Available online at http://www.journalcra.com

International Journal of Current Research
Vol. 8, Issue, 07, pp.34894-34898, July, 2016

INTERNATIONAL JOURNAL
OF CURRENT RESEARCH

ISSN: 0975-833X

RESEARCH ARTICLE

PRIVACY AND SECURITY ISSUES IN CLOUD COMPUTING

*,1Getaneh Berie Tarekegn, 2Gebreiziabher Abadi Maru and 3Habtamu Zelalem Liyew

1,2Department of Computer Science, Collage of Computing and Informatics, Assosa University, Assosa, Ethiopia
3Department of Information Technology, Collage of Computing and Informatics, Assosa University, Assosa, Ethiopia

ARTICLE INFO

Article History:
Received 25th May, 2016
Received in revised form
06th June, 2016
Accepted 28th July, 2016
Published online 31st July, 2016

Key words:

Privacy and Security,
Cloud Computing,
SaaS,
PaaS,
IaaS.

ABSTRACT

Today cloud computing is the most trending and advanced technology with high future implementation in the information and technology industries. Nowadays many cloud storages or online storages are provided by a number of companies to their customers as well as to the employees. In current scenario computing infrastructure is rapidly moving towards the cloud based architecture in which the users are enabled to move their data and application software to the network and access the services on-demand. It is a flexible, cost-effective, and proven delivery platform for providing business or consumer IT services over the Internet. Cloud computing is the most crucial research area that has many potential advantages and many enterprise applications and data are migrating to public, private or hybrid cloud. Cloud Computing has the advantage of reducing cost by sharing computing and storage resources, combined with an on-demand provisioning mechanism relying on a pay-per-use business model in both acadamic and industry. But regarding some business-critical applications, the organizations, especially large enterprises, still wouldn't move them to cloud, because, without appropriate privacy and security solutions designed for clouds, it is difficult to use cloud computing by acadamic, industries, governmental organizations, healthcare sectors or other concerned units. The primary contribution of our work is to provide a better understanding of the cloud computing, to assess how privacy and security issues occur in the context of cloud computing and discuss the mechanisms to be addressed those issues in cloud computing.

Citation: Getaneh Berie Tarekegn, Gebreiziabher Abadi Maru and Habtamu Zelalem Liyew, 2016. "Privacy and security issues in cloud computing", *International Journal of Current Research*, 8, (07), 34894-34898.

INTRODUCTION

Just a few years ago, people used to carry their documents around on disks. Then, more recently, many people switched to memory sticks. Cloud computing refers to the ability to access and manipulate information stored on remote servers, using any Internet-enabled platform, including smartphones. There is as yet no single, commonly-agreed definition of "cloud computing". The United States National Institute of Standards and Technology (NIST, http://csrc.nist.gov) has defined it as follows (Mell and Grance, 2009): Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three delivery models, and four deployment models. Recent developments in the field of could computing have immensely changed the way of computing as well as the concept of computing resources. In a cloud based computing infrastructure, the resources are normally in someone else's premise or network and accessed remotely by the cloud users (Petre, 2012; Ogigau-Neamtiu, 2012; Singh and jangwal, 2012). Processing is done remotely implying the fact that the data and other elements from a person need to be transmitted to the cloud infrastructure or server for processing; and the output is returned upon completion of required processing. In some cases, it might be required or at least possible for a person to store data on remote cloud servers. These gives the following three sensitive states or scenarios that are of particular concern within the operational context of cloud computing:

- The transmission of personal sensitive data to the cloud server,

Corresponding author: Getaneh Berie Tarekegn,
Department of Computer Science, Collage of Computing and Informatics, Assosa University, Assosa, Ethiopia.

- The transmission of data from the cloud server to clients' computers and
- The storage of clients' personal data in cloud servers which are remote server notowned by the clients.

All the above three states of cloud computing are severely prone to security breach that makes the research and investigation within the privacy and security aspects of cloud computing practice an imperative one.

Cloud computing has several advantages among them reduce implementation and maintenance costs, increased mobility for a global workforce, flexible and scalable infrastructure, quick time to market and increased availability of high performance applications to small or medium sized businesses.

Advantages of cloud computing

Cloud computing offers the following major advantages to the users.

