IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 1, Issue 1, March, 2013
ISSN: 2320 - 8791
www.ijreat.org

Research Challenges in Cloud Computing

Sudhir Shenai[1],M.Aramudhan[2],B.Monisha[3]&K.Suganya[4]

[1]Ph.D Scholar, Dept of Computer Science & Engineering, SathyabamaUniversity,Chennai.

[2]Associate Professor,Dept of Information Technology, PKIET,Chennai.

[3,4] Dept of Information Technology,EGSPEC, Nagapattinam.

Abstract

Cloud Computing defines a new paradigm of on- demand resource provisioning over the Internet.Based on the type of resources being serviced, the Cloud is broadly classified into three service models IaaS, PaaSandSaaS. The Cloud wave is believed to change the conventional business models on the Internet. Along with the opportunities of the Cloud come the threats and apprehensions. The Cloud needs to overcome many a challenge for its wide spread adoption by both the Cloud provider and consumer communities. This paper is an exploration of the challenges plaguing cloud computing.

Keywords: Cloud Computing, IaaS, PaaS, SaaS

I INTRODUCTION

Cloud Computing is one of the hottest buzzwords in technologytoday. The birth of the term traces back to 2006, when large companies such as Google and Amazon began using "cloud computing" to describe the new paradigm in which people are increasingly accessing software, computing infrastructures, and storage space over the web instead of on their desktops [26].There are many views of"what is Cloud Computing?" Over20 definitions can be found in http://cloudcomputing.sys-con.com/read/612375_p.htm.The Cloud Computing can be defined from various perspectives like consumer perspective, service provider perspective and business perspective etc…The definition by NIST covers a comprehensive view of all the perspectives. Hence we state here NIST's definition for Cloud Computing.

"*Cloud Computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources(e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."*

The Cloud services possess variety of distinct characteristics like shared virtual infrastructure, network access, dynamic provisioning, scalability, flexibility and managed metering which distinguishes it from other common services on the Internet. Every cloud service is majorly supported by virtual infrastructure as the back bone. The infrastructurescan be compute, storage, platform or application. Theseresources are provisioned dynamically through cloud services on-demand basis. The on-demand requests can scale up or scale down the resources, thus adding flexibility to the cloud service. Most of the cloud services are metered as the user is charged for their usage.

Based on the type ofresources serviced, the cloud services can be primarily grouped into three service models.

1. Software as a Service (SaaS),Consumers purchase the ability to access and use an application or service that is hosted in the cloud. A benchmark example of this is Salesforce.com. The necessary information for the interaction between the consumer and the service is hosted as part of the service in the cloud.
2. Platform as a Service (PaaS) provides consumers a platform to develop and deploy applications. It allows clients to assume more responsibilities for managing the configuration and security for the middleware, database software, and application runtime environments.Ex: Google Apps
3. Infrastructure as a Service (IaaS) model provisions computing power, networking, and storage as virtual images to the consumers on-demand basis.TheIaaS majorly depends on virtualization to share physical infrastructure multiple users. It owns the responsibility of isolation between the users sharing same physical infrastructure. Ex: Amazon EC2.

The introduction chapter is a glimpse on cloud computing and its service models.The remainder of the paper is structured as follows: Section 2 gives an overview of

thesurveys on Cloud, which express the global interest in Cloud Adoption, its barriers and apprehensions. Section 3 analyses the various security issues prevalent in Cloud. Section 4 discusses the business related challenges in Cloud adoption. Section 5 explores the technical challenges intrinsic to the Cloud.

II OVERVIEW OFCLOUD SURVEYS

As per the 2012 Cloud Computing Security Survey [24] [25] by Information Security Media Group, nearly 1 in 3 survey respondents say their organizations are not using the cloud, a strikingly high percentage considering how quickly the computing platform is maturing. By a 72 percent-to-28 percent margin, the survey respondents say concerns aboutthesecurity prevents their organizations from moving into Cloud. The greatest reservations about secure Cloud Computing as per the survey are shown in the chart below.

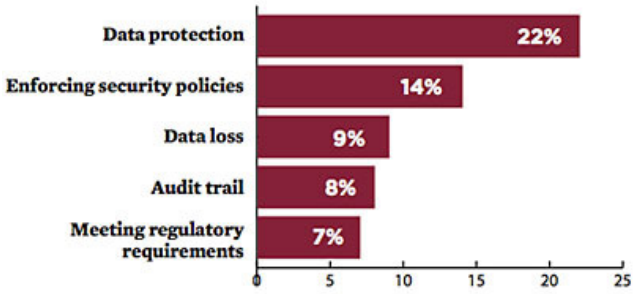

Fig.1 Survey Results on Cloud Security by iSMG-2012

Globally, 47% of the respondents who are currently using a cloud computing service reported they have experienced a data security lapse or issue with the cloud service their company is using within the last 12 months. India had the highest incidence (67%), followed by Brazil (55%).

