Volume 8, No. 5, May-June 2017
ISSN No. 0976-5697
International Journal of Advanced Research in Computer Science
REVIEW ARTICLE
Available Online at www.ijarcs.info

Security Challenges Faced in Cloud Computing Environment

Eakta Kumari
School of Engineering and Technology
Central University of Haryana, India

Abstract: Cloud computing is a forthcoming revolution in information technology (IT) industry because of its performance, accessibility, low cost and many other luxuries. Cloud computing is a model to provide convenient, on-demand access to a shared pool configurablecomputing resources.It provides gigantic storage for data and faster computing to customers over the internet. This paper gives an overview of cloud computing, and discusses related security challenges and some techniques to deal with them. There are many approaches which can be used to improve the security but no one provides better solution.

Keywords: Cloud security, compliance, homomorphic encryption.

1. INTRODUCTION

Cloud Computing, in a simple words, means Internet based Computing. Since theInternet can be thought of as clouds, and therefore the term cloud computing is used[1].The concept of cloud computing is broader than that of utility computing andrelates to the underlying architecture in which the services are designed[5]. Cloudcomputing can be used to imply internal corporate data centers and utility services. It works on the principle that the user must pay according the time for which it is using the resources from various cloud providers. It is well known that it is not easy to handle large resources.

NIST (National Institute of Standards and Technology) defines cloud computingas follows: "*Cloud computing is a model for enabling ubiquitous, convenient,on-demand network access to a shared pool of configurable computing resources(e.g., networks, servers, storage, applications, and services) that can be rapidlyprovisioned and released with minimal management effort or service provider interaction"*.[2]

Cloud computing services such as Amazon EC2 and Google App Engine are built to take advantage of the already existing infrastructure of their respective company.
Cloud computing has several actors like Cloud Consumer, Cloud Provider, Cloud Auditor, Cloud Broker, Cloud Carrier. The combination of all these actors creates the architecture of Cloud Computing [14]. There are distinctively 3 components of the cloud:

Clients: Clients refer to the devices that the end users utilize to interface with the cloud when they require the services of the cloud. They can be personal computers, laptops, smart mobile phones etc.
Data Center: It is an agglomeration of servers where the application to which the users have subscribed is placed. It can be stored anywhere and can be accessed via the internet. A superior solution is to use virtual servers through a single physical server.
Databases: The information or data is stored at these places in the cloud. The storage units can consists of several servers stored in a single place like the Facebook's data storage or it can extend over a widespread area with several servers around the world connected with each other.

2. CLOUD COMPUTING ARCHITECTURE

There are three commonly-used cloud deployment models[3]: private, public, and hybrid. An additional model is the community cloud, which is less-commonly used.
Private cloud: It is appropriate for a single organization. This infrastructure is managed internally by the organization or by a third party and can be hosted internally and externally.
Public cloud:A public cloud is one in which the cloud infrastructure and computing resourcesare made available to the general public over a public network. A public cloud is owned by an organization selling cloud services, and serves a diverse pool of clients [15].
Hybrid cloud:A third type can be hybrid cloud that is a combination of computing resources provided by both private and public clouds in order to perform various functionality within the same organization[8].
Community cloud: shares computing resources across several organizations, and can be managed by either organizational IT resources or third-party providers[4].
Service Models
Once a cloud is established, how its cloud computing services are deployed in terms of business models can differ depending on
requirements. The primary service models being deployed are commonly known as:
Software as a Service (SaaS): Consumers purchase the ability to access and use an application or service that is hostedin the cloud. Microsoft is expanding its involvement in this area, and as part of the cloud computing option for Microsoft® Office 2010, itsOffice Web Apps are available to Office volume licensing customers and Office Web App subscriptions through its cloud-basedOnline Services,salesforce are some example of SaaS
Platform as a Service (PaaS): Consumers purchase access to the platforms, enabling them to deploy their own software andapplications in the cloud. The operating systems and network access are not managed by the consumer, and there might beconstraints as to which applications can be

deployed.Windows Azure Cloud Services,OrangeScape are the example of PaaS.

Infrastructure as a Service (IaaS): It is the use of fundamental computing resources, e. g. storage, networks, servers, to provide services to endusers.The end-users can deploy and run arbitrary software including both applications and operating systems. An exampleof IaaS is Amazon EC2[6]. The consumer does not control the underlying infrastructure, but can typically launch virtualmachines with chosen operating systems which in turn are managed by the consumer.

