International Journal of Trend in Scientific Research and Development (IJTSRD)
International Open Access Journal
ISSN No: 2456 - 6470 | www.ijtsrd.com | Volume - 2 | Issue – 5

Survey on Security in Cloud Hosted Service & Self Hosted Services

Surbhi Khare[1], Dr. Uday Kumar[2]
[1]Ph.D Scholar of CSE Department
[2]Director, School of Engineering & IT
MATS University, Aarang, Raipur, Chhattisgarh, India

ABSTRACT

As more and more organizations consider moving their applications and data from dedicated hosting infrastructure, which they own and operate, to shared infrastructure leased from `the cloud', security remains a key sticking point. Tenants of cloud hosting providers have substantially less control over the construction, operation, and auditing of infrastructure they lease than infrastructure they own. Because cloud-hosted infrastructure is shared, attackers can exploit the proximity that comes from becoming a tenant of the same cloud hosting provider. As a result, some have argued that that cloud-hosted infrastructure is inherently less secure than the self-hosted infrastructure, and that it will never be appropriate for high-stakes applications such as health care or financial transaction processing.

We strive to present a more balanced treatment of the potential security impacts of transitioning to cloud-hosted infrastructure, surveying both the security costs and security benefits of doing so. The costs include exposure to new threats, some of which are technological, but many others of which are contractual, jurisdictional, and organizational. We also survey potential countermeasures to address these threats, which are also as likely to be contractual or procedural as technological. Transitioning to a cloud-hosted infrastructure may also have security benefits; some security measures have high up-front costs, may become affordable when amortized at cloud scale, and impact threats common to both cloud- and self-hosted infrastructures.

Keywords: *cloud services,cloud computing, networking.*

I. INTRODUCTION

Behind the buildup encompassing `cloud processing', and contending meanings of the term, are convincing financial powers driving changes in the framework used to have associations' applications and information. Rather than owning and working framework themselves, associations may now rent shared assets from `clouds', adequately getting to be foundation occupants as opposed to proprietors. The asset flexibility offered by cloud suppliers takes out the in advance expenses of building a self-facilitated framework and expels delays by enabling occupants to scale up their assets on request. Cloud-facilitating additionally offers cost reserve funds accomplished through economies of scale: cloud suppliers get mass costs for parts, can better use specific staff, and utilize bring down total extra limit through sharing, and amortize of the in advance expenses of building and regulating server farms over a huge number.

Hindering the potential investment funds achievable through cloud-facilitating are worries about security. In April 2009, Cisco CEO John Chambers called the security ramifications of cloud facilitating, a bad dream", clarifying that, you'll have no clue what's in the corporate server farm". Ron Rivest recommended that the expression, overwhelm registering" may better speak to the right attitude in which to look at the security ramifications of moving to the cloud. Among Bruce Schneier's much distributed computing concerns was that basic information could wind up on some cloud that suddenly vanishes in light of the fact that its proprietor goes bankrupt". Others expect that as contending suppliers hurry to snatch early piece of the pie, which is particularly profitable given the high exchanging expenses and vast scale economies of the

cloud facilitating business, they will be enticed to embrace a ship-first secure-later technique.

The majority of these security concerns encompassing cloud facilitating is not new, but rather is as of now endemic to existing facilitating offerings, for example, those that offer records on shared servers or virtual private servers that keep running on shared equipment. Different dangers, for example, the hazard that an assault on one occupant will affect another, are now endemic to content appropriation systems. What separates cloud-facilitating suppliers from customary facilitating suppliers is their capacity to offer versatile assets, available in little time units of time and offered at costs made conceivable through economies of scale. Though virtual private servers target clients trying to set up a fundamental web nearness or essential email benefit, cloud-facilitating target applications and information would have already required devoted server farms. Forthcoming inhabitants of cloud-facilitating suppliers along these lines frequently have considerably higher security necessities than those of customary web facilitating suppliers.

