ISSN:1991-8178

Australian Journal of Basic and Applied Sciences

Journal home page: www.ajbasweb.com

An Evaluations of Safety Concerns in The Ambience of Cloud Computing

Kiyana Bahadori

Department of Computer Science, Bangalore University, Bangalore, India.

ARTICLE INFO

Article history:
Received 12 October 2014
Received in revised form 26 December 2014
Accepted 1 January 2015
Available online 27 February 2015

Keywords:
Cloud Computing, Security, Hadoop, Cloud Services.

ABSTRACT

The following paper discusses on security issues in cloud computing and present a layered framework for secure clouds and then focus on two of the layers, i.e., the storage layer and the data layer. In particular, the authors discuss a scheme for secure third party publications of documents in a cloud. Next, the paper will converse secure federated query processing with map Reduce and Hadoop, and discusses the use of secure co-processors for cloud computing. Finally, the authors discuss XACML implementation for Hadoop and discuss their beliefs that building trusted applications from interested components will be a major aspect of secure cloud computing.

To Cite This Article: KiyanaBahadori.An Evaluations of Safety Concerns in The Ambience of Cloud Computing.***Aust. J. Basic & Appl. Sci.,*** *9(5): 531-537, 2015*

INTRODUCTION

Google has now introduced the MapReduce framework for processing large amounts of data on commodity hardware. Apache's Hadoop distributed file system (HDFS) is emerging as a superior software component for cloud computing combined with integrated parts such as MapReduce. The need to augment human reasoning, interpreting, and decision-making abilities has resulted in the emergence of the Semantic Web, which is an initiative that attempts to transform the web from its current, merely human-readable form, to a machine-processable form. Therefore, our goal is to make increment enhancements to securing the cloud that will ultimately result in a secure cloud. There are several benefits, especially on infrastructure costs, but, as with all new technologies, cloud computing also has some drawbacks. The question is why security is such a complicated challenge in the decision of moving to the Cloud. The answer is easy: lack of control over their data. IT infrastructures have been de-perimeterized, so security needs to be approached from another perspective; but this blurring of the perimeter is not the only issue (Jansen, W., T. Grance, 2011).

The traditional network perimeter is broken, and organizations feel they have lost control over their data. New attack vectors have appeared, and the benefit of being accessible from anywhere becomes a big threat. Amongst resilience and agility, the low costs that provide cloud computing is a real hook for companies trying to reduce costs. Start-ups looking for a place in the market pray for an economic solution that allows them to focus on their business without worrying on maintain an IT infrastructure. It is necessary to adopt virtualization technologies to allow the use of multi-tenant environments. Both give place to a new set of challenges when put together. Virtualization adds a new layer that can be targeted, and multi-tenancy facilitates the process to reach the layer. Virtualization security issues need to be reviewed from a new point of view not seen before, coexisting with possible malicious tenants. Cloud is a place which you go to use technology when you need it, for as long as you need it via just Internet network (Ormandy, T., 2007). The Cloud contains both IT Physically Infrastructure and software. It can be software you access via the web or a physical server which you use exactly when it is required. Figure 1 shows the gateway of the cloud computing (Berger, S., *et al* 2009).

Corresponding Author: Mahdi Kiani, Name of University, Jawaharlal Nehru Technological University Hyderabad, India.

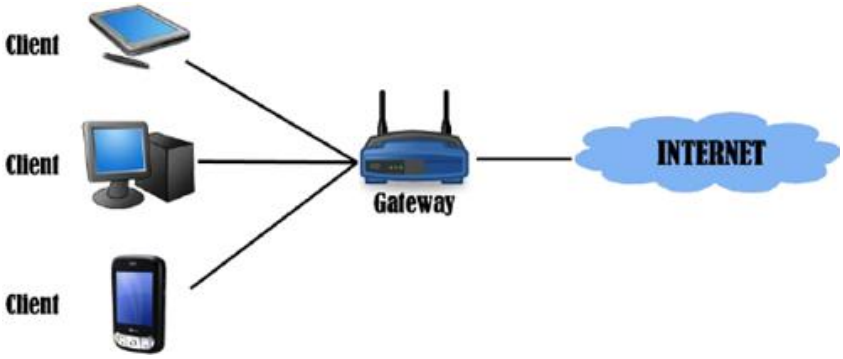


Fig. 1: the gateway of the cloud computing

Delivering computing resources via a global network was opined in the beginning of 1960s by J.C.R. Licklider. Afterwards, Part of this idea had evolved in many years and has taken its present form with its global name, Internet. But, we can take whole idea (Delivering computing resources via global network) as an underlying concept for Cloud Computing, because J.C.R. Licklider's vision was for everyone on the globe to be interconnected and accessing programs and data at any side, from anywhere. And this vision sounds like what we call Cloud Computing. (Carlin, S., K. Curran, 2011)

