Volume 5, Issue 6, June 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Review on Storage Security Challenges in Cloud Computing

Jagjit Singh
Research Fellow
Punjabi University, Punjab, India

Er. Gurjit Singh Bhathal
Asst. Professor
Punjabi University, Punjab, India

Abstract: ***Number of users used Cloud to store their data. Data storage security: it is security of data on the storage media. In cloud computing security is an important factor for ensuring clients that in the cloud, data is placed on a secure mode. For protecting Data from malicious users, client authentication becomes an important task. There are a number of security and Privacy issues/concerns associated with cloud computing but these issues fall into two broad categories: Security and Privacy issues faced by cloud providers and security and privacy issues faced by their customers. This research paper outlines what cloud computing is, the various cloud models and the main security risks and issues that are currently present within the cloud computing. This also describes various security mechanisms for particular IaaS, PaaS & SaaS. In this Multimedia Cloud Computing Storage architecture & various security challenges has also been reviewed.***

Keyword: Multimedia Cloud Computing, IaaS, PaaS, SaaS, Storage Security

I. INTRODUCTION

An emerging technology Cloud computing, aims at providing over the Internet various storage and computing services [1], [2]. It generally incorporates platform, software and infrastructure as services. Providers of Cloud service rent data-centre software and hardware to deliver computing and storage services via Internet. Through cloud computing, users of internet can access services from a cloud as though employing a super computer. Instead of storing data in own devices they could be stored in the cloud making possible to access ubiquitous data. With software deployed in the cloud, Could also run their applications on cloud computing platforms which are more powerful, mitigating the users' burden of continual upgrade and full software installation on their local devices.

With Web 2.0's development, as a service Internet multimedia is emerging. For rich media services provision, multimedia computing has come through as a noteworthy technology to, edit, generate, search and process media contents, like: video, images, graphics, audio, and so on. For multimedia services and applications over mobile wireless networks and Internet there is a strong demand for cloud computing, as significant amount of computation is needed for serving millions of mobile or Internet users at the same time. Users process and store their multimedia application data, In cloud-based multimedia computing paradigm , cloud data is stored and processed in a distributed manner, eliminating full installing on users' device or computer the media application software and thus alleviating the burden computation of user devices and saving the battery of mobile phones.

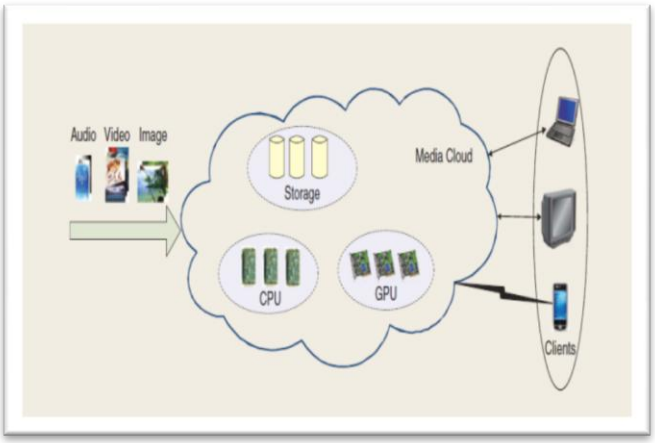

Fig 1 – Fundamental Concept of Multimedia Cloud Computing

In a cloud, Multimedia processing imposes great challenges. Some fundamental challenges for multimedia computing in the cloud are given below.

- **Multimedia and service heterogeneity:** There exist different types of services and multimedia like: video conferencing, [VoIP] voice over IP, , multimedia streaming, photo editing and sharing, image search, , video trans-coding, multimedia content delivery, image-based rendering and adaptation, the cloud shall support various types of multimedia services and multimedia for million users simultaneously.

© 2015, IJARCSSE All Rights Reserved

- **QoS heterogeneity**: As different QoS requirements are of different multimedia service, the cloud shall provide QoS support and provisioning for different type of multimedia services to fulfil multimedia QoS requirements.
- **Network heterogeneity:** As different networks, like, wireless local area network (LAN), third generation wireless network and Internet have different network characteristics like: jitter, delay, and bandwidth. For optimal delivery to different types of devices with various network latencies and bandwidths, cloud should adapt multimedia contents.
- As different devices like: mobile phones, personal computers (PCs) and TVs have varied multimedia processing capabilities , the cloud must possess multimedia adaptation capability for fitting varied devices, like:, GPU, display, memory, power, storage and CPU.

Multimedia Aware Cloud

The following functions media cloud needs to have:

1. QoS support and provisioning for different types of multimedia services along with varied QoS requirements.
2. Distributed parallel multimedia processing.
3. Multimedia QoS adaptation to fit varied types of network and devices bandwidth. In this part, first architecture of the media cloud is presented. Then discussion is done on distributed parallel multimedia processing in the media cloud and as to how the cloud can provide QoS support for multimedia services and applications.

