policies are handled differently by each Cloud provider.

According to Foundstone [16], security assessments can be addressed in many directions: (A) Architecture and design assessment (B) Cloud infrastructure security assessment (C) Governance, policies and procedures review. (A) Architecture and design assessment include Network topology, key assets, data storage and operation, input and output end points in system, trust boundaries, access controls, system and network isolation, administrative controls for Cloud vendor, administrative controls for business owner. (B) Cloud infrastructure security assessment include Internal and external penetration assessment, application or product penetration assessment, host security configuration assessment, Firewall security assessment, VPN/ remote access security assessment, physical security assessment, attack and penetration, information retrieval, pillage and cleanup. (C) Legal contract and SLA review, e-Discovery and information management, information / data lifecycle management, compliance and audit, business continuity and disaster recovery management, information integrity and confidentiality assurance, operation, administration and access management procedures, incident response management and forensics: are the various criterions from governance, policies and procedures perspective.

So keeping all this in mind, before adopting Cloud as a platform, consumer should be aware of the precautions, and be prepared accordingly. Gellman [2] presents some guidelines and tips for consumers, business and government, who plan to move to Cloud environment. (a) Understand Terms of Service and privacy policy carefully; also get you notified when there is any change in them. (b) Don’t put confidential data on the Cloud. (c) Recognize the Cloud provider rights about your information. (d) Read the privacy policy. (e) What about the access to data by Cloud provider after removing from the Cloud. (f) Make sure about any violating in law or policy. (g) Consult with your technical, security or corporate governance advisors.

2. RESEARCH IN CLOUD

Though there are many research directions in Cloud computing, some hot research topics seem to be of some degree of short-term significance to the Cloud provider/users, while some of their practical challenges appear to create new queries.

There are various classifications of Cloud research. Cloud security alliance [14] classifies Cloud research into three broad categories. (A) Cloud architecture (B) Governing in the Cloud and (C) Operating in the Cloud. The last two categories are further sub-classified as under. (B) Governing in the Cloud: (i) Governance and enterprise risk management (ii) Legal and electronic discovery

(iii) Compliance and audit (iv) Information lifecycle management (v) Portability and interoperability (C) Operating in the Cloud: (i) Traditional security, business continuity, and disaster recovery (ii) Data center operations (iii) Incident response, notification, and remediation (iv) Application security (v) Encryption and key management (vi) Identity and access management (vii) Virtualization.

Expert group [13] classifies the Cloud research into two broad categories: (A) Technological research: (i) Elastic scalability (ii) Cloud (systems) development and management (iii) Data management (iv) Programming models and resource control; (v) trust, security and privacy (B) Business Perspective: (i) Economical aspects; (ii) Legalistic issues; (iii) Green IT.

Now let us take look at some specific research issues and research going on in Cloud computing. As image is one of the core components of Cloud computing, image's meta-data management, image optimization, image loading time, image format standardization and image portability are interesting open issue. Other challenges include how to collect, design, store and present provenance information. [1]

As discussed in previous sections of this paper, another research and engineering challenge is security. Issue of security and trusted computing is hot spot of research in Cloud computing [1] [5] [8]. Security applications/services (e.g. antivirus) and identity management are also some motivating issues in Cloud computing. Building an efficient customer add-on controller outside of the Cloud utility service [3] that may include feedback control is an interesting subject of research. Another area is to study the challenges of optimization in Cloud computing and proposing a business driven Cloud optimization architecture [4] which may address the challenges to one extent.

There is a lot can be done in the way file systems are handled in Cloud environment. In the Hadoop Distributed File System (HDFS) [18] and the

Google File System (GFS) [17], a Namenode is required to keep a list of all files in the Cloud and their respective metadata (i-node). Besides it has to do almost all file related operations such as open, copy, move, delete, etc. This may not scale and can potentially make the Namenode a resource bottleneck. EDFS [6] uses a central front end server to distribute keys.

Google uses Chubby (a locking service) and Chubby uses State Machine Replication based on Paxos. Thus *Consensus*, an essential component of State Machine Replication, can be justifiable Cloud research area. Research on Consensus, new Consensus protocols and tools, alternatives to Consensus are sub-research agenda. [7]

One could also work on proposing better power management skills for Cloud i.e. exploring ways to do less during rush hours and migrating work in time to lightly loaded machines. What about the stability of a system having large-scale platforms, management technologies, hundreds or thousands of nodes, tens of data center?

Even thinking of entirely new operating systems or virtualization architectures - with support for massively scalable protocols, may not be unrealistic in near future. I-Cluster [9] enables automatic real-time analysis of the availability and workload of machines on an intranet, to take advantage of unused network resources. Defining architecture to assist the administration of compute resources from dissimilar Cloud providers in a homogenous manner [10] is also an interesting research issue. Abstraction and implementation issues in virtualization [11], datacenter virtualization without compromising server performance [12] are also some of the challenges.

Proposing different protocols and strategies for SLA negotiation [19], energy efficient resource allocation mechanisms and techniques for creation and management of Green Clouds [20], developing techniques and technologies for addressing scalability and energy efficiency are few of other research agenda.

Cloud systems monitoring is another active research topic in Cloud computing. With huge Cloud data centers and the large number of nodes, hardware and software failures are not unrealistic. We need to have a strong monitoring system which allows the Cloud services to vigorously react to failures. Tree-based systems or Gossip-based protocols are two common proposals for such monitoring and management. Spanning-tree approaches have been used in grid and distributed systems [21] [22] for such tasks.

