IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727
PP 21-24
www.iosrjournals.org

VARIOUS SECURITY ISSUES IN CLIENT SIDE CLOUD COMPUTING

Ms. Punam R. Naphade, Dr. Girish Katkar
vrushita1@gmail.com, RAICSIT, Wardha, India
girishkatkar2007@rediffmail.com, Taywade College, Koradi, Nagpur, India

Abstract: *Cloud Computing (CC) is an emerging computing paradigm that provides large amount of computing and storage to the Clients provisioned as a service over the internet in a pay-as you-go pricing model, where the Clients pay only according to the usage of their services. In Cloud Computing, the feature of multi-tenancy gives privacy, security, access control, authentication, authorization challenges, because of sharing of physical resources among un-trusted tenants so, a suitable technique with proper management should be applied before outsourcing the data and updating of data. Thus this research is focusing on the existing client side security mechanism in cloud computing in compare with the existing technique and try to proposed new and advanced technique on client side to enhance the client side security*
Keywords: *IaaS, PaaS, Saas, Vulnerability, Sustainable, OAuth, SAML etc.*

I. INTRODUCTION

Cloud computing is a model for convenient and on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management. In simple words, Cloud Computing is the combination of a technology, platform that provides hosting and storage service on the Internet. Main goal of the cloud computing is to provide scalable and inexpensive on-demand computing infrastructures with good quality of service levels. Many companies developing and offering cloud computing products and services but have not properly considered the implications of processing, storing and accessing data in a shared and virtualized environment. In fact, many developers of cloud-based applications struggle to include security. In other cases, developers simply cannot provide real security with currently affordable technological capabilities.

Cloud computing is sharing of resources on a larger scale which is cost effective and location independent. Resources on the cloud can be used by the client and deployed by the vendor such as amazon, google, ibm, salesforce, zoho, rackspace, microsoft. It also shares necessary software's and on-demand tools for various IT Industries. Benefits of Cloud computing are enormous. The most important one is that the customers don't need to buy the resource from a third party vendor, instead they can use the resource and pay for it as a service thus helping the customer to save time and money. Cloud is not only for Multinational companies but it's also being used by Small and medium enterprises.

II. WHAT IS CLOUD COMPUTING?

The official definition from the National Institute of Standards and Technology reads:"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." Cloud computing differs from the classic client-server model by providing applications from a server that are executed and managed by a client's web browser, with no installed client version of an application required. As further defined, Cloud Computing refers to the use and access of multiple server-based computational resources via a digital network to access the World Wide Web.

Services provided by cloud

Cloud Computing is a general term that provides hosted services over internet. Broadly speaking, these services are divided into three categories:

Infrastructure-as-a-Service (IaaS),
Platform-as-a-Service (PaaS)
Software-as-a-Service (SaaS).

IaaS refers to the sharing of hardware resources. The resources are all virtual machines, which has to be managed**.**

E.g. Amazon Ec2, Right Scale.

PaaS aims to protect the data, which is especially important in case of storage as a service.

E.g. Amazon SSS, Microsoft Azure.

SaaS provides different type of application and web services to the end users.

E.g. google , Sales-force.

TYPES OF CLOUD

There are basically four types of clouds, which are described below-

Public cloud: This is the one of the cloud in which cloud services are being available to users via a service provider over the Internet. It provides a control mechanism for them. The services may be free or offered on a pay-per usage model.

Private Cloud: This provides many of the benefits of public, but the main difference among two is that the data is managed properly within the organization only, without the limits of network bandwidth.

Community Cloud: This type of cloud is basically managed by group of originations that have a common objective to achieve. The members share access to the data in the cloud.

Hybrid Cloud: This is the combination of public as well as private cloud. It can also be defined as multiple cloud systems that are connected in a way that allows programs and data to be moved easily from one system to another.

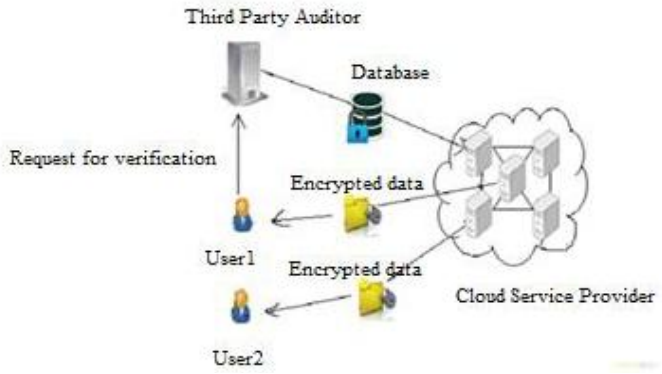
SECURITY ISSUE IN SAAS SECTION OF CLOUD COMPUTING

Security is a big challenge in cloud system due to its nature of outsourced computing. Mainly, confidentiality, integrity and authentication are the primary pain areas. Unless robust security scheme and user-centric security policy is implemented, cloud system would be vulnerable to different attacks and susceptible by the users.

Below we mention the key issues of ensuring the cloud security

Confidentiality prevents intentional (malicious) or unintentional disclosure of sensitive information. In cloud systems, confidentiality incorporates data encryption to minimize vulnerability due to covert channels, traffic analysis, and sensitive inference.