The technology is not revolutionary, but it is the outcome of the continuous advancement of the data management technology. The core idea of computing as a utility computing and grid computing developed in 1960's. Around 1999, internet as the mechanism to provide Application as Service got developed. In 2005, the term cloud computing became popular and the sub classification of IaaS, PaaS&SaaS got formalized. The phrase "Cloud" originates from the cloud symbol used by flow charts and diagrams to symbolize the Internet. The term Cloud Computing refers to both the applications delivered as services over the Internet and the servers and system software in the data centers that provide those services. What goes on in the cloud manages multiple infrastructures across multiple organizations and consists of one or more frameworks overlaid on top of the infrastructures tying them together (Mell, P., T. Grance, 2011).

Cloud Computing grounds on already established trends for decreasing the cost of the delivery of services while increasing the agility and speed with which services are deployed. Cloud Computing is incorporating Utility Computing (On-demand deployment), Virtualization, Delivering services via Internet Network and scalable dynamic application development. Cloud computing security challenges and issues discussed various researchers. The Cloud Computing Use Cases group (Naehrig, M., *et al*., 2011) discusses the different use case scenario requirements that may exist in the cloud computing model. They consider use cases from different perspectives including customers, developers and security engineers investigated the different security risks related to adopting cloud computing along with the affected assets, the risks likelihood, impacts, and vulnerabilities in cloud computing that may lead to such risks. Similar efforts discussed in"Threats to Cloud Computing" by CSA (Garfinkel, T., M. Rosenblum, 2005; Naehrig, M., *et al*., 2011) discuss the security SLA's specifications related to data locations, segregation and data (Washington, D.C., *et al*., 2008) discuss high level security cloud computing model such as data integrity, payment, and privacy of sensitive information. Kresimir security management standards such as ITIL and Open Virtualization Format (OVF). The technical security issues arising from computing model such as XML-attacks, Browsers attacks, and flooding attacks. Bernd *et al* security vulnerabilities existing in the cloud platform. The authors grouped the possible vulnerabilities into technology related, cloud characteristics -related, security controls (Jansen, W., T. Grance, 2011) discuss the security challenges service delivery model, focusing on the SAAS discusses critical areas of cloud computing. They deliver a set of best practices for the cloud provider, consumers and security vendors to follow in each domain. CSA detailed reports discussing for some of these. In our research we did a deep investigation in the cloud model to identify the root causes and key participating dimensions in such security issues/problems discussed by this will help better to understand the problem and solutions (Xiao, S., W. Gong, 2010).

Methodology:

After considering the issues the practical approach is needed. For this purpose the sample model is designed to implement in the cloud computing architecture. In this paper this model is reviewed and experimental results are observed. Cloud computing architecture is divided into bottom layer that includes virtualized resources and upper layer contains specific services to the user (Mell, P., T. Grance, 2011). Figure 2 represents the model of the study.

The experimental results are obtained from Hadoop, an open source version of Google file system and Map-reduce programming specification. It is the software that is used to write applications that process large amount of statistics (multi-terabyte data-sets) in-parallel on big clusters (thousands of nodes) of product hardware with reliable and consistent approach.

After considering the issues the practical approach is needed. For this purpose the sample model is designed to implement in the cloud computing architecture. In this paper this model is reviewed and experimental results are observed. Cloud computing architecture is divided into bottom layer that includes virtualized resources and upper layer contains specific services to the user (Mell, P., T. Grance, 2011). Figure 2 represents the model of the study.

A major part of our system is HDFS which is a distributed Java-based file system with the capacity to handle a large number of nodes storing petabytes of data. Ideally a file size is a multiple of 64 MB. Reliability is achieved by replicating the data across several hosts. The default replication value is 3 (i.e., data is stored on three nodes). Two of these nodes reside on the same rack while the other is on a different rack. A cluster of data nodes constructs the file system. The nodes transmit data over HTTP and clients' access data using a web browser. Data nodes communicate with each other to regulate, transfer and replicate data.

Data blocks are stored in Datanodes. The namenode is the single point of failure as it contains the metadata. So, there is optional secondary Namenode that can be setup on any machine. The client accesses the Namenode to get the metadata of the required file. After getting the metadata, the client directly talks to the respective Datanodes in order to get data or to perform IO actions.