II. SECURITY MECHANISMS FOR THE CLOUD SERVICE MODEL

Cloud-based system addresses three service models named IaaS, PaaS. SaaS. These service models lie on the top of each other, thereby forming the stack of a cloud. The IaaS service model can be deployed using one of the deployment models. Hence security implications need to take into account considering both service and deployment models.

Security Mechanism for IaaS

Infrastructure-as-a-Service, sometimes also referred as utility computing, can be viewed as virtual machine on demand, where this virtual machine can be accessed remotely and made available on elastic basis.[3] This means that all the necessary infrastructure, hardware, memory, networks and storage are provided by IaaS service model. Most of the security concerns for IaaS delivery model are due to sharing and pooling of resources, virtualized data centre, and virtualization of hardware, resources and networks. No matter what we opt to choose as our deployment model for IaaS, security requirements for IaaS service model must be implemented at the level of host, virtual machine, network, storage, compute and memory. For public/hybrid cloud model, all the cloud services are provided to cloud service clients via Internet. The cloud service client in this case may be client computer or any on-premises system that is connected to cloud-based IaaS system. Depending on the services offered by cloud-based IaaS system, we can control security state of the client system connected to cloud services. This can be done by enforcing the baseline security level of all clients to assure that the client has sufficient security tools, like anti-virus, anti-malware and up-to-date security patches. However, if these cloud services are available to an unaffiliated user, there is nothing that IaaS vendor can do to enforce security policy of this non-affiliated client. Therefore, system must be designed to support the level of network encryption or even in the worst scenario secure session must be established for the logging process. Another issue associated within this delivery model is network availability. Attacks like DNS misdirection, Prefix hijacking, or distributed denial of service can seriously deteriorate the network availability of the system. Therefore, constant network monitoring and auditing tool must be implemented to mitigate the attacks on network availability. Moreover, in a private/hybrid cloud network resources are consumed form a common resource pool. Consequently, logical isolation of internal system is equally important for cloud-based IaaS system. This means that in order to secure the network system of our cloud-based IaaS delivery model virtual firewall, VLAN, virtual layer [4] switches, and IPSec isolation are needed to be considered and implemented. Another issue associated with IaaS delivery model is due to its architectural representation of its cloud-based storage system. Cloud based storage system is designed for creating the pool of resources, abstracting the details like storage location, storage type, persistence of storage, etc. from its consumers. This means that data from multiple tenants reside on same disk or array and any breach in the system could lead to the exposure of private and sensitive data to a malicious user or unintended tenants. An appropriate access control (XACML) and authentication (SAML, Open ID) mechanisms in terms of identity of the user can mitigate this issue. The implementation details of this access control and authentication mechanisms depend on the deployment models of cloud-based platforms. Public cloud, offering IaaS delivery model, may use web services through web portals to provide access control and authentication mechanisms. Hybrid cloud may use public cloud storage gateway appliance on premises, where the cloud storage API is translated into conventional data retrieval protocol, like ISCSI, NFS (Network File System), SMB (Server Messaging Block), etc.

Security Mechanism for PaaS

Platform-as-a-Service model is build on the top of IaaS, which provides complete development environment where application developers can create and deploy their applications. In contrast to traditional software development tools, like Visual Studio, PaaS offers a shared development environment. This means that there must be a mechanism within the system to ensure that customers are kept separate from each other. An appropriate authentication, access control and authorization mechanisms will ensure isolation of customers. A strong and implicit authentication mechanism ensures that user is correctly identified. Most of the Paas providers still rely on the same traditional user-name and password-based authentication and then apply access control and authorization mechanisms based on verification of the credentials

© 2015, IJARCSSE All Rights Reserved

provided.[5] An alternative to this, two factor authentication mechanisms, like smart cards and biometrics, can be implemented. Moreover, identities-based authentication in terms of web services or SAML-based identity provider can be taken into account, where authentication authorization and access control in a PaaS system can be externalized.

Security Mechanism for SaaS

Software-as-a-Service is built on the top of PaaS, and all of the security mechanisms are implemented at an application level, regardless of its deployment model. Network security is typically not considered in the SaaS delivery model. However, it can be implemented with regards to some application specific control of SaaS solution. In a Public cloud scenario, high degree of trust in the cloud vendor is required, as the infrastructure and platform are under the supervision of cloud vendors. Therefore, security responsibility of both cloud vendor and customer are defined in the Service Level Agreement (SLA).[6][7] Another factor to be considered for a SaaS-based solution is its APP's store. Cloud vendor may offer their application only from their app store, and there is a possibility that any malicious user can post malware in the app store. Google Android had a similar problem in the past. Moreover, one must also assume that SaaS-based software solution will be scanned by the hacker in order to identify the vulnerabilities before deploying it. Due to the absence of App's store in a private cloud threats associated with malicious malware from outside of the company are no more the area of concern. However, App's developed with poor piece of code can be as detrimental as malware. This means that regardless of deployment model on a cloud-based platform, security guidelines for developing software based solutions, like SDL (Security Development Lifecycle), should be followed before developing SaaS-based solution in a cloud.