Currently, authentication, authorization and access control services are provided using OpenID, OAuth, SAML, XACML in SaaS section of cloud computing. However, XACML has the capability of attribute based access control, which is most suitable in cloud at Saas environment.



SECURITY CHALLENGES OF CLIENT/USER IN CLOUD COMPUTING.

One of the primary focuses to provide cloud security is to have one integrated solution enabling the required security primitives like confidentiality, authentication. Cloud security cannot be solved using conventional it security tools as private data is migrated from local Machines to global or distributed systems for storage, processing and computing. It is required to Consider cloud security from a holistic point of view rather than solving the problem requirement Basis. It is described that cloud specific security solutions like confidentiality-enabled Computing, user-defined authentication and access control are the main Issues to be addressed for a sustainable and scalable cloud computing.

TRADITIONAL SECURITY CHALLENGES

Some of the traditional security issues which also affect the SaaS model have been described below:

Data confidentiality

Confidentiality refers to the prevention of intentional or unintentional unauthorized disclosure of information. Confidentiality in cloud system is related to the areas of intellectual property rights, covert channels, traffic analysis, encryption, and inference. Cloud computing involves the sharing or storage of information on remote servers owned or operated by others, while accessing through the Internet or any other connections. Cloud computing services exist in many variations, including data storage sites, video sites, tax preparation sites, personal health record websites and many more. The entire contents of a user's storage device may be stored with a single cloud provider or with multiple cloud providers. Whenever an individual, a business, a government agency, or any other entity shares information in the cloud, privacy or confidentiality questions arise.

Authentication and authorization

The authentication and authorization applications for enterprise environments may need to be changed, to work with a safe cloud environment. Forensics tasks may become much more difficult since the investigators may not be able to access system hardware physically. The model proposed in the literature verifies user authenticity using two-step verification, which is based on password, smartcard and out of band (i.e. strong two factors) authentication. In addition, the scheme also provides mutual authentication, identity management, session key establishment, user privacy and security against many popular attacks; however the formal security proofing hasn't yet been formalized.

Availability

The availability ensures the reliable and timely access to cloud data or cloud computing resources by the appropriate personnel. The availability of cloud service providers is also a big concern, since if the cloud service is disrupted; it affects more customers than in the traditional model. For instance, the recent disruption of the Amazon cloud service in the year 2011, took down a number of websites including Reddit, Foursquare, and Quora. The SaaS application providers are required to ensure that the systems are running properly when needed and enterprises are provided with services around the clock. This involves making architectural changes at the application and infrastructural levels to add scalability and high availability. Resiliency to hardware/software failures, as well as to denial of service attacks, needs to be built from the ground up within the application. At the same time, an appropriate action plan for business continuity and Disaster Recovery (DR) needs to be considered for any exigencies as per the guidance provided.

Data Access

Data access issue is mainly related to security policies provided to the users while accessing the data. In a typical scenario, a small business organization can use a cloud provided by some other provider for carrying out its business processes. This organization will have its own security policies based on which each employee can have access to a particular set of data. The security policies may entitle some considerations, wherein, some of the employees are not given access to certain amount of data. These security policies must be adhered by the cloud to avoid intrusion of data by unauthorized users. The SaaS model must be flexible enough to incorporate the specific policies put forward by the organization. The model must also be able to provide organizational boundary within the cloud because multiple organization will be deploying their business processes within a single cloud environment

REFERANCES

[1]. Wolf Halton, "Security Solutions for Cloud Computing" July 15, 2010.
[2]. Henry J. Sienkiewicz, "Cloud Computing: A perspective" Defense Information Systems Agency - April 2009.
[3]. Privacy in the Cloud Computing Era: A Microsoft Perspective - November 2009.
[4]. Bharat Bhargava, Anya Kim, YounSun Cho, "Research in Cloud Security and Privacy" .
[5]. Ponemon Institute and CA "Security of cloud computing Users: A study of Practitioners in the US & Europe". May 12, 2010.
[6]. Ponemon Institute LLC and CA Technologies, "Security of Cloud Computing Providers Study" - April 2011.
[7]. Brian Hay, Kara Nance, Matt Bishop, "Storm Clouds Rising: Security Challenges for IaaS Cloud Computing" Proceedings of the 44th Hawaii International Conference on System Sciences -2011.
[8]. John C.Mace, Aad van Moorsel, Paul Watson, "The Case for Dynamic Security Solutions in Public Cloud Workflow Deployments" School of Computing Science & Centre for Cybercrime and Computer Security (CCCS) Newcastle University, Newcastle upon Tyne, NE1 7RU, UK.
[9]. Qiang Guo, Dawei Sun, Guiran Chang, Lina Sun, Xingwei Wang, "Modeling and Evaluation of Trust in Cloud Computing Environments" School of lnformation Science and Engineering, Northeastern University, Shenyang, P.R. China, Computing Center, Northeastern University, Shenyang, P.R. China, 2011 3rd International Conference on Advanced Computer Control (ICACC 2011).
[10]. R Buyya, Y. Chee Shin, S. Venugopal, J. Broberg and I. Brandic, "Cloud computing and emerging IT platforms: vision, hype, and reality for delivering computing as the 5th utility," Future Generation Computer Systems, vol. 25(6), Jun. 2009, pp. 599-616.