This engine consists of a Job Tracker. The client applications submit map/reduce jobs to this engine. The Job Tracker attempts to place the work near the data by pushing the work out to the available Task Tracker nodes in the cluster.

Current systems utilizing Hadoop have the following limitations:

- No facility to handle encrypted sensitive data:

Sensitive data ranging from medical records to credit card transactions need to be stored using encryption techniques for additional protection. Currently, HDFS does not perform secure and efficient query processing over encrypted data.

- Semantic Web Data Management:

There is a need for viable solutions to improve the performance and scalability of queries against semantic web data such as RDF (Resource Description Framework). The number of RDF datasets is increasing. The problem of storing billions of RDF triples and the ability to efficiently query them is yet to be solved (Muys, 2006; Teswanich, 2007; Ramanujam, 2009). At present, there is no support to store and retrieve RDF data in HDFS.

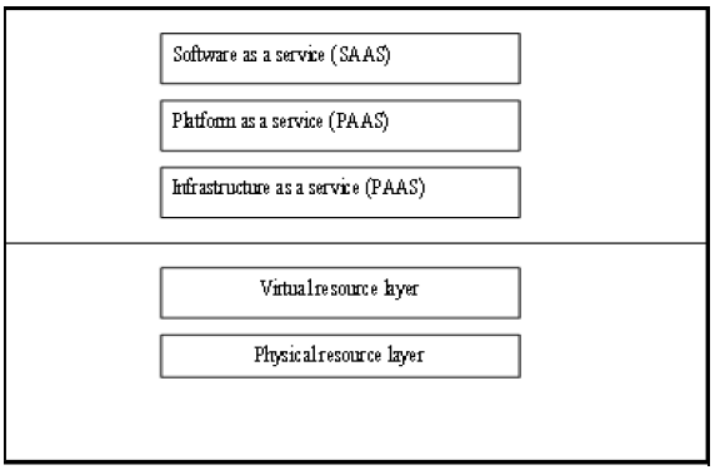
- No fine-grained access control:

HDFS does not provide fine-grained access control. There is some work to provide access control lists for HDFS (Zhang, 2009). For many applications such as assured information sharing, access control lists are not sufficient and there is a need to support more complex policies.

- No strong authentication:

A user who can connect to the JobTracker can submit any job with the privileges of the account used to set up the HDFS. Future versions of HDFS will support network authentication protocols like Kerberos for user authentication and encryption of data transfers. However, for some assured information sharing scenarios, we will need public key infrastructures (PKI) to provide digital signature support.

In order to provide strong security guarantees for our system, we will apply automated software verification technologies, including type and model-checking, which we have previously used to certify the output of binary-rewriters. Such certification allows a small, trusted verifier to independently prove that rewritten binary code satisfies the original security policy, thereby shifting the comparatively larger binary-rewriter out of the trusted computing base of the system.