With its many advantages, cloud computing is currently being used in large corporationssuch as Google, Yahoo, Amazon, IBM, Whatsapp and Facebook. Cloud Computing is used by other companines for moving their applications to the cloud to reduce the investment and operational cost and to increase their business efficiency[7].

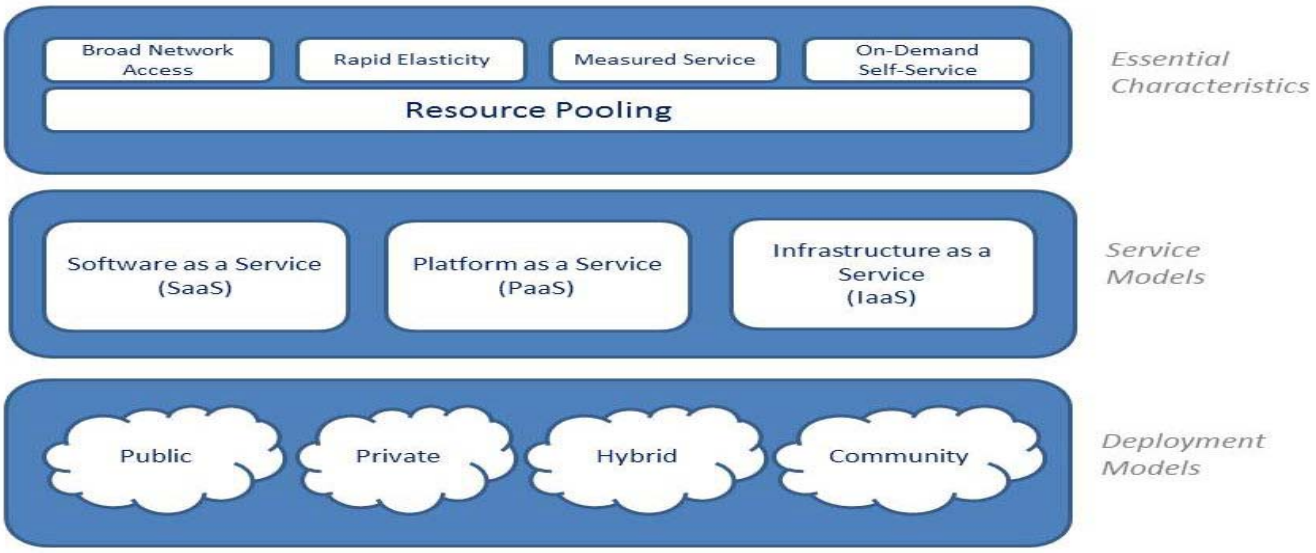

Fig1. Cloud definition framework

Cloud Characteristics

NIST define cloud computing essential characteristics[9][10] as follows:

1 **On-demand Self-service**: Cloud services are on-demand; that is, consumers can automatically request the service based on their needs, without human interaction with the service providers [16].

2 **Reduction of Cost** There are an umber of reasons to attribute Cloud technology with lower costs. The billing model is pay as per usage; the infrastructure is not purchased thus lowering maintenance. Initial expense and recurring expenses are much lower than traditional computing..

3 **Resource Pooling**: Cloud resources, such as storage, processing, memory, and network bandwidth are pooled to provide for multiple clients using a multi-tenant model, according to user's demand. Private cloud may only be offsite at a location controlled by the owner or the provider may allow clients to specify general server locations.

4 **Rapid Elasticity**: Services offered by cloud are rapidly provisioned, and in few cases by itself, rapidly released to quickly scale in. To consumer, the capabilities available for provisioning appears to be endless and could be purchased whenever required..

5 **Measured service:** Cloud Computing provides Mechanisms to measure service usage and health of the system. This enables
optimization of resources and provides transparency for both users and providers allowing better utilization of the service[16].

6. **Flexibility** Cloud computing mainly stress on deployment of applications in market as quickly possible , by using the most appropriate building blocks necessary for deployment.

7.**Broad Network Access**: A user can access the data shared on cloud fromany location across the globe

3. SECURITY CHALLENGES

Where is your data more secure, on your local hard driveror on high security servers in the cloud? Some argue that customer data is more secure when managed internally, while others argue that cloud providers have a strong incentive tomaintain trust and as such employ a higher level of security. Security challenges[12] in cloud computing are important issue for cloud service providers and cloud service cu stomers. Challenges usually are related information security because of data and application.

