ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)
Vol. 2, Issue 2, Ver. 3 (April - June 2014)
International Journal of Advanced Research in Computer Science & Technology (IJARCST 2014)

# An Overview of Security and Privacy Issues for Cloud Computing Environment

[I]Anuradha Mishra, [II]Suresh Kashyap, [III]Dr. K.N. Singh
[I]M.Phil. (CS) Student, [II]Asst. Prof. in IT Department, [III] Assoc. Prof. in Physics Department
[I,II,III]Dr. C. V. Raman University, Bilaspur (C.G.), India

**Abstract**
Cloud Computing represents one of the most significant shifts in information technology many of us are likely to see in our lifetimes. *We are reaching the point where computing functions as a utility, promising innovations yet unimagined. The major roadblock to full adoption of Cloud Computing has been concern regarding the security and privacy of information. Much work has been done regarding the security of the cloud and data within it, but until now, there have been no best practices to follow when developing or assessing security services in an elastic cloud model—a model that scales as client requirements change. The aim of this guide is to provide a practical reference to help enterprise information technology (IT) and business decision makers as they analyse and consider the security implications of cloud computing on their business. In this paper we present a list of steps, along with guidance and strategies, designed to help these decision makers evaluate and compare security offerings in key areas from different cloud providers.*

**Keywords**
*Cloud Computing, security, privacy, technology, information technology, model.*

## I. Introduction

Cloud computing has been defined by NIST as 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 cloud provider interaction . Cloud computing technologies can be implemented in a wide variety of architectures, under different service and deployment models, and can coexist with other technologies and software design approaches. The security challenges cloud computing presents, however, are formidable, especially for public clouds whose infrastructure and computational resources are owned by an outside party that sells those services to the general public. The emergence of cloud computing promises to have far-reaching effects on the systems and networks of federal agencies and other organizations. Many of the features that make cloud computing attractive, however, can also be at odds with traditional security models and controls.

The primary purpose of this report is to provide an overview of public cloud computing and the security and privacy considerations involved. More specifically, this document describes the threats, technology risks, and safeguards surrounding public cloud environments, and their treatment. Cloud providers are generally not aware of a specific organization's security and privacy needs. Adjustments to the cloud computing environment may be warranted to meet an organization's requirements. Organizations should require that any selected public cloud computing solution is configured, deployed, and managed to meet their security, privacy, and other requirements. Non-negotiable service agreements in which the terms of service are prescribed completely by the cloud provider are generally the norm in public cloud computing. Negotiated service agreements are also possible. Similar to traditional information technology outsourcing contracts used by agencies, negotiated agreements can address an organization's concerns about security and privacy details, such as the vetting of employees, data ownership and exit rights, isolation of tenant applications, data encryption and segregation, tracking and reporting service effectiveness, compliance with laws and regulations, and the use of validated products meeting federal or national standards (e.g., Federal Information Processing Standard 140).

## II. Cloud Computing Architecture

The Cloud Computing architecture comprises of many cloud components, each of them is loosely coupled. We can broadly divide the cloud architecture into two parts:

A. Front End
B. Back End

Each of the ends is connected through a network, usually via Internet. The following diagram shows the graphical view of cloud computing architecture:

### A. Front End

Front End refers to the client part of cloud computing system. It consists of interfaces and applications that are required to access the cloud computing platforms, e.g., Web Browser. The server employs certain protocols, known as middleware, helps the connected devices to communicate with each other.

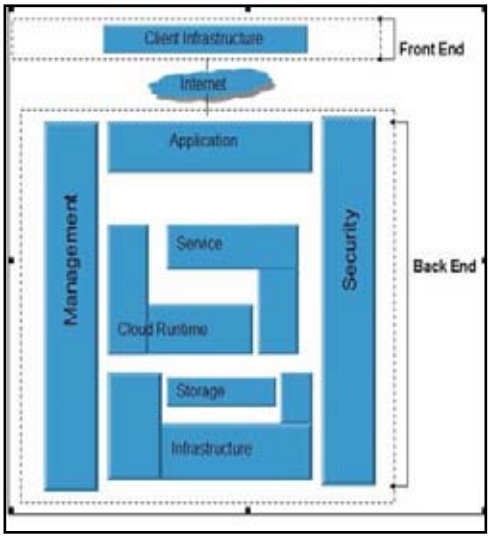


Fig. 1: Cloud Computing Architecture

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

### B. Back End

Back End refers to the cloud itself. It consists of all the resources required to provide cloud computing services. It comprises of huge data storage, virtual machines, security mechanism, services, deployment models, servers, etc. It is the responsibility of the back end to provide built-in security mechanism, traffic control and protocols.

## III. Important THINGHS ABOUT Cloud Security

More so than other types of hosted environments, when it comes to the cloud, companies worry about the Security.