III. MULTIMEDIA STORAGE SECURITY IN CLOUD COMPUTING

Cloud storage, is a model of networked enterprise storage where data is stored in the user's computer and also in virtualized pools of storage that are generally hosted by third parties, too. Companies that host operate large data centres, and those who want their data to be hosted buy or lease storage capacity from them. in the background operators of data centres, , , according to the requirements of the customer, virtualizes the resources and expose them as storage pools, that customers can by themselves use to store data or files objects. Physically, across multiple servers resource may span. Hosting websites are responsible for the safety of the files.

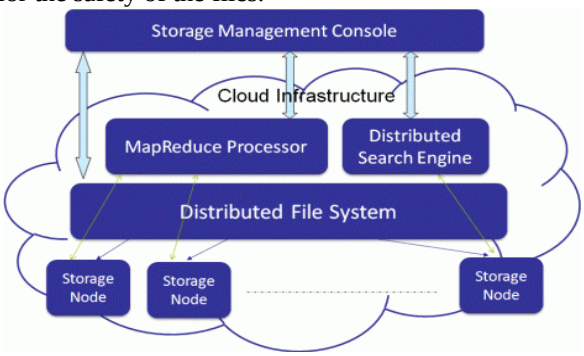

Fig 2: Cloud Storage Architecture

Cloud storage services may be accessed through a web service application programming interface (API), a cloud storage gateway or through a Web-based user interface.

Cloud storage is:

- made up of many distributed resources, but still acts as one
- highly fault tolerant through redundancy and distribution of data
- highly durable through the creation of versioned copies
- Typically eventually consistent with regard to data replicas.

Data storage security refers to the security of data on the storage media, which means non-volatile or fast recovery after loss. This security should be taken into account by software engineers in design stage of cloud storage services. It includes not only data redundancy and dynamic, but also isolation. Redundancy is the most basic measures to protect data storage security, and dynamic means user data may often change, so effective measures are needed to ensure data consistency.[8] Isolation is that since different user's data is stored in the same platform, to guarantee the independence between the data, which means user can only access their own data, and data changes of other users will not affect the current user.

Major Risks of Cloud Computing Security

In cloud computing service environments, there are many security issues like: distributed big data processing, virtualization, serviceability, cryptography traffic-handling, authentication, access control and application security etc. Especially, data access through varied resources require access control model and user authentication for integrated control and management in cloud computing environments.

Cloud computing security is a hot topic for research, its freshness, interestingness and recognition created an appeal for researches to pursue this topic in specific. Many security concerns evolved while weighing the benefits of using cloud computing over local resources. Below are the major risks introduced by the cloud are:

© 2015, IJARCSSE All Rights Reserved

- Data Storage
- Legal and Regulatory Risks
- Privacy and Confidentiality
- Availability
- Integrity
- Computationally feasible
- Proper usage metering
- Internal and external attacks
- Abusing cloud's resources

IV. RELATED WORK

P. Garbacki et al. [9] in cloud computing system solved the issue of data security by introducing in cloud computing data security: fully homomorphism encryption algorithm**,** the new type of data security solution to the insecurity of the cloud computing is proposed and the scenarios of this application are hereafter constructed. For the retrieval and processing of the encrypted data effectively, this new security solution is fully equipped leading to the broad applicable prospect storage of the cloud computing and the security of data transmission.

Prakash G L et al. [10] proposed that how to protect the outsourced sensitive data as a service is becomes a major data security challenge in cloud computing. To address these data security challenges, we propose an efficient data encryption to encrypt sensitive data before sending to the cloud server. This exploits the block level data encryption using 256 bit symmetric key with rotation. In addition, data users can reconstruct the requested data from cloud server using shared secret key. We analyze the privacy protection of outsourced data using experiment is carried out on the repository of text files with variable size. The security and performance analysis shows that the proposed method is highly efficient than existing methods performance.

Hanumantha Rao et al. [11] has proposed a business model for cloud computing for data security using data encryption and decryption algorithms. In this method cloud service provider has responsible for data storage and data encryption/decryption tasks, which takes more computational overhead for process of data in cloud server. The main disadvantage of this method is, there is no control of data for data owner i. e, data owner has completely trusted with cloud service provider and he has more computational overhead.

