International Journal of Research Studies in Computer Science and Engineering (IJRSCSE)
Volume 1, Issue 6, October 2014, PP 1-5
ISSN 2349-4840 (Print) & ISSN 2349-4859 (Online)
www.arcjournals.org

Security Aspects in Cloud Computing

Birkeshwar Prasad Singh

M. Tech (Weekend) Student,
Department of Computer Engineering
Manav Rachna international university,
Faridabad (Haryana,India)
birkeshwar@rediffmail.com

Abstract: *The purpose of this paper is to study various security aspects in Cloud Computing. It is a service delivery system which provides computing services including storage of data to users in all sectors through internet or private networks. In this paper, we explore security threats associated with cloud computing and related privacy issues. We will also explore the strategies for better Cloud security.*

Keywords: *Cloud Computing; Cloud service model; Security; Privacy***;** *Encryption.*

1. INTRODUCTION TO CLOUD COMPUTING

Cloud Computing is broader concept of converged infrastructure and shared services [1]. Basically it is a service of computing techniques rather than a product. The word "**Cloud**" indicates focus of maximizing the advantages of shared resources. Resources involved in Cloud are usually not only shared by multiple users but are also dynamically reallocated per user's requirements.

Cloud Computing integrates a number of technologies, including multi-tenant application hosting, resource scheduling, memory management, transaction management, server virtualization etc. Here, the computing power belongs to Internet or private networks and subscribers access this power as per their requirements via the Internet/private networks.

The NIST Definition of Cloud Computing [2]

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 rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models. [2]

A Cloud Deployment Models

Public Cloud - Any person can access a public cloud with membership subscription and the way to access the cloud space is a network connection. Generally public clouds are run by third parties, and applications from different subscribers are likely to be mixed together on the cloud's servers, storage systems, and networks.

Private Cloud - A private cloud is run by a specific group or organization and limits access to just that group. These clouds are built for specific purpose of one client/group/organization. These clouds provide full control over data, security, and quality of service, even the organization owns the cloud infrastructure and keeps full control over deployment of cloud applications. Deployment of a private cloud can be in an enterprise datacenter also.

Community Cloud – Cloud shared among two or more organizations that have similar requirements is termed as Community Cloud.

Hybrid Cloud - A combination of at least two different clouds can be termed as Hybrid Cloud, that means these clouds are a mixture of public, private, or community clouds.

B Cloud Service Models

The cloud computing is on-demand service delivery system which gives computing capabilities as per requirement automatically. This service delivery system can be utilized through many instruments/devices/machines such as desktop, laptop, PDA, mobile phone, Tabs etc. The cloud service model include mainly three types: SaaS (Software as a Service), PaaS (Platform as a Service) and IaaS (Infrastructure as a Service). These models are described below in brief:

Software as a Service - In this model, provider gives authority for accessing both resources and applications to subscribers. This model provides the facility to subscribers to install all the required software on Cloud and can access the software by all of their personal devices through network or internet connection. Here, subscribers do not need to have a physical copy of software to install on the devices. In agreement with SaaS provider, subscribers get least control over the cloud.

Platform as a Service - In this model, subscriber goes a level up in terms of control over cloud above the Software as a Service model. Here, a PaaS provider gives authority to subscriber at the component level access so that they can develop and operate cloud applications as per requirements over the internet/computer network. In agreement with PaaS provider, subscribers get more control over the cloud in respect of SaaS model.

Infrastructure as a Service - In this model, subscribers gets maximum control over cloud. Here, an IaaS provider deals primarily with computational infrastructure. In agreement with IaaS provider, the subscriber completely outsources the storage and resources, such as hardware and software, that they need.

2. SECURITY AND PRIVACY ISSUES

Basically, in cloud data storage system, users store their data in the cloud and no longer possess the data locally. Thus, correctness and availability of the data files being stored on the distributed cloud servers must be guaranteed. One of the key issues is to effectively detect any unauthorized data modification and corruption, possibly due to server compromise and/or random cloud system breakdown. Besides, in the distributed case when such inconsistencies are successfully detected, to find which server the data error lies in is also of great significance, since it can be the first step to fast recover the storage errors.