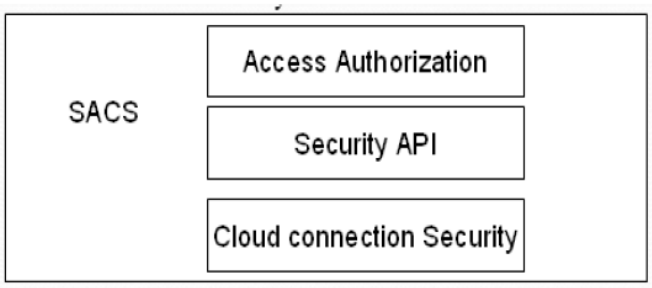


Fig. 2: modelling

RESULTS AND DISCUSSION

There are several groups interested in developing standards and security for clouds and cloud security. The Cloud Security Alliance (CSA) is gathering solution providers, non-profits and individuals to enter into discussion about the current and future best practices for information assurance in the cloud (Cloud Security Alliance (CSA) – security best practices for cloud computing, 2009) The Cloud Standards web site is collecting and coordinating information about cloud-related standards under development by other groups (Clouds Standards, 2010). The Open Web Application Security Project (OWASP) maintains a "top 10" • list of vulnerabilities to cloud-based or Software as a Service deployment models which is updated as the threat landscape changes (OWASP, 2010). The Open Grid Forum publishes documents to containing security and infrastructural specifications and information for grid computing developers and researchers. The best security solution for web applications is to develop a development framework that shows and teaches a respect for security. Tsai, W., Jin, Z., &Bai, X. (2009) put forth a four-tier framework for web-based development that though interesting, only implies a security facet in the process (Tsai, Jin, &Bai, 2009, p. 1). Towards best practices in designing for the cloud by Berre, Roman, Landre, Heuvel, Lennon, &Zeid (2009) is a road map toward cloud-centric development the X10 language is one way to achieve better use of the cloud capabilities of massive parallel processing and concurrency.Halton and Basta (2007) suggest one way to avoid IP spoofing by using encrypted protocols wherever possible. They also suggest avoiding ARP poisoning by requiring root access to change ARP tables; using static, rather than dynamic ARP tables; or at least make sure changes to the ARP tables are logged. Raj, Nathuji, Singh and England (2009) suggest resource isolation to ensure security of data during processing, by isolating the processor caches in virtual machines, and isolating those virtual caches from the Hypervisor cache (Raj, Nathuji, Singh, & England, 2009, p. 80). Hayes points out that there is no way to know if the cloud providers properly deleted a client's purged data, or whether they saved it for some unknown reason. Hayes (2008) points out an interesting wrinkle here, â€œAllowing a third-party service to take custody of personal documents raises awkward questions about control and ownership: If you move to a competing service provider, can you take a data with you? Could you lose access to documents if you fail to pay a bill? The issues of privacy and control cannot be solved, but merely assured with tight service-level agreements (SLAs) or by keeping the cloud itself private.One simple solution, which Milne (2010) states to be a widely used solution for UK businesses is to simply use in-house private clouds (Milne, 2010). Nurmi, Wolski, Grzegorczyk, Obertelli, Soman, Youseff, &Zagorodnov show a preview of one of the available home-grown clouds in their (2009) presentation. The Eucalyptus Open-Source Cloud-Computing Systems.Some methods have been developed that serve as alternatives to encryption. These methods are generally faster than encryption but have their own drawbacks.Data Splitting was initially developed by DivyakantAgrawal and his colleagues. The idea is to split the data over multiple hosts that cannot communicate with each other; only the owner who can access both hosts can collect and combine the separate datasets to recreate the original. This method is extremely fast compared to encryption but it requires at least two separate, but homogeneous service providers.