- The 3rd party provider owns and manages all the computing resources (servers, software, storage, and networking) and electricity needed for the services. The users only need to "plug into" the cloud. The users do not need to make a large upfront investment on computing resources; the space needed to house them; electricity needed to run the computing resources; and the cost of maintaining staff for administering the system, network, and database.
- The users can increase or decrease the level of use of the computing resources and services flexibly and easily.
- The users pay most likely much less for the services, because they pay only for the computing resources and services they use, and the subscription-based or pay-per-use charges are likely much lower than the cost of maintaining on-premises computing resources. If the users are to maintain on-premises computing resources, they also need to make the worst-case plan to account for the occasional or seasonal peak needs.
- The users can in practice access the cloud for services anytime from anywhere.

Essential Characteristics of Cloud Computing

It state that Cloud Computing allows business to increase IT capabilities on the fly and in real time i.e., Internet-enabled, without investing in new infrastructure, training new personnel or licensing new software, and as a pay-per-use service.

A.On-demand self-service

- It refers to the service provided by cloud computing vendors that enables the provision of cloud resources on demand whenever they are required.
- The user accesses cloud services through an online control panel.
- Example: The public providers like Amazon, Google, and Microsoft have this facet, smaller niche providers typically do not.

B. Broad network access

- It refers to resources hosted in a private cloud network that are available for access from a wide range of devices, such as tablets, PCs, Macs and smart phones.
- These resources are also accessible from a wide range of locations that offer online access
- These can include, Laptop, Desktop, Smartphone, Tablet device, and so on.

C.Resource pooling

- It means that customers draw from a pool of computing resources, usually in remote data centers. Services can be scaled larger or smaller; and use of a service is measured and customers are billed accordingly (2)
- Typically, user organizations of similar security levels or needs are grouped together on a particular community cloud offering all federal organizations, all pharmaceutical organizations, all general availability organizations
- Examples: Storage, processing, memory, network bandwidth, and virtual machines.

D.Rapid elasticity

- The major characteristics that set cloud computing apart from traditional datacenter computing.
- Multiple tenants that share components of a shared resource pool (and in the case of a private cloud, all the tenants are part of a single corporate entity). Your tenants use the networking, compute and storage assets in the shared pool, and then return them to the pool when they no longer need those assets. They can also get more resources from the shared pool if and when they need to – but when they no longer need these additional resources, they return them to the pool. In a well architected cloud, the acquisition and release of assets from and to the shared pool would be automated, based on service demands and driven by an intelligence policy.

E. Measured services or usage

- It is simply called as ***Pay per use*** i.e., consumers are charged fees based on their usage of a combination of computing power, bandwidth use and/or storage
- Services can be scaled larger or smaller and use of a service is measured and customers are billed accordingly.
- Example: companies sell power to subscribers, telephone companies sell voice and data services, IT services such as network security management, data center hosting or even departmental billing can now be easily delivered as a contractual service

F.Multi Tenacity

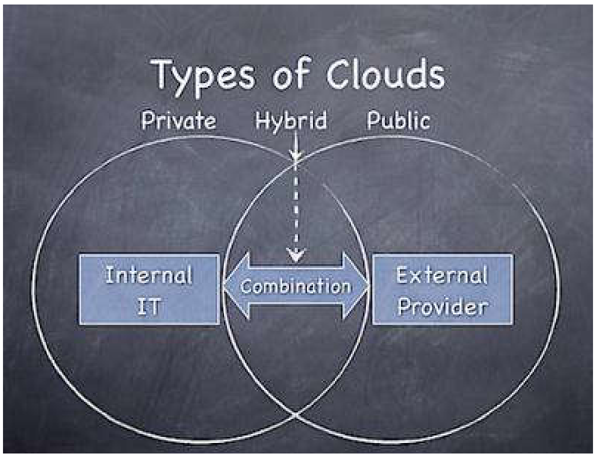
- It is a critical technology to allow one instance on application to serve multiple customers by sharing resources.

- It needs policy-driven enforcement, segmentation, isolation, governance, service levels, and chargeback/billing models for different consumer constituencies.
- The user might utilize a public cloud provider's service offerings or actually be from the same organization, such as different business units rather than distinct organizational entities, but would still share infrastructure.

Types of Cloud

Cloud computing is typically classified in two ways (http://thecloudtutorial.com/cloudtypes.html), location of the cloud computing and type of services offered.