Regardless of various worries about the security of cloud-facilitated foundation that are both true blue and huge, it is out of line to expect that cloud-facilitated framework is intrinsically less secure than self-facilitated foundation. The individuals who contend cloud facilitating is inalienably less protected unavoidably contrast it with a security perfect in which associations that work and possess their own particular foundation have boundless assets to secure it legitimately. Actually, securing a facilitating framework is costly and loaded with costs that must be consumed paying little respect to scale. An adjusted treatment must perceive not just new dangers acquainted by moving with cloud facilitating yet additionally the economies of scale in tending to existing dangers endemic to both cloud-and self-facilitating. Working at cloud scale opens the outline space for safety efforts to incorporate arrangements not beforehand attainable: those with in advance costs that are restrictively costly beneath cloud scales, yet that accomplish net investment funds over contending arrangements by decreasing the negligible per-occupant and per-machine costs.

Commitments and degree

We endeavor to review the long haul security ramifications of cloud facilitating autonomous of the imperatives of the present usage.

Our first commitment is to study and inventory the new dangers that are presented when applications and information are moved to rented/shared (cloud-facilitated) framework from possessed/devoted (self-facilitated) foundation. A significant number of these dangers relate less to innovation than to issues of HR, motivation arrangement, and locale. While a considerable lot of these dangers have been raised somewhere else, we amass them together in an available way. We likewise investigate existing mechanical, hierarchical, and lawful roads to address distributed computing dangers.

At long last, we recognize safety efforts that may profit by the economies of cloud scale, conceivably empowering occupants of cloud facilitating suppliers to get more security for their dollar than could be accomplished by facilitating their own particular framework.

We have deliberately confined the extent of this overview to cloud facilitating of occupants' applications and information, and not cloud applications in which the facilitating and application framework are assembled totally by an outsider (e.g. Google's Docs, Office Live, Drop Box, Flickr). While cloud facilitating and cloud applications are frequently treated close by each other in talks of `cloud figuring' patterns and security dangers, the administrations and their security suggestions are very unique.

We have additionally purposefully picked not to manufacture scientific recipes or models for the choice to move to cloud facilitating. This decision is taken a toll/advantage choice, and keeping in mind that we try to give knowledge by specifying and looking at these expenses and advantages, once these components are measured the bookkeeping it is direct. We accept there is minimal further to be picked up (and a lot of clearness and sweeping statement to be lost) from the presentation of numerical choice models and the disentangling presumptions required to settle on general claims about these choices.

While we specify various dangers, countermeasures, and wellsprings of economies of scale in cloud-foundation security, exclusions are certain to be found in every one of these sets. This is a working archive, and one that we hope to change both in light of input from the workshop, the acknowledgment of unanticipated dangers, and the advancement of new security plans.

II. Literature Review

1. The idea of providing computing as a utility is far from new, as are security issues with shared computing infrastructure, but recent developments have catalyzed explosive interest and growth of what we now call `cloud computing'. Karger and Schell discuss lessons learned from the security evaluation of Multics, which was one of the first systems to tackle the problems of secure shared computing. Ambrust et al. discuss the reasons for the cloud computing's recent popularity growth and outline key features that make it different from prior shared computing systems, such as the ability to scale down to small pilot projects or up to large projects.

Many others have discussed threats arising from cloud computing. Talbot's article in MIT's Technology Review provides a high-level examination of cloud security issues, covering both cloud applications (e.g. Facebook and Gmail) and cloud-hosting. Schneier observes many potential threats of cloud hosting and notes similarities between cloud hosting and traditional timesharing computing, while Balding and Hoff each discuss problems with compliance in today's cloud hosting regimes. The Cloud Security Alliance enumerates technological threats to cloud providers and tenants. Varia describes best practices such as frequent patching for virtual machines as part of a white paper on architecting for cloud computing.

Many of the threats we have enumerated have origins in real events. Amazon S3 suffered data corruption due to a flaky border gateway router. The experience highlighted the difficulty today's cloud customers have in verifying the integrity of cloud infrastructure and isolating the source of failures. Under provisioning is already a concern of some cloud tenants and third-party monitors.