Swati Paliwal et al. [12] proposed an Attribute Based Encryption (ABE) and verifiable data decryption method to provide data security in cloud based system. They have been designed the data decryption algorithm based on the user requested attributes of the out sourced encrypted data. One of the main efficiency drawbacks of this method is, cloud service provider has more computational and storage overhead for verification of user attributes with the outsourced encrypted data. While introducing third party auditor we can reduces the storage, computation, and communication overheads of the cloud server, which improves the efficiency of the cloud data storage.

ShivShakti et al. in [13] discussed the performance of six different symmetric key RSA data encryption algorithms in cloud computing environment. They have proposed two separate cloud servers; one for data server and other for key cloud server and the data encryption and decryption process at the client side. The main drawback of this method is to maintaining two separate servers for data security in cloud, which creates a more storage and computation overheads.

J.Srivivasi et al. [14] proposes Cloud Computing is a versatile technology that can support a broad-spectrum of applications. In this paper, explore the different concepts involved in cloud computing. Cloud computing is not only application oriented but service oriented, it offers on demand virtualized resources as measurable and billable ulitilities. The low cost of cloud computing and its dynamic scaling renders it an innovation driver for small companies, particularly in the developing world. The summary of the survey conducted by them on the basic issues of the cloud computing like: - security, performance, availability, cost, regulatory requirements, Bandwidth, quality of service and data limits.

V. CONCLUSION

One of the biggest security worries with the cloud computing model is the storage of secret data/information. Cloud service providers need to inform their customers on the level of security that they provide on their cloud. In this paper, we first discussed various models of cloud computing, security issues and research challenges in cloud computing. Data security is major issue for Cloud Computing. This paper has highlighted all the issues of cloud computing. New security techniques need to be developed and older security techniques needed to be radically tweaked to be able to work with the clouds architecture. The development of cloud computing technology is still at an early stage. So, new enhanced architectures need to be developing for security purposes.

REFERENCES

[1] Qian Wang, Cong Wang, Kui Ren, Wenjing Lou, Jin Li ,"Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing", IEEE Transactions On Parallel And Distributed Systems, Vol. 22, No. 5, 2011.

[2] Cong Wang, Qian Wang, Kui Ren, Wenjing Lou, "Privacy Preserving Public Auditing for Data Storage Security in , cloud Computing", 2010.

[3] M. Sudha, Dr. Bandaru Rama Krishna Rao, M.Monica, „A comprehensive approach to ensure secure data communication in cloud environment" International Journal of Computer Application (0975-8887), Volume 12-No 8, Dec 2010.

© 2015, IJARCSSE All Rights Reserved

[4] Palivela Hemant , Nitin.P.Chawande, Avinash Sonule, Hemant Wani,‟ Development of Server in cloud computing to solve issues related to security and backup‟, in IEEE CCIS 2011.

[5] Jianyong Chen, Yang Wang, and Xiaomin Wang, "On demand security Architecture for cloud computing", 0018- 9162/12, published by the IEEE Computer society in 2012.

[6] John Harauz, Lori M. Kaufman and Bruce Potter, "Data security in the world of cloud computing" published by the IEEE computer and reliability societies in July/August 2009.

[7] Nabendu Chaki, "A Survey on Security issue in Cloud Computing " in 6th International conference on Electrical Engineering/Electronics, Computer, Telecommunication and Information Technology, May 2009.

[8] Nils Gruschka and Meiko Jensen ,"Attack surface : A taxonomy for attacks on cloud services" in 2010 IEEE 3rd international conference on cloud computing.

[9] P. Garbacki and V. K. Naik(2007) "Efficient Resource virtualization and sharing strategies for heterogeneous Grid environments," inProc. IFIP/IEEE IMSymp., pp. 40–49.

[10] Prakash G L National Institute of Standards and Technology(2009), The NIST Definition of Cloud Computing, Information Technology Laboratory.

[11] Hanumantha Rao.Galli etc(2013 October)."Data security in cloud using hybrid encryption and decryption" International journal of advanced research in computer science and software engineering vol3.

[12] Swati Paliwal, Ravindra Gupta(2013 February),"A Review of Some Popular Encryption Techniques",International Journal of Advanced Research in Computer Science and Software Engineering,Volume 3, Issue 2, ISSN: 2277 128X.

[13] ShivShakti etc(2013 January-Febuary)."Encryption using different techniques:A Review" international journal in Multidisciplinary and academic research (SSIJMAR) vol.2 No.1 - (ISSN 2278-5973).

[14] J.Srinivas, K.Venkata Subba Reddy, Dr.A.Moiz Qyser(2012 july)"Cloud Computing Basics" International Journal of Advanced Research in Computer and Communication Engineering ,Vol. 1, Issue.

© 2015, IJARCSSE All Rights Reserved