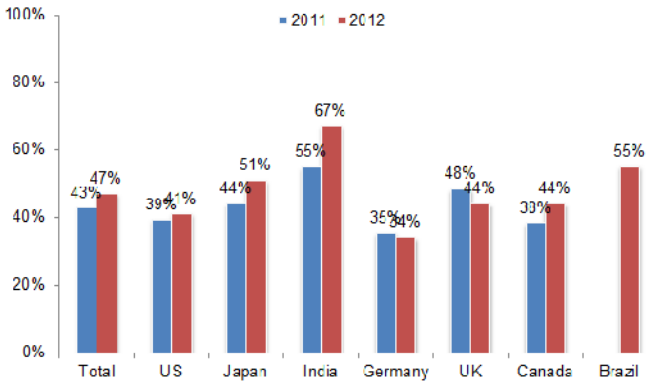

Fig.2 Incidence of Data Security Lapse or issue with cloud service (%) Survey by Trend Micro Inc.-2012

The above surveysgive a clear indication of importance of various challengesto be addressed for wide spread adoption of cloud services.

The challenges faced by Cloud are inherent to the characteristics associated with the Cloud.The Cloud is not an isolated concept [27] but has overlap with other domains like Grid, Virtualization, Web Services, and SOA etc. Also, the Cloud characteristics are influenced by these related domains.There are multiple characteristics associated with Cloud partially due to the relationship andapplicability in other domains, partially due to the background and intentions of theproviders and finally partially due to the actual Cloud specific features inherent to Cloud itself [27]. The perspective of Cloud from the viewpoints of various stake holders of the Cloud like consumer, Cloud service provider, Cloud Developer varies widely. Hence the characteristics requirements of the Cloud from various viewpoints also vary. The Table I give the classification of the Cloud characteristics from various viewpoints.

TABLE I CLASSIFICATION OF CLOUD CHARACTERISTICS

Technical	Business/Economic	Social/Legal
Elasticity/ Scalability	Outsourcing	Security
Virtualization	Pay per use	Provenance
Agility & Adaptability	Resource Utilization	Privacy
Availability	Energy Efficiency	
Multi Tenancy	Cost Efficiency	
Data Management	Metering	
Reliability		
Programmability		

The above classification of Cloud characteristics based on Technical, Business/Economic, and Social/Legal perspective is essential to categorize various challenges faced by Cloud. Thus the challenges are categorized as per the above classification of characteristics and explained in the following sections.

III SECURITY CHALLENGES

The cloud security issues can be broadly classified as Generic and Cloud Specific based on the relevance of the issues to the cloud characteristics. The Generic security issues are already prevailing security issues in general computing and networking environments which is applicable to cloud as well. It is pertinent to extrinsic characteristics of Cloud, which are inherited or extended

characteristics from other related domains to which the Cloud is associated with. The Cloud Specific Security (CSS) issues are inherent to cloud and not prevalent in other environments.It is pertinent to intrinsic characteristics of Cloud. A security issue can be deemed as Cloud Specific [4] if it

- is intrinsic to or prevalent in a core cloud computing technology
- has its roots in one of NIST's essential cloud characteristics
- is caused when cloud innovations make tried-and tested security controls difficult or impossible to implement or
- is prevalent in established state-of-the-art cloud offerings.

Some of the Cloud specific security issues are isolation failure, data interception, malicious insider, insecure or incomplete data deletion, lack of security perimeter, larger attack surface, and management interface compromise. An elaborate discussion of various security challenges related to cloud computing can be seen in the papers [4][5][6][7].The security threats can also be classified based on the security requirements at various levels of services provided by the cloud [8]. Basically the cloud services are provided at Application Level, Platform Level and Infrastructure Level. The services provided at various levels differ from each other by virtue, hence the security requirements too. Table II gives the summary of the classification of threats and security requirements at all the three levels of cloud services by Cloud Security Alliance (CSA)[9].