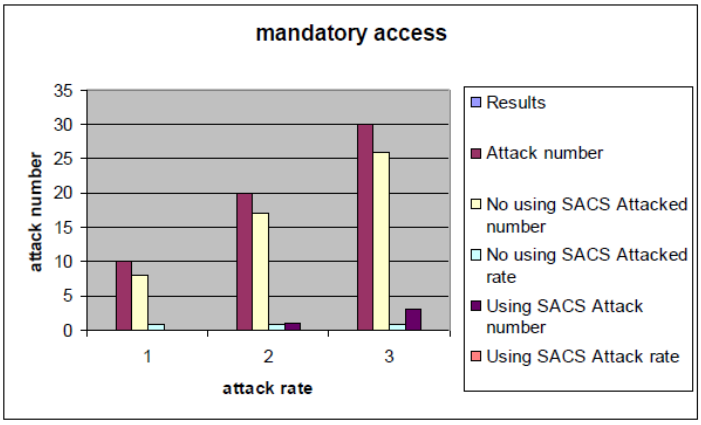


Fig. 3: Mandatory Access Result

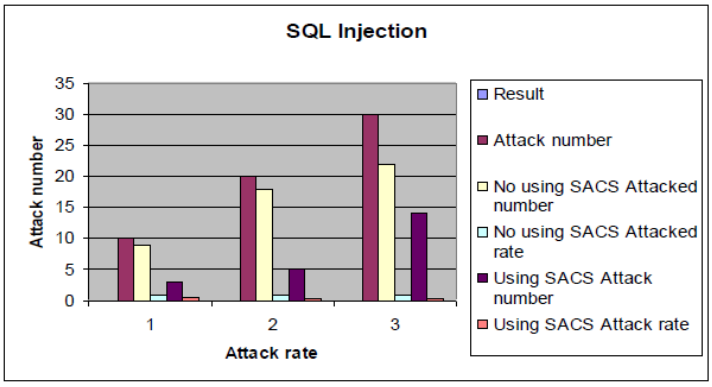


Fig. 4: SQL injection

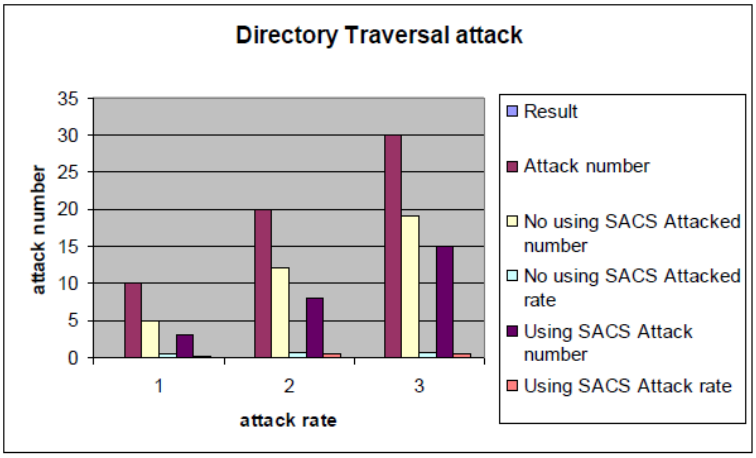


Fig. 5: Directory Traversal

Figure 6 shows the comparison results of all attacks (Mandatory access, directory traversal, SQL injection) using SACS model and not using SACS model. The quick adoption of the cloud model is plain in the success of the Amazon Elastic Cloud Computing (EC2) product, the buy-in from IBM with their backing of the highly concurrent, massively parallel language X-10 and Microsoft's investment in its Azure cloud. Janine Milne reported that eight of ten businesses surveyed in the UK were opting for private cloud initiatives rather than public cloud projects and they stated the issues of concern to be data security in transit, in storage or during processes. It is plain that the field is full and the harvest for the IT security profession and IT in general are excellent. The literature available on cloud security is plentiful, and there is enough higher-quality work to develop a conceptual framework for security issues and solutions. It is the human right to secure his private and sensitive information. In cloud context privacy occurs according to the cloud deployment model (Berger, S., *et al*., 2009). In Public cloud (accessed through the Internet and shared amongst different consumers) is one of the

dominant architecture when cost reduction is concerned, but relying on a CSP to manage and hold customer information raises many privacy concerns.

In SAAS environment service provider is responsible to control data. Now how customer can retain its control on data when information is processed or stored. It is legal requirement of him and also to make trust between customer and vendor (Han-zhang, W., H. Liu-sheng, 2010). In this new paradigm user sensitive information and data is processed in 'the cloud' on systems having no any, therefore they have danger of misuse, theft or illegal resale. Adding more, this is not patent that it will be possible for a CSP to guarantee that a data subject can get access to all his/her PII, or to comply with a request for deletion of all his/her data. This can be difficult to get data back from the cloud, and avoid vendor lock-in (Carlin, S., K. Curran, 2011).

One of the threats can occur if information is placed for illegal uses. Cloud computing standard business model tells that the service provider can achieve profits from authorized secondary uses of users' data, mostly the targeting of commercials (Mell, P., T. Grance, 2011). Now a days there are no technological barriers for secondary uses. In addition, it has the connected issue of financial flexibility of the CSPs: for example, possibility of vendor termination, and if cloud computing provider is bankrupted or another company get data then what would happen (Santos, N., *et al*., 2009)

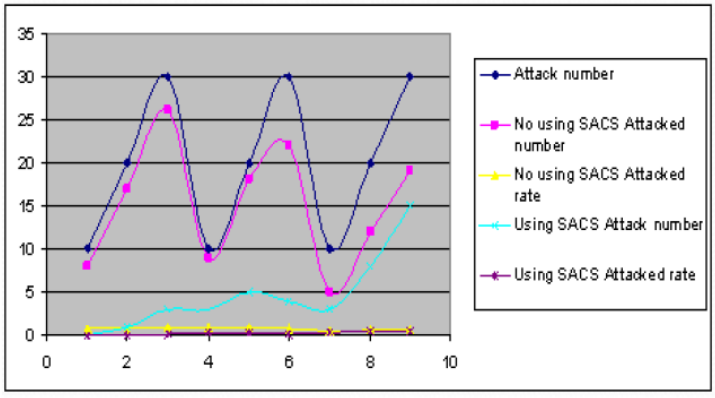


Fig. 6: comparison result using SACS and no SACS

These days, it's awfully hard for anyone who follows technology trends to avoid the cloud. Just as fluffy white clouds however overhead, news about cloud computing follows the tech and IT sectors everywhere. Cloud based solutions have the potential to increase efficiency while also lowering costs for some organizations.

However, the cloud also presents security concerns. With gigabytes of data stored remotely, it is imperative for that information to remain as well guarded as possible. A layered security approach can help protect against many of the risks associated with cloud technology. Decision makers should ensure that their providers follow best practices and stay aware of the most recent threats.