2. Amazon, Microsoft, and other cloud providers rely heavily on hypervisor-based virtual machines to isolate tenants, thus making their security a key area of concern. While virtual-machine level isolation provided by hypervisors is easier to reason about than most OS-level isolation, it is not immune to security flaws. The Cloudburst exploit found by Kortchinsky demonstrated how a specially crafted guest video driver could take control of a host machine running VMW are Workstation or ESX Server. The flaw exploited by Cloudburst was failures by VMW are too properly bounds check certain calls from the guest video card driver to VMW are emulated 3D hardware. Ormandy found that simple random fuzzing of common virtualization software, including QEMU and VMW are uncovered potentially exploitable bugs. Like the Cloudburst exploit, several of these bugs were also located in hardware emulation code. Garfinkel and Rosenblum discuss further issues with security in virtualized environments, such as the challenge of patching virtual machine images or the potential for re-use of randomness in cryptographic operations.

The drive towards features has pushed commodity virtual machine monitors to include more code, which increases the risk that a serious bug will appear. Recent academic work has pushed back against this trend by focusing on smaller, easier to verify hypervisors. For example, Flicker and Trust visor reduce the size of their hypervisors by exploiting new CPU features designed to make writing hypervisors easier.

The timing attacks that may impact tenant-shared CPUs in the cloud have their roots in cryptosystems. Kocher demonstrated timing attacks on smart cards and later Boneh and Brumley showed that timing attacks could be carried out over the network. Tromer et al. showed that cache effects could lead to timing attacks even on symmetric encryption schemes such as AES [47], which could potentially be used to attack a tenant sharing a CPU. Bortz and Boneh show how timing attacks can reveal information about web applications as well.

3. Ristenpart et al. demonstrate side channel attacks on the Amazon Elastic Compute Cloud and Xen hypervisor that allow them to determine whether their tenant VM is co-located with a VM belonging to a target web service and, if so, to learn keystroke timing information.

In the area of audit, the Cloud Audit working group is currently drafting a specification for an API focused on audit, assertion, assessment, and assurance" for

cloud providers. The goal of the API is to generate machine readable assertions that detail which security features and certifications a provider does and does not have. Prospective tenants can then programmatically decide whether to purchase resources from a provider for their application given their security needs.

4. Kelsey and Schnier introduce the concept of secure audit logs, a possible mechanism for implemented the audit countermeasures. Iliev and Smith propose logs that utilize a security coprocessor, such as the IBM 4758, to achieve tamper evidence. Their work followed on the Packet Vault project, which aimed at capturing and recording every packet over a 10 MBps link indefinitely on commodity disk storage.

For new security features that could be deployed to cloud tenants, Cui's work shows how to detect malware from scanning memory images, and more generally how to identify specific objects in a memory dump [10]. Cloud providers could use this functionality as part of a cloud infrastructure to audit tenant execution with modest overhead. Garfinkel et al. describe architecture for embedding intrusion detection directly inside a hypervisor.

5. Gordon et al. model the optimal amount of information sharing between different entities. Their analysis reveals a free rider problem that leads to systematic under investment in security when each firm is free to choose its level of sharing. A cloud provider can avoid this free riding problem by bundling a given level of information sharing with the cloud service.

III. HOSTED SERVICES

Facilitated administrations are, in the most non specific sense, benefits that are given over the Internet. In the facilitated benefit condition, one PC is arranged to give a few or the majority of its assets for client utilization in return for a predetermined charge. The Internet is utilized to associate the server to a customer machine(s), which get to server information, substance and administrations.

All facilitated benefit composes encompass the fundamental idea of a site or web benefit, however they might be generally separated, as takes after:

- Web facilitating provides ceaseless, continuous Internet get to; an extraordinary accumulation of programming projects or administrations (like FTP and email); and a domain for working with different programming dialects (like PHP, .NET and Java).
- File facilitating: Hosts record storerooms, as opposed to Web applications or locales. A protected document facilitating administration is perfect for putting away records, decreasing or killing information robbery, misfortune or debasement.
- Image facilitating: The host server stores picture documents or other level records, which allows simple and versatile sharing, regularly as a substance conveyance organize (CDN) that streamlines conveyance.
- Email facilitating: Either through an outsourced server, for example, Microsoft Exchange or by means of a locally electronic email benefit like Gmail.