TABLE II SUMMARY OF SECURITY REQUIREMENTS AND THREATS CLASSIFICATION

Level	User	Requirements	Threats
Application Level (SaaS)	Person or Organization subscribed to a cloud Provider	• Service Availability • Communication Protection • Access Control • Privacy • Data protection	• Privacy Breach • Traffic Flow Analysis • Session Hijacking • Exposure in network • Impersonation
Virtual Level (PaaS,IaaS)	Person or Organization that deploy software on the cloud infrastructure	• Virtual Cloud protection • Secure images • Cloud Management Security • Application Security	• Connection Flooding • Programming flaws • Software modification • Software Modification • Software interruption • DDoS
Physical Level	Person or Organization owns the infrastructure	• Hardware Security • Hardware reliability • Network protection • Network resource Protection	• Network Attacks • Hardware theft • Natural Disasters • Hardware Modification • DDoS

IV BUSINESS CHALLENGES

The Cloud comes with both boon and bane. It has abundance of promising opportunities as well as risk and management complexity. For a wide spread Cloud adoption, the cloud provider should meet various business requirements like QoS, SLA, licensing, auditing policies etc…This section briefs the various business related challenges plaguing cloud.

A. Managing the contractual relationship[31]Cloud computing contracts are a mix of outsourcing, software and leasing. Some observers have argued that contracting for cloud is simpler than traditional approaches to IT sourcing because only one contract is required instead of multiple agreements for software, hardware and systems integration. In reality, however, few software, platform or infrastructure providers meet all of a client's functional requirements, so contracting for cloud services typically involves ecosystems of providers that must be integrated to provide complete solutions.

B. Dealing with lock-in[30]Exit strategies and lock-in risks are key concerns for companies looking to exploit cloud computing. There is always a switching cost for any company receiving external services. However, cloud providers have a significant additional incentive to attempt to exploit lock-in. If computing were to become a very liquid commodity, and if switching to a lower-cost provider were too easy, margins would rapidly become razor thin

*C. Overcoming cultural barriers*Culturalbarriersmay act as an obstacle in implementing cloud solutions. The geography is divided by cultures, ethnics, and varieties of

administrations. The business model in one region may not suit other region. Since the Cloud transcends geographical

boundaries, the Cloud cannot maintain unified solution approach for the same business belonging to different cultural backgrounds. Some organizations may be more sensitive to disclosure of private information, than the others.Example: For Department of Defense, public leaks of sensitive information may put the agency on a more risk-averse footing, which makes it more reluctant to migrate to a cloud solution [28].

D. Meeting federal security requirements[29]Cloudvendors may not be familiar with security requirements that are unique to government agencies, such as continuous monitoring and maintaining an inventory of systems. For example, State Department officials described their ability to monitor their systems in real time, which they said cloud service providers were unable to match. U.S. Treasury officials also explained that the Federal Information Security Management Act's requirement of maintaining a physical inventory is challenging in a cloud environment because the agency does not have insight into the provider's infrastructure and assets.

E. Certifying and accrediting vendors[29]Agencies may not have a mechanism for certifying that vendors meet standards for security, in part because the Federal Risk and Authorization Management Program had not yet reached initial operational capabilities. This is partly due to the lack of standards for the cloud services whose characteristics vary widely by virtue of its application.

F. *Procuring services on a consumption(on-demand) basis)*[28]Because of the on-demand, scalable nature of cloud services, it can be difficult to define specific quantities and costs upfront. These uncertainties make contracting and budgeting difficult because of the fluctuating costs associated with scalable and incremental cloud service procurements. It is difficult to budget for a service that could consume several months of budget in a few days of heavy use.

G. *Loss of governance*[30]By using cloud services theclientpasses control to the provider. This passing off, of control to the provider, results in loss of control over a number of issues which in turn may affect the security posture of the client data and applications. This is aggravated by the fact that SLAs may not tender commitment on the part of the provider, and thus widening the security cover gap.

H. Legal and compliance issues[30]With data &application hosted by a third party, the cloud service provider; issues of ascertaining the legal and compliance impact to participating parts is difficult. Issues relatedto data protection, privacy, jurisdiction of storage and processing and e-discovery raise. It also raises the issue related to the responsibility of the aforementioned issues

V TECHNICAL CHALLENGES

The characteristics of Cloud intrinsic to the core technology and the related domains enabling the Cloud introduce many challenges. Those challenges are categorized as technical challenges.A brief discussion of those challenges is given in this section.

*A. Scalability*One of the important properties of the Cloud is dynamic scalability, i.e. the resources provisioned by the Cloud will be scaled up or down based on user's demand. Thus this elasticity feature of Cloud introduces lots of challenges. From the user perspective, the Cloud contains infinite resources. But from the Cloud provider perspective, managing the ever depleting resources due to ever growing demand is a challenge. The provider should meet the performance as per SLA at the same time should optimize the resource provision to reduce both the OPEX and CAPEX. This dynamic scalability/elasticity if not controlled effectively, leave open larger attack surface, thereby increasing difficulty in enforcing perimeter (boundary level) security like firewall.