Resource location: end-users use the services provided by the cloud providers without knowing exactly where there sources for such services are located, possibly in other legislative domains. This poses a potential problem when dispute shappen, which is sometimes beyond the control of cloud providers. Data stored at the cloud service providers is not only affectedby the provider policies but also by the legislation of countrieswhere the providers reside. When using such services, users have to agree to the ''Terms of Service'' which grant theproviders the right to disclose user information in compliance with laws and law enforcement requests, for example, asnoted in the recent Dropbox's[11] terms of Service.

Multi-tenancy issue: this issue poses a challenge to protect user d ata against unauthorized access from other users runningprocesses o n t he s ame p hysical s ervers. T his i s i n fact n ot a new i ssue ta king into c onsideration th e c urrent concern withweb ho sting s ervices. H owever, with t he widespread u se o f cl oud co mputing an d with t he f act t hat users store moreimportant data in the cloud, this issue needs to be reconsidered seriously.

Authentication and trust of acquired information: As the critical d ata is lo cated in th e c loud p rovider in frastructure, the d atamay b e al tered without t he o wner's co nsent. T he modified da ta may t hen be retrieved an d processed b y t he owner tomake critical decisions. The authenticity of the data in t his ca se i s very i mportant, an d t herefore n eeds t o b e guaranteed.However, co mmon s tandards t o en sure d ata integrity do not exist.

System monitoring and logs: As more b usiness c ritical applications ar e migrated t o t he cl oud, cu stomers may request t hatcloud pr oviders provide m ore monitoring a nd log d ata f or t he cu stomers' p ersonnel. As t he r esults o f monitoring a nd l ogsmay c ontain s ensitive i nfrastructure information, a nd a re t raditionally u sed i nternally b y t he providers, s haring p arts o fsuch d ata t o ei ther cu stomers o r third-party e xaminers i s not something a ll c loud p roviders are willing to do. It willrequire a lot of negotiation between cloud providers and customers to come up with appropriate monitoring a nd l oginformation a s pa rt of a ny s ervice agreement.

4. MITIGATION OF SECURITY CHALLENGES

Firstly, cl oud co mputers' cu stomers f ind t he b est cl oud provider. E ach cl oud s ervice p rovider h as d ifferent d ata security and data management. Hence, customer determines requirements for cl oud s ervices t hen ch oose r ight cl oud provider. A lso, c loud pr ovider m ust h ave e xperience, standards and regulation about cloud service. Data transfer between cu stomers' n etwork an d cl oud i n t he Internet. Therefore, data must b e always travelling on a secure channel. HTTP is insecure due to s end d ata al l as p lain text.Attackers gain acces s t o w ebsite acco unts an d sensitiveinformation w ith m an-in-the-middle a nd eavesdroppingattacks. Connect to browser with HTTPS. Because everythingin the HTTPS message is encrypted with SSL. A lso, s tandardprotocols s hould be u sed f or authentication [13].User access control is important in cloud computer b ecauseof s ensitive an d p rivate d ata. O nly authorized p ersons s houldsee t he i nformation a nd pe rsons should be a uthorized u ntilthey n eed i t. C ustomers t o a sk service providers for specificsabout the people who manage their data and the level of accessthey have to it. All systems and n etwork c omponents' l og m ust be storedand m onitored so a s t o a nalyze unw anted e vents. Logging a ndmonitoring events i s t he p rocess o f a uditing. Auditing isimportant for analyzing e vents. Auditing is necessary toprovide s ecurity. Cloud c omputing c ustomers di scuss c loudprovider a bout monitoring logs day-to-day. In addition, theaudit log should be cen trally p reserved. Authentication an dauthorization should be don e f or pe ople t o m onitor t he auditlog.Unfortunately, a uditing is a p assive d efense because ofbecoming aware of critical security event after the occurrenceof the event. Auditing help people to response to unwantedeventquickly.

For providing data security we can encrypt the data with the help of f ully homomorphic e ncryption[17] [21] schemes. Fully homomorphic e ncryption i ncludes t o basic homomorphism t ypes. T hey a re m ultiply homomorphic encryption a lgorithm a nd a dditively h omomorphic encryption a lgorithm. Fully homomorphic e ncryption i s t o find an encryption algorithm, which can be any number of addition a lgorithm a nd multiplication algorithm in th e encrypted d ata. There a re va rious fully homomorphic algorithms like RSA[18] with padding, Elagamal[19] encryption, Pallier [20] encryption schemes.