In light of the accessibility of server assets and client consents, and also number of records facilitated by a server, facilitating might be sorted as takes after:

- Shared Web facilitating: One of the most prominent types of Web facilitating, this is "shared" in light of the fact that few distinctive Web applications are put away on a solitary physical server, in this way sharing accessible assets.
- Semi-devoted facilitating: The server is arranged to have less site assets with more extraordinary data transfer capacity.
- Dedicated facilitating: Client applications don't impart server assets to the utilizations of different clients. Besides, the server utilizes accessible transfer speed for its own particular execution.
- Virtual server facilitating: Here, a physical server is part into different individual, virtual servers. An alternate OS is set up, per client necessities.

IV. CLOUD HOSTED SERVICES

Corporate and government entities utilize cloud computing services to address a variety of application and infrastructure needs such as CRM, database, compute, and data storage. Unlike a traditional IT environment, where software and hardware are funded up front by department and implemented over a period of months, cloud computing services deliver IT resources in minutes to hours and align costs to actual usage. As a result, organizations have greater agility and can manage expenses more efficiently.

Similarly, consumers utilize cloud computing services to simplify application utilization, store, share, and protect content, and enable access from any web-connected device.

How cloud computing services work

Cloud computing services have several common attributes:

- **Virtualization**- cloud computing utilizes server and storage virtualization extensively to allocate/reallocate resources rapidly
- **Multi-tenancy** -resources are pooled and shared among multiple users to gain economies of scale
- **Network-access** - resources are accessed via web-browser or thin client using a variety of networked devices (computer, tablet, smart phone)
- **On demand** - resources are self-provisioned from an online catalogue of pre-defined configurations
- **Elastic** -resources can scale up or down, automatically
- **Metering/chargeback** -resource usage is tracked and billed based on service arrangement

Among the many types of cloud computing services delivered internally or by third party service providers, the most common are:

- **Software as a Service (SaaS)** – software runs on computers owned and managed by the SaaS provider, versus installed and managed on user computers. The software is accessed over the public Internet and generally offered on a monthly or yearly subscription.
- **Infrastructure as a Service (IaaS)** – compute, storage, networking, and other elements (security, tools) are provided by the IaaS provider via public Internet, VPN, or dedicated network connection. Users own and manage operating systems, applications, and information running on the infrastructure and pay by usage.
- **Platform as a Service (PaaS)** – All software and hardware required to build and operate cloud-based applications are provided by the PaaS provider via public Internet, VPN, or dedicated network connection. Users pay by use of the platform and control how applications are utilized throughout their lifecycle.

Benefits of cloud computing services

Cloud computing services offer numerous benefits to include:

- Faster implementation and time to value
- Anywhere access to applications and content
- Rapid scalability to meet demand
- Higher utilization of infrastructure investments
- Lower infrastructure, energy, and facility costs
- Greater IT staff productivity and across organization
- Enhanced security and protection of information assets