There are a lot of security issues for cloud computing apart from data security. Main reason is that it involves many technologies like different type of computer networks, operating systems and database techniques. Thus, security and privacy issues related to these systems and technologies are also applicable to cloud computing system. Therefore, the network that interconnects these systems in a cloud has to be ensured about its security.

The security issues in cloud computing can be categorized into the following three broad classes:

I Common attack vectors to Cloud: These security issues are Virtual Machine level attacks, vulnerabilities related with cloud service providers, or phisers. Normally a cloud provider use virtual machines and a hypervisor to separate customers. Vulnerabilities in the hypervisor or VM technology used by cloud service providers are a potential threat to cloud security. Normally Cloud service providers use sophisticated monitoring tools like firewalls to mitigate these VM-level vulnerabilities.

II Cloud data availability to user: Here, concerns center on critical cloud applications and data being available to subscribers. Here, maintaining the cloud system uptime, 'Distributed denial of service' attacks prevention and robustness of computational integrity are major issues.

III Legal issues related to data control: In cloud storage system, a user stores his data in the cloud, it means that the stored data do not exist locally. This storage of data can be held by many parties. Here, a potential lack of control and transparency exists because the legal implications of data and applications being held by a third party are very complex and it varies as per country rules and regulations.

There are some additional security threats that are relevant in cloud computing and are being detected and researched by academia, security organization and both cloud service providers and the cloud customers which are given below:

Distributed denial of Service Attacks [3] : These threats are associated with network layer distributed attacks flooding infrastructure with excessive traffic in order to cause critical components to fail or to consume all available hardware resources. Shared resource consumption and VM & hypervisor exploitation are example of DoS attacks.

Data leakage through hypervisor or VM instances: It causes data leakage across co-resident virtual machine instances. Here, attackers act as a rogue customer within a shared cloud infrastructure to access other customers' data.

Attack using personal data available on social networking sites: Giant popularity of business and personal social networking sites give greater advantages to attackers to access personal and important data to target user they know and the online social network they use. Attackers can setup identities to gain trust, and use online information to determine relationships and roles of target user to prepare their attacks. A combination of technical attack and social engineering attacks can be deployed against a target user by taking advantage of social networking data.

Attacks on mobile devices: These attacks are now emerging. It target to mobile devices and rely on features traditionally associated with laptops and desktops, including rich application programming (APIs) that support network communications and background services, target user wireless Internet presence, and large local data storage capabilities. As mobile devices now have greater features equivalent to desktops, Internet-based spyware, worms or even physical attacks are more likely to occur against mobile devices, as they are potentially a less risky target to an attacker that wishes to remain undetected. Actual fact is that most mobile devices do not have the equivalent security features enabled, or in some case available.

Unauthorized data mining for Commercial purpose: It is well known that companies like Google uses its cloud infrastructure to collect and analyze consumer data for its advertising network. The availability of data and cheap data mining techniques has high impact on the privacy of user data. The attackers have massive and centralized databases available for analysis and also the raw computing power to mine these databases which compromise the cloud security.

Organized crimes: Cloud providers store a range of different data types, including credit card information, other financial and personal data. All of these data can be aggregated from multiple customers and therefore it can be extremely valuable to criminals. There is a risk that insiders are deliberately used to gain access to customer data and probe systems in order to assist any external attackers that require additional information in order to execute complex Internet-based attacks.

3. POSSIBLE STRATEGIES OF CLOUD SECURITY

For security of data in cloud, cryptographic mechanisms are best methods. Other option for protecting data is Software encryption, but it reduces the speed of process and it is less secure also. Apart from this, there is also chance of theft of encryption key without being detected. For data security in transit period, encryption can be counted as best option. In addition, strong authentication and data integrity protection mechanisms must be applied so that it must ensure that data only reach to right place in right form through right path and must not modified during transit. Strong authentication is the essential requirement to access control for user and data both. Thus strong authentication and access control becomes more important for the cloud user. When a subscriber's access privilege gets revoked or reassigned, the subscriber's identity management system must notify the cloud service provider in real-time basis so that the subscriber's cloud access can also be revoked simultaneously or within a very short span of time.

Here, we suggest three security approaches that can be utilized in cloud computing deployments in such a way that the current capabilities of the cloud are not curtailed while limiting the cloud provider control on data and enabling all cloud users to benefit from the cloud.

