International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 3, Issue 01, January 2016
Available at http://internationaljournalofresearch.org

Data Integrity in Cloud Computing Security

STUDENT DETAILS:
NAME: **Keesara Naveen Kumar**
Branch: cse
Qualification: M-Tech(cse)

GUIDE DETAILS:
NAME : **N. Srinivas**
Qualification: M-Tech (cse)
Designation: **Associate Professor** & **HOD**

Hod details
Name: N. Srinivas
Qualification:M-Tech(cse)
Designation:Associate Professor & **HOD**

ABSTRACT
Cloud computing requires comprehensive security solutions based upon many aspects of a large and loosely integrated system. The application software and databases in cloud computing are moved to the centralized large data centers, where the management of the data and services may not be fully trustworthy. Threats, vulnerabilities and risks for cloud computing are explained, and then, we have designed a cloud computing security development lifecycle model to achieve safety and enable the user to take advantage of this technology as much as possible of security and face the risks that may be exposed to data. A data integrity checking algorithm; which eliminates the third party auditing, is explained to protect static and dynamic data from unauthorized observation, modification, or interference.

Keyword: Cloud Computing; Cloud Computing Security; Data Integrity; Cloud Threads; Cloud Risks

INTRODUCTION: There are several different definitions of cloud computing, but all of them agree on how to provide services to users of the network. Cloud computing is an Internet-based development and use of computer technology. It refers to the use of computing resources; hardware and software, available on demand as a service over the Internet. It offers a range of services for users of the network, which include applications, storage, and various operations and remote printing, etc. [1]. It typically involves over the Internet provision of dynamically scalable and often virtualized resources [2]. Businesses are running all kinds of apps in the cloud. Cloud computing can be considered as the technology that keeps the data, uses in different applications and is remotely controlled without the need to download certain applications on computers. Some of the potential benefits that apply to almost all types of cloud computing includes the following: 1. Cost Savings: Companies can reduce their capital expenses and use operational expenses for increasing their computing capabilities. 2. Flexibility: The flexibility of cloud computing allows companies

to use additional resources in peak times, to enable them to satisfy consumer demands. 3. Reliability: Services using multi-redundant sites can support business continuity and disaster recovery. 4. Reduce Maintenance: Cloud service providers do the system maintenance that does not require application installations onto PCs. 5. Mobile Accessible: Mobile workers have increased productivity due to systems accessible in an infrastructure available from anywhere. 6. Transparency: Additional servers to be added to the provisioned service without interrupting the service or requiring reconfiguration of the application delivery solution. If the application delivery solution is integrated via a management API, then transparency is also achieved through the automated provisioning and de-provisioning of resources. Information security can be viewed as including three functions: Access control, secure communications, and protection of private data [3]. Information security is also defined as the protection of private data and processing from unauthorized observation, modification, or interference. This paper describes several information security concepts that apply to all information security research specific to cloud computing. Cloud computing requires comprehensive security solutions based upon many aspects of a large and loosely integrated system. Cloud Computing has been considered as the next generation architecture of IT Enterprise, and this new paradigm makes many new security challenges. Therefore, the security issues that are related to static and dynamic data in cloud computing are investigated. Security on the cloud will be a major research topic in itself. Cloud computing increases some of security risks to the cloud users and businesses. It might be difficult for the user to effectively verify the data managing of the cloud provider and therefore to make sure that the data is being handled in a valid way. The greater damages in the cloud will often caused by malicious insider. The cloud architectures, which involve system administrators and security service providers, are extremely high-risk by their nature. Data breaches is the most important concerns facing the cloud computing users whether from inside or outside the cloud. The rest of paper is organized as follows: section 2 describes the related works. Section 3 addresses a general description of cloud computing, types, service models, and deployment models. Section 4 is a description of threads and attacks on cloud computing. Section 5 presents the security risks. The description of the proposed model is discussed in section 6. And finally, the conclusions are summarized in section

RELATED WORK Recently the cloud computing technology became widely used by most of the business companies to increase their productivity and with that there are still some concerns about the security provided by cloud computing [4]. In 2013, cloud computing is still in high demand where the organizations are either already using or intending to use cloud computing infrastructure services, and the share of cloud service will continue to increase as a percentage of total revenue [5]. One of the biggest concerns with cloud data storage is the verification of data integrity at untrusted servers, and how to deal with sensitive data. It is not an easy task to maintain customer's most sensitive cloud data securely, which is needed in many applications for clients. This makes some companies wary of switching to cloud computing because the user does not know on which server the data is stored and is this server provides secure data or not. The first proposed a solution to remote data integrity is proposed by Deswarte