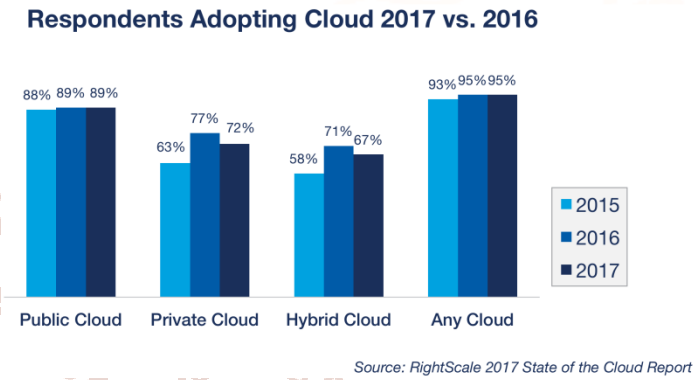

Fig.1 Public Cloud Adoption Comparison 2015- 2017

Table1. Growth of Cloud service

S. No	Year	Billion Dollar
1	2010	77
2	2011	93
3	2012	110
4	2013	131
5	2014	155
6	2015	181
7	2016	210

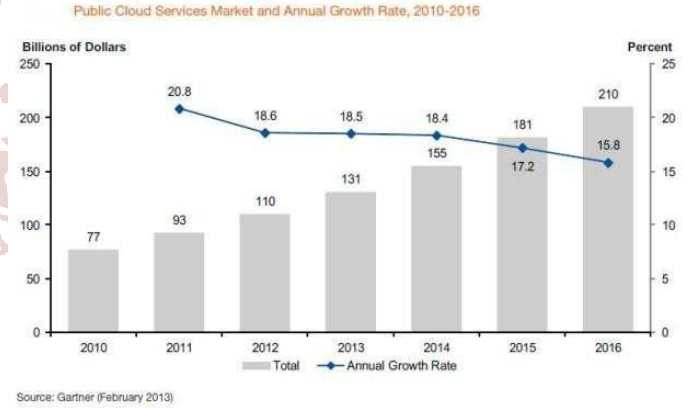

Fig.2 Public cloud service Market growth 2011-2017

Table2. Cloud Service Users

S. No.	Cloud Service	V. of Users
1.	Cloud Beginners	40%
2.	Cloud Explorers	60%
3.	Cloud Focused	80%

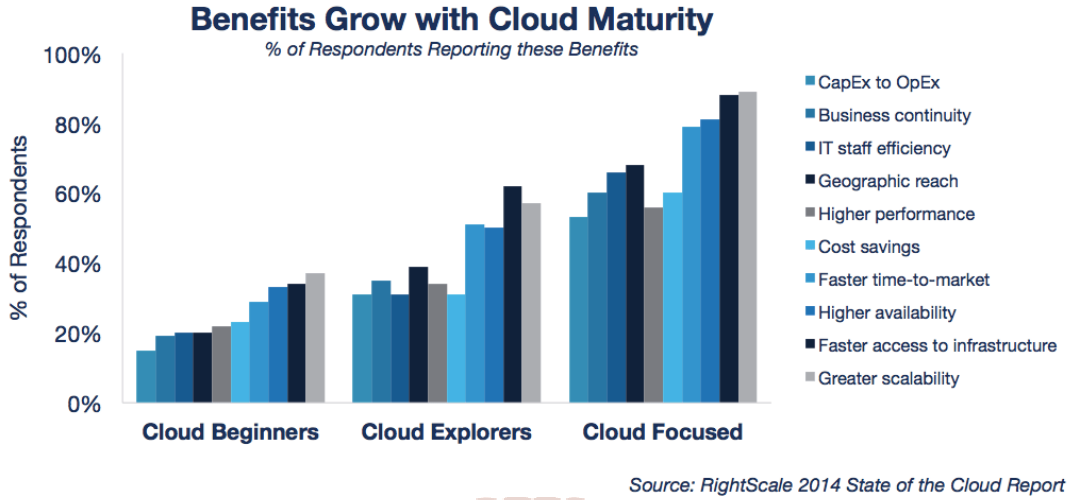

Fig.3 Cloud Service Users& their Growth

V. SECURITY BENEFITS OF BUILDING INFRASTRUCTURE AT CLOUD SCALE

Though self-hosted infrastructure may be free from threats specific to cloud-hosted infrastructure, meeting the security expectations of those who depend on it can prohibitively expensive. Securing a hosting infrastructure has significant costs that are fixed with respect to the number of machines to be secured. Examples of these fixed costs include:

- Assembling a host and network security strategy
- Training staff on the full range of tasks required by the security strategy
- Keeping abreast of new threats and countermeasures
- Developing a relationship with law enforcement

Cloud-infrastructure operators can amortize these fixed costs over a much larger infrastructure than self-hosting organizations can. Staff in cloud hosting providers can become more specialized than their counterparts administering self-hosted infrastructure, allowing them to develop expertise that increases productivity while receiving lower per-employee training.

Managed security solutions already allow owners of self hosted infrastructure to achieve some of these scale benefits. These managed offerings range from solutions in a box these boxes may provides firewalls, backup, or spam filtering to full service security consulting and system monitoring. Alas, managed security solutions may expose their clients to many of the same threats that cloud providers' tenants face. For example, a spam filtering box will have access to the client's network infrastructure and all incoming email, and is susceptible to secret search.