Classification based upon location



Public cloud

A public cloud is one in which the infrastructure and other computational resources that is comprises are made available to the general public over the internet. It is owned by a cloud provider selling cloud services and, by definition, is external to an organization. In this model, no access restrictions can be applied and no authorization and authentication techniques can be used. Public cloud providers such as Google or Amazon offer an access control to their clients. Examples of a public cloud includes Microsoft Azure, Google App Engine.

Private cloud

It is used to deliver services to individual or personal users from databases designed for business data. Such type of services is flexible as well as convenient while maintaining its original control security and managerial aspects. Private cloud can be owned or leased and managed by the organization or a third party and exist at on-premises or off-premises. It is more expensive and secure when compared to public cloud. In private cloud there are no additional security regulations, legal requirements or bandwidth limitations that can be present in a public cloud environment, by using a private cloud, the cloud service providers and the clients have optimized control of the infrastructure and improved security, since user's access and the networks used are restricted. One of the best examples of a private cloud is Eucalyptus Systems (Kandukuri *et al*., 2009).

Hybrid cloud

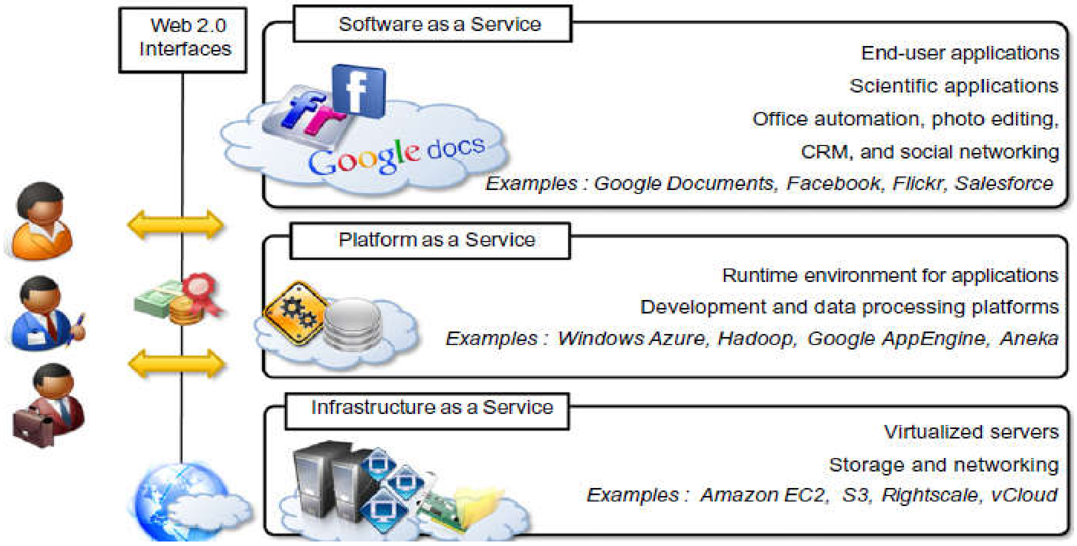
It is the mixture of private as well as public cloud. Generally, organizations run all the applications have the requirements of both public and private clouds. On private clouds important and secure applications are executed while public clouds are used for lengthy tasks and they run as and when required. An example of a Hybrid Cloud includes Amazon Web Services (AWS).

Classification based upon service provided

The term services in cloud computing is the concept of being able to use reusable, fine-grained components a cross a vendor's network. This is widely known as "as a service". Based upon the services offered, clouds are classified in the following ways.

Infrastructure as a service (IaaS)

IaaS is a model of software deployment where by the basic computing infrastructure of servers, software, and network equipment is provided as an on-demand service upon which a platform to develop and execute applications can be established. Its main purpose is to avoid purchasing, housing, and managing the basic hardware and software infrastructure components, and instead obtain those resources as virtualized objects controllable through a service interface.