5. CONCLUSION

In t his pa per, we di scuss a f resh t echnology: c loud computing. Describe its definition and some existing issues. There is no doubt that cloud computing is the development trend i n t he f uture. C loud c omputing p rovides us i nfinite computing capabilities service on demand, good scalability but also have challenges at security privacy legal issues and so o n. H owever s ecurity c hallenges ar e major problem f or enterprises. For that reason cloud computing customers must explore a ll c loud c omputing pr oviders w hen they de cide t o take c loud c omputing s ervice.This pa per i s t o provide a fundamental step towards the development of guidelines and standards for secure cloud computing environment.

6. REFERENCES

[1] Zaigham M ahmood a nd R ichard H ill, C loud C omputing f or enterprise architectures, Springer,2011

[2] Peter M ell a nd T im Grance,"The N IST definition o f c loud computing" 53(6):50, 2009. 7, 9

[3] http://en.wikipedia.org/wiki/Cloud_computing

[4] T. Dillon, Chen Wu, and E. Chang,"Cloud computing: Issues and challenges",
In 2 010 2 4th I EEE International C onference on A dvanced Information N etworking a nd A pplications (AINA), pa ges 27 {33, April 2010.

[5] Geva P erry. H ow cl oud a nd utility c omputing a re d ifferent, Feb 2008.

[6] Amazon. A mazon E lastic C ompute C loud(EC2). <http://aws.amazon.com/ec2/>.

[7] J oo L ee H ong .".Analysis of bus iness a ttributes in information technology e nvironments". J I nform P rocess S yst 2011;7(2):385–96.

[8] Yang Jianfeng,ChenZhi bin ,"Cloud c omputing r esearch a nd security i ssues", 201 0 I EEE international co nference o n advance information networking and application

[9] T. Dillon, C. Wu, and E. Chang, "Cloud Computing: Issues and Challenges," i n AdvancedInformation N etworking and Applications (AINA), 2010 24 th IEEE I nternational Conference , pp. 27–33.

[10] B. Grobauer, T. Walloschek, and E. Stocker, "Understanding Cloud Computing
Vulnerabilities," Security Privacy, IEEE, vol. 9, no. 2, pp. 50–57, Mar. 2011.

[11] ropbox's Blog. P rivacy, security & yourdropbox;2011.http://blog.dropbox.com/?p=735>[retrieved 25.04.11].

[12] ChunmingRong,S.T.Nguyen,M.G.Jaatun, "Beyond Lighting:Aservey on security challenges in cloud computing", Elsevier ;2012.

[13] EkenHamm,"Security T hreats a nd s olutions i n c loud computing".IEEE 2013.

[14] X. Li, X. Jiang, P. Huang, and K. Ye, \Dartcsim: An enhanced user-friendly cloud simulation system based on cloudsim with better pe rformance," i nCloud Computing a nd I ntelligent Systems (CCIS), 2 012 IE EE 2 nd In terna-tional C onference on, vol. 1, pp. 392{396, IEEE, 2012.

[15] A. L i, X. Y ang, S . K andula, and M . Z hang, \Cloudcmp: comparing publiccloud providers," in Proceedings of the 10th ACM S IGCOMM co nference o nInternet m easurement, p p. 1{14, ACM, 2010.

[16] R M adhubala. A n i llustrative s tudy on c loud c omputing. International j ournal of s oft computingand e ngineering, 1(6):286{290, 2012.

[17] Feng Z hao,ChaoLi,Chun Feng l iu,"*A cloud computing security solution based on fully homomorphic encryption*".feb,19,2014.

[18] R. L . R ivest, L . A dleman, a nd M . L . D ertouzos, \On d ata banks a nd privacy hom omorphisms," F oundations of s ecure computation, vol. 4, no. 11, pp. 169-180, 1978.

[19] T. E lGamal, \A publ ic k ey c ryptosystem a nd a s ignature scheme ba sed ondi screte l ogarithms," i n A dvances i n Cryptology, pp. 10{18, Springer, 1985.

[20] P. P aillier, \Public-key c ryptosystems ba sed on c omposite degree r esiduosityclasses," i n A dvances i n cryptologyEUROCRYPT99, pp. 223-238, Springer,1999.

[21] C. G entry, A fully hom omorphic e ncryption s cheme. P hD thesis, Stanford University, 2009.