Economics will likely drive cloud-infrastructure operators to provide many of the solutions offered by managed security solutions today. Since the cloud provider must already be trusted with tenants' applications and data, tenants can obtain these services without growing their trusted employee and organization base. For example, a cloud-hosting operator, who already controls your network, needs no additional privileges to filter incoming traffic on port 25. What's more, security features built into the infrastructure can be cheaper to integrate into an application than those that require new components to be installed or that have APIs that may not be customized to the infrastructure. Once a cloud-infrastructure provider incurs the cost to develop a managed security solution for a security-conscious customer, the marginal cost to deploy the feature to other tenants is often negligible.

Some examples of security features that could be built into clouds, some of which are already present in hosting tools such as CPanel, are:

- Network and operating system auditing tools
- Tracking of all installed software, publishers, versions, and patch levels
- Credit card storage and fraud detection
- Public/private key generation, certificate generation, and storage
- Automatic authentication and protection of intra-tenant network communications
- Secure (append-only) logging of system events
- Spam filtering
- Password hashing and storage
- CAPTCHA generation and verification
- Software widgets such as password-strength meters

Many of these features would not be affordable if tenants had to cover the up-front costs, but become affordable if tenants only have to cover their share of the marginal costs. The leads to positive externalities whenever a security-conscious prospective tenant demands a new security feature.

Another benefit of building security features into the cloud infrastructure is to leverage data from multiple tenants. For example, when monitoring tools detect a new attack against one tenant the monitoring team and system will be more alert to similar attacks against other clients. Such systems must be designed not to restrict undesirable information from leaking from one tenant to the other. Still, reputation systems that identify bots, spammers, and other malicious activity can benefit from a wealth of data and few tenants would have a reason to opt out of providing it. Employees of the cloud provider entrusted to perform forensics on one tenant's compromised system may leverage what they learned from inspecting others' systems without leaking data. Bundling managed security into the cloud helps to overcome the free-riding problem in security data sharing identified by Gordon, Loeb, and Lucyshyn [17]. Tracking jurisdictional threats and keeping up with myriad laws and regulations is an expensive task, but one that has economies of scale. If infrastructure within the cloud providers' purview can be certified to provide compliance with security or privacy regulations, cloud providers may be able to assist with compliance at cloud scale. Cloud providers may also be able to assist in disseminating information that allows tenants to evaluate jurisdictional risks and keep up with local laws.

The economies of scale exhibited by these security solutions explain why existing managed security solutions are a big business, despite scale limitations that result from having clients in distributed locations with heterogenous infrastructures. Gartner estimates the total managed security service provider market had revenues of roughly $500 million in 2009. Major telecommunications carriers such as BT (via its acquisition of Counterpane) and Verizon now offer these services [41].

As we noted previously, cloud-hosting providers benefit from the opportunity to build relationships through their recurring interactions with regulators and law enforcement. If law enforcement officials know the cloud provider can guarantee them access to audit logs and data snapshots even if a tenant turns out to be malicious, they are less likely to take a tenant -or an entire data center! -offline in order to protect an investigation. More strategically, cloud providers can take an active role in shaping compliance and legal regimes to favor their tenants. The sheer scale of cloud hosting providers may make their security practices defacto best practices. Since liability law faults those who fail to take precautions that other reasonable parties would take, joining the herd that has put its security in the hands of the cloud may actually provide protection against liability suits.

VI. CONCLUSION

Cloud hosting has desirable features including low upfront costs, elasticity of resources, and cost savings that result from economies of scale. Self hosting provides greater direct control over infrastructure than can be achieved when leasing shared infrastructure from the cloud. However, achieving the benefits of cloud infrastructure by transferring infrastructure control to a third party needn't necessarily result in a net loss of security may also benefit from scale economies.

In particular, cloud providers can afford security measures with up-front costs that would be unaffordable in self-hosting environments, amortizing these costs over myriad machines or tenants. A key research opportunity is to develop security measures that reduce marginal costs even if they incur greater up-front costs. With three new workshops on cloud security emerging in the past year [1, 39, 22], we hope to see new technical solutions that exploit the economics of deploying security in cloud-hosting infrastructures.