There are three important things need to know about cloud security. First, cloud security is almost exactly like your internal security. The security tools you use every day are the same tools that will be used to protect your data in the cloud. The one difference is that the cloud is a multi-tenant environment with more than one company (multiple tenants) sharing the same cloud service provider.

Second, security issues involving the cloud can all be addressed using your current security tools. Security needs should be carefully considered. But they shouldn't be viewed as a hindrance if you are considering a move to the cloud.

The commodity nature of IT will, over time, require that you move some of your technologies to the cloud to remain financially competitive. So you should begin addressing your security issues and get ready for the move.

Third, if you select a quality cloud services provider, your security in the cloud will be as good as, or better, than your current security in most cases.

Typically, the level of security you get will be designed to meet the needs of the most risky client in the cloud. And, if you use the tools identified in this paper as a starting point, you will have a good idea of how comparable your cloud security versus internal security will be.

## IV. Security And Privacy Issues in Cloud Computing Technology

The process of creating and managing a secure cloud space is a more challenging task than creating a secure classical IT environment. Given the immaturity of this technology the new resources and the reallocation of traditional ones are not fully tested and come with new risks that are still under research. The main risks of adopting cloud computing are:

### A. Misunderstanding Responsibilities

There is a tremendous potential for misguided risk management decisions if cloud providers do not disclose the extent to which the security controls are implemented and the consumer knows which controls are further needed to be adopted. If in a traditional scenario the security of data is entirely the burden of the company owning data. In the cloud computing scenario the responsibilities are divided between the two actors: the cloud provider and the client.. Different kinds of cloud services adopted mean different responsibilities for the service provider and the customer. If an IaaS service model is adopted, then the provider is responsible for physical security, environment security and the virtualization software security, whereas the consumer is responsible for securing everything else above this layer including operating system, applications and data. However, in an SaaS cloud service model the provider is responsible not only for the physical and environmental security but also for all the software services he uses in order to provide that particular software service to the client. In this case, the responsibilities of the consumer in the field of security are much lowered.

### B. Data security and confidentiality issues

One of the biggest security concerns people have when moving to the cloud is related to the problem of keeping data secure and confidential. In this respect, some particular problems arise: who can create data, where the data is stored, who can access and modify data, what happens when data is deleted, how the back-up is done, how the data transfer occurs, etc. Worth reminding in this respect is that it is much more difficult for the cloud customer to effectively check the data handling practices of the cloud provider and thus be sure that the data is handled in a proper way. To counter such a risk, strategies like data encryption, particular public key infrastructure, data dispersion, standardization of APIs, etc are Proposed to customers as security measures to create a trusted and secure environment.

### C. Lack of Standards

As a result, many standard development organizations were established in order to research and develop the specifications. Organizations like Cloud Security Alliance, European Network and Information Security Agency, Cloud Standards Customer Council, etc. have developed best practices regulations and recommendations. the immaturity of this technology makes it difficult to develop a comprehensive and commonly accepted set of standards. Other establishments, like Distributed Management Task Force, The European Telecommunications Standards Institute, Open Grid Forum, Open Cloud Consortium, National Institute of Standards and Technology, Storage Networking Industry Association etc., centered their activity on the development of working standards for different aspects of the cloud technology. The excitement around cloud has created a flurry of standards and open source activity leading to market confusion. That is why certain working groups like Cloud Standards Coordination, TM Forum etc. act to improve collaboration, coordination, information and resource sharing between the organizations acting in this research field.

### D. Interoperability issues

The cloud computing technology offers a degree of resource scalability which has never been reached before. Companies can benefit from additional computational needs, storage space, bandwidth allocation, etc. whenever they need and without great investments to support peak load demands. If the demand falls back the additional capacity can be shut down just as quickly as it was scaled up without any hardware equipment sitting idle. This great advantage has also a major drawback. It comes alongside with the risk of managing data within a shared environment (computation, storage, and network) with other cloud clients. Additionally, at one time one company may have multiple cloud providers for different services which have to be interoperable. In time, for different reasons, companies may decide to move their services to another cloud and in such a case the lack of interoperability can block or raise heavy obstacles to such a process. Cloud providers may find the customer lock-in system attractive, but for the customers interoperability issues mean that they are vulnerable to price increases, quality of services not meeting their needs, closure of one or more cloud services, provider going out of business, disputes between with the cloud provider.

### E. Reliability breakdowns

Another important aspect of the cloud computing is the reliability or availability of services. The breakdown of an essential service operating in a cloud has an impact on many clients. For example, in April 2012 there was a Gmail disruption hat made Gmail services unavailable or almost 1 hour. The company first aid that it affected less than 2 % of heir customers, then they updated to 0 %, which sums around 35 million liens of a total of 350 million users. These incidents are not rare and evidence the customer lack of control over there data.