et al [6], use RSA-based functions to hash the whole data file for every verification challenge. It is inefficient for the large data files, which need more time to compute and transfer their hash values. Caronni proposed another protocol [7], where the server has to send Message Authentication Code (MAC) of data as the response to the message instead of storing the hash of all data. The verifier sends a unique random key for the message authentication code to achieve integrity on data from any modification or deletion. Instead of storing the whole data at server specific portions of data is stored; a deterministic verification approach is used. Ateniese et al proposed a model for using homomorphic verifiable tag that is calculated as a number that is equal to two times of number of data chunks, and stores the data file and it tags on the server. Then, the client can verify that data integrity of the file Using the queried blocks and their corresponding tags and the server generates a proof of integrity [8] [9]. For the dynamic data integrity verification, Wang et al.[9] discussed the problem of ensuring the availability and integrity of data storage in cloud computing. They utilized the homomorphic token and error correcting codes to achieve the integration of storage correctness insurance and data error localization.

CLOUD COMPUTING COMPONENTS: Cloud Computing has been considered as the next generation architecture of IT Enterprise. Cloud computing moves the application software and databases to the centralized large data centers, where the management of the data and services may not be fully trustworthy. This new paradigm makes many new security challenges. Figure (1) depicts Cloud Data Storage Model [10]. A cloud computing is made up of several elements: Cloud users, cloud service providers, third parity auditors [11]. Each element plays a specific role in delivering functional cloud-based application. a. Cloud Users: The users can be an individual or an organization storing their data in cloud and accessing the data. He can use: • Mobile including PDAs and smart phones • Thin, where the client's computer does not have hard drive and the work is done by the server. Thin client becomes popular because of low hardware cost and since data is stored on servers there is less chance for data to be lost or stolen • Thick, uses regular computer that uses a web browser to connect to the cloud.

b. Cloud Service Providers (CSP): The CSP, who manages cloud servers (CSs) and provides a paid storage space on its infrastructure to users,. Servers are geographically housed on different locations. The servers on cloud computing is based on the principle of virtual servers because the user does not know which server will give him the required service. This is the main difference between cloud computing and distributed computing. c. Datacenters: A collection of servers form the data center, where the application is housed. Cloud data centers are known as cloud data storages (CDSs). The software can be installed on one physical server and allowing multiple instances of virtual servers to be used. The number of virtual servers depends on the size and speed of physical server and what application will be running on the virtual server. The data on the cloud computing can be either static or dynamic i. Static data: It is data that cannot be altered or edited them and any amendment thereto will become the new data and this data can be read and re-write them again but without modification. Example: Data Centers. ii. Dynamic data: It is the data obtained by the modification or change continuously which are used in transfer between users on

cloud computing. Example: E-mail. d. Third Party Auditor (TPA) or Verifier: The TPA or Verifier has expertise and capabilities (that users may not have) and verifies the integrity of outsourced data in cloud on behalf of users. The TPA could release an audit report to user. Cloud Computing Service Models The cloud service provider (CSP) offered its customers with kind of services and tools, which are: a. Software as a Service (SaaS): involves using their cloud infrastructure and cloud platforms to provide customers with software applications. In this service, the user can take advantage of all applications. The end user applications are accessed by users through a web browser, such as Microsoft SharePoint Online. The need for the user to install or maintain additional software is eliminated [12]. b. Platform as a Service (PasS): enables customers to use the cloud infrastructure; as a service plus operating systems and server applications such as web servers. The user can control the development of web applications and other software and which use a range of programming languages and tools that are supported by the service provider [12]. c. Infrastructure as a Service (IaaS): the registered user may access to physical computing hardware; including CPU, memory, data storage and network connectivity of the service provider. IaaS enables multiple customers referred to as "multiple tenants" using virtualization software. The user gains greater flexibility in access to basic infrastructure [12]. d. Security as a service (SecaaS): categorize the different types of Security as a Service and to provide guidance to organizations on reasonable implementation practices [13]. 3.2 Deployment Models of Cloud Computing Cloud Computing can be run on different deployment models. The deployment model is selected depending on the user requirements and market availability: a. Private Cloud: a cloud that is used exclusively by one organization. The cloud may be operated by the organization itself or a third party. If the private cloud is properly implemented and operated, it has reduced potential security concerns. The St Andrews Cloud Computing Co-laboratory and Concur Technologies are example organizations that have private clouds [14]. b. Public Cloud: a cloud that can be used (for a fee) by the general public, and involves an organization using a cloud infrastructure which is shared via the Internet with many other organizations and other members of the public; such as Microsoft, Google and Amazon [14]. Public cloud has variety of inherent security risks that need to be considered. c. Community Cloud: is shared by several organizations and is usually setup for their similar security requirements and a need to store or process data of similar sensitivity; such as several agencies of the same government [14]. d. Hybrid Cloud: is a combination of cloud deployment models. Each cloud could be independently managed while applications and data would be allowed to move across the hybrid cloud. A private cloud can burst-out to a public cloud when it requires more resources [14]. A specific business and technology requirements are used in designing hybrids, which helps to optimize security and privacy with a minimum IT costs [15].