*B. Multi-Tenancy Issues*The multi-tenancy isanimportantfeatureof Cloud Computing, which allows more than one virtual host(tenants)to be resident on the same physical machine. In general, the placement of virtual host on the physical machine is not under the control of Cloud consumer, it is effectively automated by the Cloud provider leaving the mechanism opaque. Since environment is open, virtual host of different companies can reside on the same machine leaving scope for attacks like side channel attacks. Isolation of tenants depends on whatis shared and to what degree; it is currently difficult to distinguish whichpart of the resource consumption is caused by which user [27]. This however is necessary for accurateusage / cost assessment per individual user.

C. Lock in[27]Applications developed for one Cloud often enough have to be redeveloped for other Cloud providers, if the execution environment is supposed to be

shifted. Dueto this switching cost, the average user is quickly locked-in into the environment thathe started to host his services on. Thus there is a high necessity of inter-operability between the Cloud providers to overcome this lock-in problem. This can be achieved if the Cloud adherestocommon agreed upon standards by various Cloud providers. Due to lacking generality in the approaches to realize Cloud, there is implicitlya strong divergence between the Cloud offerings and thus the interfaces theyexpose and the way they are programmed / controlled.These pose a big challenge for standardization efforts. Some ongoing standardization efforts are listed below. Open Virtualization Formatfor virtual images, the efforts by OpenStack to agree on standard interfaces

*D. Moving to the Cloud*Beforemoving the existing application into cloud many things need to be considered. First the application should be cloud ready; the amount of rework involved in making the application suitable for cloud is an important factor which decides whether the rework is sufficient or complete new development from the scrap is needed. Most of the Cloud applications are not programmed to exploit the full potential of Cloud. The current Cloud APIs and programming models don't address this issue in Toto. Also, switching cost arises from the portability /interoperability restrictions ofthe different CLOUD environments.

E. Data Challenges: Streaming, Multimedia, Big Data

The Cloud is crowded, it witness ever increasing user base. Naturally, the Cloud has to manage large amount of data with varyingdegree of different data types like voice, video chat, livevirtualization etc. The management of these big data seeks support from storage medium and communication medium. Managing the ever growing volume of data needs storage hardware support and storage virtualization support.Thechallenge is managing data in both active and rest state without data leakage and guaranteeing data security for the Cloud users.Also, the communication demand grows faster than expected.The demand for communication bandwidth always supersedes the technological support enabling communication. With the latency inherent to the internet and the dynamicity inherent to the Cloud, meeting the real-time requirements of both interactive andstreaming applications with a promised QoS is a highly complex task. The real challenge ahead is in developing a future Cloud ecosystem which can manage heterogeneity of resources, ever increasing user base and mobility of the devices.

F. Performance[27]Due to the high amount of availability resources, Clouds are often compared toinfinite high performance computing systems, i.e. it is assumed that they offer infinite highperformance. The effective performance however depends highly on the degree ofscalability, the utilization of resources and the communication strength.Accordingly, it depends on how the software was written, how the infrastructure isset up and how it is maintained. The necessity of high through put performance increases as the demand for ever increasing power (computational power) hungry applications increases. In the traditional computing environment the number of processing core is increased to manage the performance issues.Future CLOUD systems must be able to support a wide range ofdifferent devices and use cases and therefore be able to understandthe various strengths and capabilities and relate them to the actual requirements.

VI CONCLUSION

Cloud computingis a paradigm shift in the model of services provided over the Internet which comes with both boon and bane.The cloud services range in varieties such asApplication,PlatformandInfrastructure; it adds complexity and hinders unified solution approach for all the problems faced by cloud. Also the cloud's innovative services coupled with shared infrastructure introduce new challenges to the wide adoption of cloud by various user communities.Thechallenges faced by cloud are multitudewhichranges from business to technical. This paper explored the variouschallengesfaced by cloud computing and its research directions.

REFERENCES

[1] Alexander Lenk, Markus Klems, Jens Nimis, Stefan Tai , Thomas Sandholm,"What's Inside the Cloud? An Architectural Map of the Cloud" In:International Conference on Software Engineering,Proceedings of the 2009 ICSE Workshop on Software Engineering Challenges of Cloud Computing,2009.p.23–31,ISBN:978-1-4244-3713-9.