The irony is that, in terms of reliability, cloud providers have set high standards which are rarely achieved in an internal environment. However, because these outages effect large numbers of consumers t cast doubts in the minds of IT excision makers over the viability f replacing desktop functionality itch the functionality offered by the cloud. also, in this industry, the leading companies have set some high level quality services.Those levels are not easy to be reached by the other cloud service providers which do not have such a well developed infrastructure. Unfortunately for the clients these quality services may come at higher costs and sometimes the decision makers, lured by the cheaper services, will be reluctant to collaborate with such a provider.

### F. Malicious insider

A malicious insider is a person motivated to create a bad impact on the organization's mission by taking action that compromises information confidentiality, integrity, and/or availability. When sensitive data is processed outside the enterprise the organizational managers are less immediately aware of the nature and level of risk and they do not possess quick and direct capability to control and counter these risks. Experienced security specialists are highly aware of the inverse

## IV. Conclusions

Cloud computing promises to have far-reaching effects on the systems and networks of federal agencies and other organizations. Emphasis on the cost and performance benefits of public cloud computing, however, tend to overshadow some of the fundamental security and privacy concerns federal agencies and organizations have with these computing environments. Many of the features that make cloud computing attractive can also be at odds with traditional security models and controls. Several critical pieces of technology, such as a solution for federated trust, are not yet fully realized, impinging on successful cloud computing deployments. Determining the security of complex computer systems composed together is also a long-standing security issue that plagues large-scale computing in general, and cloud computing in particular. In the process of adopting cloud based services companies and IT organizations should evaluate the business benefits and risks. The cloud's economies of scale and fl edibility are both a friend and a foe from a security point of view. The management of security risk involves users, the technology itself, the cloud service providers, and the legal aspects of the data and services being used. The massive concentrations of resources and data present a more attractive target to attackers, but cloud-based defenses can be more robust, scalable and cost-effective than traditional ones.

## References

[1] *Ivona Brandic,—Towards Self manageable Cloud services‖ 0730-3157/09 , 2009 IEEE.*
[2] *http://www.cloudsecurity.org, accessed on April 10, 2009.*
[3] *D.J. Solove, —A Taxonomy of Privacy, University of Pennyslavania Law Review, vol 154, no 3, January 2006*
[5] *T. R. Peltier, J. Peltier, and J. Blackley, —Information Security Fundamentals". Auerbach Publications, Boston, MA, USA, 2003.*
[6] *John Harauz, Lori M. Kaufman and Bruce Potter, —Data security in the world of cloud computing —,2009 IEEE CO Published by the IEEE Computer and Reliability Societies.*
[7] *Siani Pearson, —Taking account of Privacy when Designin Cloud computing Services CLOUD'09, May 23, 2009,Vancouver, Canada, □2009 IEEE.*
[8] *Meiko Jensen, Jorg Schwenk, Nils Gruschka and Luigi Lo Iacono, —On technical security issues in cloud computing 978-0-7695- 3840-2/ 092009,IEEE Computer Society.*
[6] *Balachandra Reddy Kandukuri, Ramakrishna Paturi V and Dr. Atanu Rakshit, —Cloud securityIssues‖ 978-0-7695-3811-2/09 2009, IEEE computer society.*
[7] *Guy Bunker, Farnam Jahanian, Aad van Moorsel and Joseph Weinman,‖ Dependability in the cloud: Challenges and opportunities‖, IEEE 2009.*
[8] *Lizhe Wang, Jie Tao, Marcel Kunze , Alvaro Canales Castellanos, David Kramer and Wolfgang Karl, —scientific Cloud computing: early Definition and Experience‖, 2008 IEEE.*
[9]. *Zissis D, Lekkas D (2012) Addressing Cloud Computing Security issues. Futur Gener Comput Syst 28(3):583–592*
[10] *Jansen W, Grance T (2011) Guidelines on Security and privacy in public Cloud Computing. NIST, Special Publication 800–144, Gaithersburg, MD*
[11] *Mell P, Grance T (2011) The NIST definition of Cloud Computing. NIST, Special Publication 800–145, Gaithersburg, MD*
[12] *Zhang Q, Cheng L, Boutaba R (2010) Cloud Computing: state-of-the-art and research challenges. Journal of Internet Services Applications 1(1):7–18*
[13] *Ju J, Wang Y, Fu J, Wu J, Lin Z (2010) Research on Key Technology in SaaS. In: International Conference on Intelligent Computing and Cognitive Informatics (ICICCI), Hangzhou, China. IEEE Computer Society, Washington, DC, USA, pp 384–387*
[14] *Owens D (2010) Securing elasticity in the Cloud. Commun ACM 53(6):46–51*
[15] *OWASP (2010) The Ten most critical Web application Security risks.*
[16] *Zhang Y, Liu S, Meng X (2009) Towards high level SaaS maturity model: methods and case study. In: Services Computing conference. APSCC, IEEE Asia-Pacific, pp 273–278*
[17] *Chong F, Carraro G, Wolter R (2006) Multi-tenant data architecture. Online.*