CLOUD COMPUTING SECURITY THREATS: Although cloud computing certainly gives organizations with significant cost savings and operational efficiencies, it also brings new security risks and uncertainties. The increased attack surface in a Cloud environment allows for other vulnerabilities to be exploited, thereby increasing the organization's risk [An Introduction to Securing a Cloud Environment].

The risk is defined as a given threat that exploits vulnerabilities of an asset or group of assets and thereby cause harm to the organization [16]. The increased attacks in cloud environment; virtual switches and hypervisor that are not present in the traditional data center, allows for other vulnerabilities to be exploited, thereby increasing the organization's risk [17]. The most important threats facing cloud computing are identified as follows [18], [19] [20]: a. Data breaches: The most important thing is to prevent any data violation. The challenge addressing the threats of data loss and data leakage is that "the measures you put in place to improve one can worsen the other". Data is encrypted to reduce the impact of a violation, but if the encryption key is lost, then data will be lost. However, if offline backups of data are chosen to reduce data loss, exposure data breaches are increased. b. Data Loss/Leakage: There are many ways to compromise data because of insufficient authentication, authorization, and audit (AAA) controls, such as deletion or alteration of records without a backup of the original content. Loss of an encoding key may result in effective destruction. Unauthorized parties may gain access to sensitive data. A malicious hacker might delete a target's data. c. Account or Service hijacking: Attack methods such as phishing, fraud, and exploitation of software vulnerabilities still achieve results. If an attacker gains access to credentials, he can eavesdrop on user activities and transactions, manipulate data, falsify information, and redirect your clients to illegal sites. d. Insecure Application Programming Interfaces APIs: APIs are integral to security and availability of general cloud services. These interfaces must be designed to protect against both accidental and malicious attempts. Anonymous access and/or reusable tokens or passwords, clear-text authentication or transmission of content, inflexible access controls or improper authorizations, limited monitoring and logging capabilities; are examples of this type of threats. e. Malicious insiders: a provider may not reveal how it allows employee's access to physical and virtual assets, how it monitors these employees, or how it analyzes. In cloud computing, the organization doesn't need to know the technical details of how the services are delivered. In situations, the risk is great. Without full knowledge and control, your organization may be at risk. In situations, the risk is great. Without full knowledge and control, your organization may be at risk. f. Unknown risk Profile: Versions of software, code modifications, security policies and applications, vulnerability reports, interference attempts, and security design, are all important factors for estimating company's security status. Information about who is sharing your infrastructure may be relevant. g. Cloud abuse: Some providers offer free limited trial periods. By abusing the relative secrecy behind these registration and usage models, spammers, malicious code authors, and other criminals have been able to conduct their activities with relative invulnerability, such as password and key cracking. A malicious hacker uses cloud servers to launch a Distributed Denial of Service (DDoS) attack, propagate malware, or share illegally copied software. The challenge here is for cloud providers to define what constitutes abuse and to determine the best processes for identify it. h. Shared Technology Issues: (IaaS) is based on shared infrastructure (e.g. disk partitions, CPU caches, GPUs, etc.), were not designed to offer strong isolation properties for a multitenant architecture. A virtualization hypervisor mediates access between guest operating systems and the physical compute resources. Overlooked flaws

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 3, Issue 01, January 2016
Available at http://internationaljournalofresearch.org

have allowed guest operating systems to gain unauthorized levels of control and/or influence on the platform. i. Changes the business model. Cloud computing changes the way IT services are delivered. No longer delivered from an onsite location, servers, storage, and applications are provided by external service providers. Organizations need to evaluate the risks associated with the loss of control of the infrastructure. j. Exploiting browser vulnerabilities: Several years ago, hackers used to attack software operating systems. More recently, hackers have shifted their attacks to target user browsers.