Cloud computing is the most modern technology so lots of issues are remained to consider. It has many open issues some are technical that includes scalability, elasticity ,data handling mechanism, reliability, license software, ownership, performance, system development and management and non-technical issues like legalistic and economic aspect. Cloud computing still unknown "killer application" will establish so many challenges and solutions must develop to make this technology work in practice. So the research is not stop here much work can be done in future. The model presented in this paper is the initial step and needs more modifications; however it can provide the basis for the deeper research on security deployment of cloud computing for the research community working in the field of Cloud Computing.

Conclusion:

In this paper, we first discussed security issues for cloud. These issues include storage security, middleware security, data security, network security and application security. The main goal is to securely store and manage data that is not controlled by the owner of the data. Then we focused on specific aspects of cloud computing. In particular, we are taking a bottom up approach to security where we are working on small problems in the cloud that we hope will solve the larger problem of cloud security. First, we discussed how we may secure documents that may be published in a third party environment. Next, we discussed how secure co-processors may be used to enhance security. Finally, we discussed how XACML may be implemented in the Hadoop environment as well as in secure federated query processing with SPARQL using MapReduce and Hadoop.

We have discussed several security issues that currently affect cloud systems; however, there may be many unmentioned and undiscovered security issues. Research is currently being done on the different known issues

faced by cloud systems and possible solutions for these issues, however there is still a need for better solutions if cloud systems are to be widely adopted.

REFERENCES

Berger, S., R. Cáceres, K. Goldman, D. Pendarakis, R. Perez, J.R. Rao, E. Rom, R. Sailer, W. Schildhauer, D. Srinivasan, S. Tal, E. Valdez, 2009. Security for the Cloud infrastructure: trusted virtual data center implementation. IBM J Res Dev., 53(4): 560-571.

Carlin, S., K. Curran, 2011. Cloud Computing Security. International Journal of Ambient Computing and Intelligence., 3(1): 38-46.

Garfinkel, T., M. Rosenblum, 2005. When virtual is harder than real: Security challenges in virtual machine based computing environments. In: Proceedings of the 10th conference on Hot Topics in Operating Systems, Santa Fe, NM. volume 10. CA, USA: USENIX Association Berkeley, pp: 227-229.

Han-zhang, W., H. Liu-sheng, 2010. An improved trusted cloud computing platform model based on DAA and privacy CA scheme. In: International Conference on Computer Application and System Modeling (ICCASM), vol. 13, V13–39.

Washington, D.C., USA: S. Berger, R. Cáceres, D. Pendarakis, R. Sailer, E. Valdez, R. Perez, W. Schildhauer, D. Srinivasan, 2008. TVDc: managing Security in the trusted virtual datacenter. SIGOPS Oper. Syst. Rev., 42(1): 40-47.

Jansen, W., T. Grance, 2011. Guidelines on Security and privacy in public Cloud Computing. Gaithersburg, MD: NIST, Special Publication, pp: 800-144.

Jasti, A., P. Shah, R. Nagaraj, R. Pendse, 2010. Security in multi-tenancy cloud. In: IEEE International Carnahan Conference on Security Technology (ICCST), KS, USA. Washington, DC, USA: IEEE Computer Society, pp: 35-41.

Mell, P., T. Grance, 2011. The NIST definition of Cloud Computing. Gaithersburg, MD: NIST, Special Publication, pp: 800-145.

Naehrig, M., K. Lauter, V. Vaikuntanathan, 2011. Can homomorphic encryption be practical? In: Proceedings of the 3rd ACM workshop on Cloud Computing Security workshop. NY, USA: ACM New York. pp: 113-124.

Ormandy, T., 2007. An empirical study into the Security exposure to hosts of hostile virtualized environments. In: CanSecWest applied Security conference. Vancouver.

Santos, N., K.P. Gummadi, R. Rodrigues, 2009. Towards Trusted Cloud Computing. In: Proceedings of the 2009 conference on Hot topics in cloud computing, San Diego, California. CA, USA: USENIX Association Berkeley.

Xiao, S., W. Gong, 2010. Mobility Can help: protect user identity with dynamic credential. In: Eleventh International conference on Mobile data Management (MDM). Washington, DC, USA: IEEE Computer Society, pp: 378-380.

Zhang, Q., L. Cheng, R. Boutaba, 2010. Cloud Computing: state-of-the-art and research challenges. Journal of Internet Services Applications., 1(1): 7-18.