REFERENCES

1. C. J. Antonelli, M. Undy, and P. Honeyman. The packet vault: Secure storage of network data. In Proceedings USENIX Workshop on Intrusion Detection and Network Monitoring, April 1999.
2. David Brumley and Dan Boneh. Remote timing attacks are practical. In Proceedings of the 12th USENIX Security Symposium, pages 1{14. Usenix, 2003
3. Andrew Bortz and Dan Boneh. Exposing private information by timing web applications. In WWW '07: Proceedings of the 16th international conference on World Wide Web, pages 621{628, New York, NY, USA, 2007. ACM.

4. Michael Armbrust, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy H. Katz, Andrew Konwinski, Gunho Lee, David A. Patterson, Ariel Rabkin, Ion Stoica, and Matei Zaharia. Above the clouds: A Berkeley view of cloud computing. Technical Report UCB/EECS- 2009-28, EECS Department, University of California, Berkeley, Feb 2009.

5. Craig Balding. What everyone ought to know about cloud security, 2009.

   http://www.slideshare.net/craigbalding/what everyone ought- to-know-about-cloud-security.

6. ACM. CCSW 2010: the ACM cloud computing security-workshop,2010

   http://crypto.cs.stonybrook.edu/ccsw10

7. Amazon. Request to remove email sending limitations, February2010.

   http://aws.amazon.com/contact-us/ec2-email-limitrequest/

8. P. Wendell, J. W. Jiang, M. J. Freedman, J. Rexford, "Donar: decentralized server selection for cloud services", ACM SIGCOMM Computer Communication Review, vol. 40, no. 4, pp. 231-242, 2010.P. Wendell, J. W. Jiang, M. J. Freedman, J. Rexford, "Donar: decentralized server selection for cloud services", ACM SIGCOMM Computer Communication Review, vol. 40, no. 4, pp. 231-242, 2010.

9. Y. A. Wang, C. Huang, J. Li, K. W. Ross, "Estimating the performance of hypothetical cloud service deployments: A measurement-based approach", INFOCOM 2011 Proceedings IEEE, pp. 2372-2380,2011.

10. S. Govindan, J. Liu, A. Kansal, A. Sivasubramaniam, "Cuanta: quantifying effects of shared on-chip resource interference for consolidated virtual machines", Proceedings of the 2nd ACM Symposium on Cloud Computing, pp. 22, 2011.

11. M. Jarschel, D. Schlosser, S. Scheuring, T. HoBfeld, "Gaming in the clouds: Qoe and the users perspective", Mathematical and Computer Modeling, vol. 57, no. 11, pp. 2883-2894, 2013.

12. C. Delimitrou, C. Kozyrakis, "Paragon: Qos-aware scheduling for heterogeneous datacenters", ACM SIGPLAN Notices, vol. 48, no. 4, pp. 77-88, 2013.

13. H. Yang, A. Breslow, J. Mars, L. Tang, "Bubbleflux: Precise online qos management for increased utilization in warehouse scale computers", ACM SIGARCH Computer Architecture News, vol. 41, no. 3, pp. 607-618, 2013.

14. M. Kwon, Z. Dou, W. Heinzelman, T. Soyata, H. Ba, J. Shi, "Use of network latency profiling and redundancy for cloud server selection", 2014 IEEE 7th International Conference on Cloud Computing, pp. 826-832, 2014.

15. B. Zhou, A. V. Dastjerdi, R. N. Calheiros, S. N. Srirama, R. Buyya, "A context sensitive offloading scheme for mobile cloud computing service", Cloud Computing (CLOUD) 2015 IEEE 8th International Conference on. IEEE, pp. 869-876, 2015.

16. F. Caglar, S. Shekhar, A. Gokhale, X. Koutsoukos, "An Intelligent Performance Interference-aware Resource Management Scheme for IoT Cloud Backends", 1st IEEE International Conference on Internet-of-Things: Design and Implementation, pp. 95-105, Apr. 2016.