Web 2.0 Interfaces
Software as a Service
End-user applications
Scientific applications
Office automation, photo editing,
CRM, and social networking
Examples : Google Documents, Facebook, Flickr, Salesforce
Google docs
Platform as a Service
Runtime environment for applications
Development and data processing platforms
Examples : Windows Azure, Hadoop, Google AppEngine, Aneka
Infrastructure as a Service
Virtualized servers
Storage and networking
Examples : Amazon EC2, S3, Rightscale, vCloud

The cloud subscriber generally has broad freedom to choose the operating system and development environment to be hosted. Infrastructure as a service provides companies with computing resources including servers, networking, storage, and data center space on a pay-per-use basis. Infrastructure as a service (IaaS) refers to the sharing of hardware resources for executing services using Virtualization technology. Its main objective is to make resources such as servers, network and storage more readily accessible by applications and operating systems. Thus, it offers basic infrastructure on-demand services and using Application Programming Interface (API) for interactions with hosts, switches, and routers, and the capability of adding new equipment in a simple and transparent manner. In general, the user does not manage the underlying hardware in the cloud infrastructure, but he controls the operating systems, storage and deployed applications. The service provider owns the equipment and is responsible for housing, running and maintaining it. The client typically pays on a per-use basis. Its main purpose is to avoid purchasing, housing, and managing the basic hardware and software infrastructure components, and instead obtain those resources as virtualized objects controllable via a service interface. Examples of IaaS providers include Amazon Elastic Cloud Computing (EC2), S3, Go Grid, 3 Tera and Flexi Scale (Agarwal and Agarwal, 2011).

Platform as a Service (PaaS)

Platform is an environment that provides services on which other higher user- oriented applications can be created and executed, for example, a web site developer develop its own application and share space on internet to deploy its website by paying certain amount. PaaS is a model of software deployment where by the computing platform is provided as on-demand service upon which applications can be developed and deployed. Its main purpose is to reduce the cost and complexity of buying, housing and managing the underlying hardware and software components of the platform, including any needed program and database development tools. The development environment is typically special purpose, determined by the cloud provider and tailored to the design and architecture of its platform. The cloud subscriber has control over application environment settings of the platform. Security provisions are split between the cloud provid3r and the cloud subscriber.

PaaS is the delivery of a computing platform and solution stack as a service without software downloads or installation for developers, IT managers or end-users. It provides an infrastructure with a high level of integration in order to implement and test cloud applications. The user does not manage the infrastructure (including network, servers, operating systems and storage), but he controls deployed applications and, possibly, their configurations. Examples of PaaS includes: Force.com, Google App Engine and Microsoft Azure.

Software as a service (SaaS)

SaaS is a model of software deployment whereby one or more applications and the computational resources to run them are provided for use on demand as turnkey service. Its main purpose is to reduce the total cost of hardware and software development, maintenance, and operations. Security provisions are carried out mainly by the cloud provider. The cloud subscriber does not manage or control the underlying cloud infrastructure or individual applications, except for preference selections and limited administrative application settings. It means sharing the applications of the users of that cloud along with data as and when demand is generated. Single instance of a service can run on shared cloud and multiple instances run at end users platform. SaaS can be described as a process by which Application Service Provider (ASP) provide different software applications over the Internet. This makes the customer to get rid of installing and operating the application on own computer and also eliminates the tremendous load of software maintenance; continuing operation, safeguarding and support (Grossman, 2009). SaaS vendor advertently takes responsibility for deploying and managing the IT infrastructure (servers, operating system software, databases, data center space, network access, power and cooling, etc.) and processes (infrastructure patches/upgrades, application patches/upgrades, backups, etc.) required to run and manage the full solution. SaaS features a complete application offered as a service on demand. Examples of SaaS includes: Salesforce.com, Google Apps.

Security and Privacy Issues Related to Cloud Computing

Cloud computing and storage solutions provide users and enterprises with various capabilities to store and process their data in third-party data centers.

Table 1. Comparison between the three services

IaaS	PasaS	SaaS
In this services storage, database management and compute capabilities area offered.	This service provides design, development, build and test applications.	This is internet based application and offers the services to end-user.
Services:- Computing infrastructure is rented to the user	Services:- Enables developers to write applications without installing any tools in local system but run on the cloud.	Services:- Software is offered as Service and delivered through a browser
Example:- Infrastructure Scalability & Availability	Example:- *Scripting Coding* Coding and integration	Example:- *Excel, Web Page, CRM, ERP* Access, SQL Server
Providers:- Amazon AWS, Go Grid, 3 Tera, Sun Grid, SAVVIS, Windows.	Providers:- Google's App Engine, Force.com, Amazon AWS, IBM, NetSuite, Microsoft, Windows Azure,	Providers:- Google Docs, Salesforce.com, Microsoft, Gmail.com, WebEx.
Advantage:- *Scalability,* *Pay as you go* Best-of-breed technology and resources	Advantage:- *Scalability,* *Reliability and security* Pay-per-use	Advantage:- *Reduce the cost* Centralized control