Each Cloud computing service has a distinct interface and employs a different access protocol. A unified interface to provide integrated access to Cloud computing services is nonexistent, although portals and gateways can provide this unified web-based user interface. Designing interoperable systems between different Cloud offerings that provide higher-availability guarantees could be of great interest.

Even if we keep the core Cloud computing technological issues aside, there are business perspective research agenda which are yet to be explored in detail. They can be classified as under: (1) Cloud computing economics (expense can be analyzed in conjunction with capacity investment decisions and QoS guarantees) (2) Strategy issues in Cloud computing (intra-organizational issues, cultural change, employees' mind set for this changed scenario) (3) Cloud computing and IT strategy/policy issues (Data: privacy, security, ownership, consistent Business Policy, IT Audit Policy) (4) Technology adoption and implementation issues (Proposing the best application, moving in-house application to Cloud) (5) Cloud computing and green IT; and (6) Regulatory issues (Issues regarding government and International laws and regulations). (7) The problem of the return-on-investment (*ROI*) and the total-cost-of-ownership (*TCO*).

3. CONCLUSION

Cloud computing is a child of already available technologies such as virtualization, distributed computing, utility computing, and more recently networking, web and software services. It implies a service oriented architecture, reduced information technology overhead for the end-user, great flexibility, reduced total cost of ownership, on-demand services and many other things. There are security issues related to Cloud computing such as confidentiality, privacy and integrity. Therefore, it is noteworthy to make sure that proper security measures are in place. While these concerns may not be complete obstacles to adopting Cloud computing, undoubtedly they are major barriers. Cloud consumer should be prepared to present the consumer with detailed security and legal requirements applicable to their business needs and the nature of the information being stored or transacted. This paper discussed the security implications and research issues related to Cloud.

6. REFERENCES

1. M. Vouk, Cloud Computing – Issues, Research and Implementations, Proceeding of the ITI 200830th Int. Conf. on Information Technology Interfaces, June 2008.

2. R. Gellman, P.Dixon, Cloud Computing Privacy Tips, World Privacy Forum, www.worldprivacyforum.org, February 23, 2009.

3. H. Lim,S. Babu,J. Chase,S. Parekh, Automated Control in Cloud Computing: Challenges and Opportunities,ACDC'09, ACM, Barcelona, Spain, June 19, 2009.

4. M. Litoiu, M.Woodside, J.Wong, J.Ng, G.Iszlai, A Business Driven Cloud Optimization Architecture, ACM, SAC'10, Sierre, Switzerland, March 22-26, 2010.

5. R.Chow, P.Golle, M.Jakobsson, R.Masuoka, J.Molina, E.Shi, J.Staddon, Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control, CCSW'09, ACM, Chicago, Illinois, USA, November 13, 2009,

6. D.Fesehaye, R.Malik, K.Nahrstedt, EDFS : A Semi-centralized Efficient Distributed File System, Springer-Verlag, 2009.

7. K.Birman, G.Chockler, R.Renesse, Toward a Cloud Computing Research Agenda, ACM SIGACT News, vol. 40, no. 2, June 2009.

8. N.Santos, K.Gummadi, R.Rodrigues, Towards Trusted Cloud Computing, 2008.

9. B.Richard, N.Maillard b, C. Rose, R.Novaes, The I-Cluster Cloud: distributed management of idle resources for intense computing, Parallel Computing 31, 813–838, elsevier, www.sciencedirect.com, 2005.

10. R.Dodda, C.Smith,A.Moorsel, An Architecture for Cross-Cloud System Management, IC3 2009, CCIS 40, pp. 556–567, Springer-Verlag Berlin Heidelberg 2009.

11. S.Schocken, Virtual Machines: Abstraction and Implementation, ITiCSE'09, ACM, Paris, France, July 6–9, 2009.

12. F.Kamoun, Virtualizing the Datacenter Without Compromising Server Performance, ACM Ubiquity, Vol. 2009, Issue 9 August 17, 2009.

13. Expert Group, The Future of Cloud Computing, Opportunities for European Cloud Computing Beyond 2010, Expert Group Report, December 2009.

14. Cloud Security Alliance, Security Guidance for Critical Areas of Focus in Cloud Computing V2.1,December 2009.

15. L. Youseff, M. Butrico, D. Silva, Toward a Unified Ontology of Cloud Computing, ieeexplore.ieee.org, 2009.

16. Foundstone, Cloud Computing Security Assessment, Services datasheet, www.foundstone.com, 2008.

17. Ghemawat S, Gobioff H, Leung ST. The Google file system. In: Proc. of the 19th ACM Symp. on Operating Systems Principles. New York: ACM Press, 2003. 29-43.

18. Borthakur, D. The Hadoop Distributed File System: Architecture and Design. The Apache Software Foundation, 2007.

19. S. Venugopal, X. Chu, R. Buyya, A negotiation mechanism for advance resource reservation using the alternate offers protocol, in: Proc. 16th Int. Workshop on Quality of Service, IWQoS 2008, Twente, The Netherlands, June 2008.

20. R.Buyya, S.Pandey, C.Vecchiola, Cloudbus Toolkit for Market-Oriented Cloud Computing, CloudCom 2009, LNCS 5931, pp. 24–44,© Springer-Verlag Berlin Heidelberg 2009.

21. A. Deligiannakis, Y Kotidis, and N. Roussopoulos, "Hierarchical in-network data aggregation with quality guarantees," in In EDBT, 2004.

22. R. Wolski, N. T. Spring, and J. Hayes, "The network weather service: a distributed resource performance forecasting service for metacomputing," Future Generation Computer Systems, vol. 15, no. 5-6, pp. 757-768, 1999.