First approach is **Information centric data security**. It is self-protection technique in which intelligence requires to be put in the data itself. Here, data requires to be self-describing and defending, regardless of its environment. When data accessed by potential subscriber, data

consults its policy and attempts to recreate itself in a secure environment. This whole process is to be verified as trustworthy by application of the framework of trusted computing.

Second approach is **Remote server attestation**. Major reason of discouraging businesses from transferring their data to the cloud is lack of transparency in the cloud system. Subscribers do not know that how their data is being managed at the cloud, and in particular, how would they ensure that their data is not being mismanaged with their nature. Currently, subscribers must be satisfied with cloud service providers using manual auditing or electronic audit procedures. Here, trusted computing [4] can be a good approach to solve this problem. A trusted monitor gets installed at the cloud server in a trusted computing environment. The trusted monitor has ability to minutely check or audit the operations of the cloud server. As result, proof of compliance is to be provided by the trusted monitor to the subscribers means it is giving guaranty to the subscribers that certain access policies which are necessary for cloud security have not been violated by the cloud service provider and their cloud operations. To ensure integrity of the trusted monitor, trusted computing also allows secure bootstrapping of this trusted monitor to run beside the subscriber's operating system and cloud applications. The trusted monitor has ability to enforce strong access control policies necessary for cloud security. When the subscriber gets proof of compliance, he can verify that the correct monitor code is being run or not, and the cloud server has complied with necessary access control policies.

Third approach is **Encryption based business intelligence.** A magnificent approach for retaining control of data is to encrypt of all cloud data. The practical obstacle in this approach is that encryption limits data use. Data stored in clear-text form can be searched efficiently by using just keyword. This function cannot be performed with randomized encryption schemes. Solution for these problems is the state-of-the-art cryptographic mechanisms [5]. Versatile encryption mechanisms invented by cryptographers are available nowadays which allow various computations and operations on cipher-texts also. Encryption or predicate encryption required to be searched allows subscriber to compute a capability from his own secret key. This capability enables the system to encode a search query which is used by the cloud to decide that the documents match with the search query or not. As these cryptographic techniques are still in being maturity phase, they has capability to open up possibilities and directions for research and development for new cloud security protocols and algorithms. More extensive research and development projects are required to enable these cryptographic tools sufficiently practical and user friendly for the cloud subscribers.

4. CONCLUSION

Despite immense surge in activity and interest in cloud computing, there are significant concerns about cloud security specially security of data that are creating obstacle for its momentum and eventually affecting the vision of cloud computing as a new IT procurement model. Despite the immense business and technical advantages of cloud computing, many potential cloud users are hesitating to join the cloud, and those major corporations being cloud users are putting only their less sensitive data in the cloud due to fear of loss of data or related data theft. We see that security threats to Cloud is more complex rather than normal computer network. So developers have to be more cautious about security of data. There is history of security breaches of data for Cloud even by Service Provider. We feel that many of these security and privacy issues are essentially old problems in a new dimension, even they can be more acute. So correct approach towards cloud security which are suggested in this paper becomes more important. As these approaches' give more transparency and freedom to subscriber, people gets encouragement to join cloud. In short, "**The cloud**" is full of potential of being top computational technique and is yet to be realized. In future, we feel that state-of-art cryptographic mechanisms and electronic audit will play vital role towards cloud security and have much scope of work and research by academia.

REFERENCES

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

[2] The NIST definition of Cloud Computing. http://csrc.nist.gov/publications/nistpubs/800-45/SP800-145.pdf

[3] A Survey A Cisco Guide to Defending Against Denial of Service Attacks; http://www.cisco.com/web/about/security/intelligence/guide_ddos_defense.html

[4] Trusted Computing: Concepts; http://www.cs.bham.ac.uk/~mdr/teaching/modules/security/lectures/TrustedComputingConcepts.html

[5] Omer K. Jasim, Safia Abbas, El-Sayed M. El-Horbaty and Abdel-Badeeh M. Salem; Cloud Computing Cryptography "State-of-the-Art" World Academy of Science, Engineering and Technology, International Journal of Computer, Information, Systems and Control Engineering Vol:7 No:8, 2013