Organizations use the Cloud in a variety of different service models (SaaS, PaaS, and IaaS) and deployment models (Private, Public and Hybrid). There are a number of security concerns associated with cloud computing. These issues fall into two broad categories: security issues faced **bycloud providers** (organizations providing software-, platform-, or infrastructure-as-a-service via the cloud) and security issues faced **bytheir customers** (companies or organizations who host applications or store data on the cloud). The responsibility is shared, however. The provider must ensure that their infrastructure is secure and that their clients' data and applications are protected while the customer must ensure that the provider has taken the proper security measures to protect their information. Security has always been the main issue for IT Executives when it comes to cloud adoption. However, cloud computing is an agglomeration of technologies, operating systems, storage, networking, virtualization, each fraught with inherent security issues. Cloud computing is an emerging technology with shared resources, lower cost and rely on pay per use according to the user demand. Due to many characteristics it has effect on IT budget and also affect security and privacy. All these issues are discussed here (Alvi and Chaudhary).

Privacy issue

It is the human right to secure his private and sensitive information. The data privacy is also one of the key concerns for Cloud computing. A privacy steering committee should also be created to help make decisions related to data privacy. This committee will ensure that your organization is prepared to meet the data privacy demands of its customers and regulators. Data in the cloud is usually globally distributed which raises concerns about jurisdiction, data exposure and privacy. Organizations stand a risk of not complying with government policies as would be explained further while the cloud vendors who expose sensitive information risk legal liability (Rabi Prasad Padhy and Manas Ranjan Patra, 2011). The key challenge for software engineers to design cloud services in such a way as to decrease privacy risk and to ensure legal compliance. The following tips are recommended for cloud system designers, architects, developers and Testers.

- Minimize personal information sent to and stored in the cloud.
- Protect personal information in the cloud.
- Maximize user control.
- Specify and limit the purpose of data usage.
- Provide feedback

Security

Public cloud increases the privacy issue and very much concern about security. Some of them are described below:

Access

It has the threat of access sensitive information. The risk of data theft from machine has more often occur in cloud system. Some useful data stored in cloud for a long time can be hacked by the hacker.

Conclusion

Cloud computing is a growing area of concern in the IT security community. Basically, cloud computing is storing the data on someone else's computer and accessing it via a network. Many companies, such as Google.com, Amazon.com, Microsoft, Oracle/Sun, Canonical/Eucalyptus and many other vendors accelerate their paces in developing Cloud computing systems and enhancing their services to provide for a larger amount of users. However, security and privacy issues present a strong barrier for users tco adapt into Cloud computing systems. This work gives an overview regarding characteristics, security-architecture, and threats and existing solutions.

Acknowledgment

The Authors would like to thank Assosa University by providing full time internet service to do this research and development. And also would like to thank the reviewers for their constructive comments.

REFERENCES

Agarwal, A. and Agarwal, A. 2011. The Security Risks Associated with Cloud Computing, *International Journal of Computer Applications in Engineering Sciences*, vol 1 (Special Issue on CNS), pp. 257-259.

Alvi F. A. and B.S Chaudhary," review on cloud computing security issues &challenges".

Grossman, R. L. 2009. "The Case for Cloud Computing," IT Professional, vol. 11(2), pp. 23-27, ISSN: 1520-9202.

http://thecloudtutorial.com/cloudtypes.html.

http://thecloudtutorial.com/related.html.

Kandukuri B. R., R. Paturi V, A. Rakshit, 2009. "Cloud Security Issues", In Proceedings of IEEE International Conference on Services Computing, pp. 517-520.

Mell, P. and Grance, T. 2009. NIST Definition of Cloud Computing. Retrieved from NISTwww.nist.gov/itl/cloud/upload/cloud-def-v15.pdf.

Rabi Prasad Padhy, Manas Ranjan Patra, Suresh Chandra Satapathy "Cloud Computing: Security Issues and Research Challenges", *International Journal of Computer Science and Information Technology & Security (IJCSITS),* Vol. 1, No. 2, December 2011

****