[2] A Taxonomy and Survey of Cloud Computing System", Fifth International Joint Conference on INC, IMS and IDC

[3] Bernd Grobauer, Tobias Walloschek, and ElmarStöcker "Understanding Cloud Computing Vulnerabilities" Cloud Computing, Copublished by The IEEE Computer And Reliability Societies

[4] KrešimirPopović, ŽeljkoHocenski "Cloud computing security issues and challenges", MIPRO 2010, May 24-28, 2010, Opatija, Croatia

[5] Paul Wooley ,Tyco Electronics ,"Identifying Cloud Computing Security Risks"

[6] V VenkateswaraRao , G. Suresh Kumar, Azam Khan, S SanthiPriya,"Threats and Remedies in Cloud

[7] A Survey on Cloud Computing Security,Challenges and Threats", Journal of Current Computer Science and Technology Vol. 1 Issue 4[2011]101-106

[8] DimitriosZissis, DimitriosLekkas,"Addressing cloud computing
security issues", Future Generation Computer Systems.
[9] "Critical Areas of Focus in Cloud Computing", Cloud Security Alliance,December 2009.
[10] KetkiArora ,Krishan Kumar, And Monika Sachdeva ," Impact analysis of DDOS Attack", International Journal on Computer Science and Engineering (IJCSE)- Vol. 3 No. 2 Feb 2011
[11] Metz C, "DDoS attack rains down on Amazon Cloud", http://www.theregister.co.uk/2009/10/05/amazon_bitbucket_outage.
[12] IrfanGul, M. Hussain "Distributed Cloud Intrusion Detection Model" International Journal of Advanced Science and Technology Vol. 34, September, 2011
[13] Shantanu Pal, SunirmalKhatua, NabenduChaki, SugataSanyal ,"A New Trusted and Collaborative Agent Based Approach for Ensuring Cloud Security Implementing Trust in Cloud Infrastructures",
[14] Qi Chen, Wenmin Lin, Wanchun Dou , Shui Yu "CBF A Packet Filtering Method for DDoS Attack Defense in Cloud Environment"
[15] Siqin Zhao, Kang Chen, WeiminZheng ,"Defend Against Denial of Service Attack with VMM" , Eighth International Conference on Grid and Cooperative Computing
[16] Mohammed H. Sqalli Fahd Al-HaidariKhaled Salah,"EDoS-Shield - A Two-Steps Mitigation Technique against EDoS Attacks in Cloud Computing ",Fourth IEEE International Conference on Utility and Cloud Computing
[17] Ashley Chonka,Yang Xiang n, Wanlei Zhou, AlessioBonti, "Cloud security defence to protect cloud computing against HTTP-DoS and XML-DoS attacks", Journal of Network and Computer Applications 34 (2011) 1097–1107
[18] Soon HinKhor Akihiro Nakao, "sPow On-Demand Cloud-based eDDoS Mitigation Mechanism"
[19] Mehmet Yildiz, JemalAbawajy, TuncayErcan and Andrew Bernoth,"A Layered Security Approach for Cloud Computing Infrastructure", 10th International Symposium on Pervasive Systems, Algorithms, and Networks.
[20] Thomas Ristenpart, EranTromer, HovavShacham, Stefan Savage,"Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds",
[21] KaziZunnurhain, Susan V. Vrbsky,"Security in cloud computing",
[22] Meiko Jensen, J¨orgSchwenk , Nils Gruschka, Luigi Lo Iacono ,"On Technical Security Issues in Cloud Computing", IEEE International Conference on Cloud Computing
[23] Nils Gruschka and Luigi Lo Iacono,"Vulnerable Cloud: SOAP Message Security Validation Revisited", IEEE International Conference on Web Services
[24]http://www.bankinfosecurity.com/p-survey-cloud-security-2012
[25] "Overcoming the Apprehension of Cloud Computing: Results from the 2012 Cloud Computing Security Survey ", Information Security Media Group, 2012.
[26] http://www.technologyreview.com/news/425970/who-coined-cloud-computing/
[27] Lutz Shubert, Keith Jeffery, "Advances in CLOUDS, Research in Future Cloud Computing", *Expert Group Report, Public version 1.0,* Information Society and Media, European Union, 2012
[28]http://gcn.com/Articles/2012/09/11/AGG-GAO-7-major-cloud-problems.aspx?Page=2
[29]http://gcn.com/articles/2012/09/11/agg-gao-7-major-cloud-problems.aspx
[30] Faith Shimba, "Cloud Computing:Strategies for Cloud Computing Adoption",*Dublin Institute of Technology*, 2010-09-01
[31]http://www.accenture.com/us-en/outlook/Pages/outlook-online-2011-challenges-cloud-computing.aspx