CLOUD COMPUTING SECURITY RISKS: Virtualized servers will be less secure than the physical servers. However, all risks are not reduced by moving operations to a cloud environment. While some risks are reduced, other risks may increase. With the addition of virtual network switches, hypervisors and virtual images, the attack surface increases. A single host with multiple virtual machines may be attacked by one of the guest operating systems, or a guest operating system may be used to attack other guest operating systems. • vulnerabilities are particularly risky because other virtual machines residing on the host and the data files stored out sides the owner's trusted domain • Movement from one provider to while unencrypted or logged access. Anyone sniffing the network has an opportunity to extract sensitive data such as passwords or logins. • With virtualization, a customer's sensitive data is stored over a shared infrastructure that may be distributed on multiple sharing of servers and data centers. • Organizations should consider their risks due to anonymous signup, lack of validation, service fraud, and ad-hoc services. Virtualized platforms Risks are: • Management console vulnerabilities • Management server vulnerabilities • Administrative VM vulnerabilities • VM vulnerabilities • Hypervisor vulnerabilities • Hypervisor escape

PROPOSAL CLOUD DATA SECURITY MODEL From a business point of view, cloud Security is a set of organization safe policies, layered technologies and controls which are designed to protect data and infrastructure from attacks. In order to deliver reliable, well-managed, secure, and patched services, a cloud computing system development model is proposed, as it is welldescribed in figure 2. It aims to be the standard that defines all the tasks required for developing and maintaining the cloud security, where the cloud training staff needs to follow the following phases in order: a. Identifying Cloud Security Domains and Their Subcategories: including physical and logical infrastructure as well as the hosted applications and platform services with different risk classes. The physical infrastructure includes the data center facilities themselves, as well as the hardware and components that support the services and networks. The logical infrastructure consists of operating system instances, routed networks, and unstructured data storage, whether running on virtual or physical objects. Platform services include compute runtimes, name services (DNS), and other advanced functions consumed by online services. Infrastructure services may be virtualized or actual. • Physical Infrastructure Security: including servers, routers, storage devices, power supplies and other components that support operations—should be physically secure. Security includes managing, controlling and monitoring of physical access, protection from fire, natural disasters, burglary, theft, vandalism, and terrorism • Network, servers and End Points

Security: applies many security layers of security appropriately to data center devices and network connections. • Data Security: Data can be classified as high, moderate or low- sensitive data. It may be stored virtually and distributed across many locations; static or dynamic data. The data may reside on removable data storage or include in external network transfers. The encryption for storage, internal system and network transfers are required • Security of personal information: to help protect personal information from unauthorized access, use, or disclosure. • Identity and Access Management: rolebased access controls are used to allocate logical access to specific job functions or areas of responsibility. They are based on an identified business requirements and authentic and authorized for the requested access.

CONCLUSION: In order to provide a secure environment and to protect sensitive static and dynamic data on cloud computing, firstly, different threats, vulnerabilities and risks are explained. Then, we have proposed a cloud computing security development lifecycle model to achieve safety and enable the user to take advantage of this technology as much as possible of security and face the risks that may be exposed to data. The data integrity checking algorithm that eliminates the third party auditing is explained. The cloud user has to deal with the cloud provider as the third party through managing the data integrity checking and evaluation in efficient way using set of hash functions. The data and its corresponding hash value are retrieved back when the cloud user needs cloud data, and checked for any data altercation by re-generating and comparing the hash result with the pre-generated hash value. Cloud computing security approach provides better protection in terms of filtering, risk management, deployment of standard information security policies.

REFERENCES:

[1] Brian O. and others, Cloud Computing, authors:, 2012-11- 06, page 6, publish Swiss.

[2] http://www.kalyxinfotech.com/cloud.php

[3] Sehgal NK, et al.: Information Security and Cloud Computing, Iete Technical Review, Vol 28, Issue 4, Jul-Aug 2011.

[4] Rajiv R.Bhandari, Mishra N., Encrypted IT Auditing and Log Management on Cloud Computing, IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 5, No 1, pp. (302), September 2011.

[5] Cloud Computing Evolution in the Cloud. Available at: http://www.pwc.de/de_DE/de/prozessoptimierung/assets/cloud_computing_2013.pdf.

[6] Deswarte Y., Quisquater J.-J., and Saidane A.. Remote Integrity Checking, Proc. of Conference on Integrity and Internal Control in Information Systems (IICIS'03), November 2003, Switzerland.

[7] Caronni G. and Waldvogel M., "Establishing Trust in Distributed Storage Providers", In Third IEEE P2P Conference, Linkoping 03, 2003.

[8] Golle P., Jarecki S. and Mironov I., "Cryptographic Primitives Enforcing Communication and Storage Complexity", In proc. of Financial Crypto 2002. Southampton, Bermuda.

[9] Syam Kumar P., Subramanian R., An Efficient and Secure Protocol for Ensuring Data Storage Security in Cloud Computing, IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 6, No 1, November 2011.