Available online at www.sciencedirect.com

ScienceDirect

Materials Today: ProceedingsXX (2016) XXX–XXX

materialstoday: PROCEEDINGS

www.materialstoday.com/proceedings

PMME 2016

Comparative Study On Trustee Of Third Party Auditor To Provide Integrity And Security In Cloud Computing

K.SHIRISHA REDDY[1], Dr.M.BALARAJU[2]

[1]shirishakasireddy20@gmail.com, [2]drraju.jb@gmail.com

[1]Associate Professor, Vignan Bharathi Institute of Technology, Hyderabad, Telangana State, India,

[2]Professor& Principal, KITE,JNTUH, Hyderabad, Telangana State, India

Abstract – One of the storage device in the market are cloud services, there can be some security issues and conflicts between the client and service provider to resolve the third party auditor issues. This comparative analysis ensure reliable data storage providing computing resources in the form of service rather than a product and utilities are provided to users over world wide web. Cloud is a platform where data remotely stores in the server and also protects the data against threats; cloud environment is a domain which comes under the property of users for further development from research scholars. The information technology huge number of clients which is accessing the data and updating the data application and services move to centralized huge data centre and services management trust into cloud environment the computing resources are under control of service provider and the third party auditor ensures the data integrity over the sourced data. Compare Information Technology audit is a manual work our Cloud Third party auditor mechanism in cloud standard audit not only stores or reads the data also updates the data through query.

Keywords – Cloud Storage Provider, Third Party Audit, Information Technology Audit.

Introduction I

Appropriate security protection when using cloud services could ultimately result in higher costs and potential loss of business, thus eliminating any of the potential benefits of cloud computing. Enterprise information technology (IT) and business decision makers analyze the security implications of cloud computing on their business. When considering a move to cloud computing, customers must have a clear understanding of potential security benefits and risks associated with cloud computing, and set realistic expectations with their cloud provider.

Selection and Peer-review under responsibility of International Conference on Processing of Materials, Minerals and Energy (July 29th – 30th) 2016, Ongole, Andhra Pradesh, India.

Different service categories: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) as each model brings different security requirements and responsibilities, cloud security and also identifies areas where future standardization could be effective. Cloud Security Landscape provides an overview of the security and privacy challenges pertinent to cloud computing and points out considerations that organizations should weigh when migrating data, applications, and infrastructure to a cloud computing environment. Cloud Security Guidance is the heart of the guide and includes the steps that can be used as a basis for evaluation of cloud provider security. It discusses the threats, technology risks, and safeguards for cloud computing environments, and provides the insight needed to make informed IT decisions on their treatment. Although guidance is provided, each organization must perform its own analysis of its needs, and assess, select, engage, and oversee the cloud services that can best fulfill those needs. Cloud Security Assessment provides customers with an efficient method of assessing the security capabilities of cloud providers and assessing their individual risk. A customer to conduct their own assessment across each of the critical security domains is provided, the Practical Guide to Cloud Service Agreements [1], provides additional guidance on evaluating security criteria from prospective cloud providers. The security standards and certifications those are currently available in the market as well as the cloud specific security standards that are currently being developed.

The management by operational support systems of cloud directs to the capability to scale for supporting a huge number of virtual machines image library as well as storages load balancers firewalls virtual local area networks IP addresses and bundles of software as a service cloud providers are supplier of these resources depending on demands from their huge pools that are installed in the carrier clouds which is dedicated private virtual networks that can easily be configured. For deploying the applications the users of cloud that have to install on the devices the operating systems images along with their application pieces of software in the basic model of infrastructure as a service.

Figure 1 Cloud service Providers

Storage as a service is the service comes under the infrastructure as a service manages all the services of storage in the cloud computing, in fact several security issues that need to be taken into account data integrity confidentiality reliability etc. platform as a service the client creates software by using the tools and libraries that are provided by the providers client controls the software deployment as well as the configuration settings. Software as a service has indeed become one of the common models of delivery for a number of business applications together with accounting collaboration management information systems and modifies the sets of configuration preferences so as to have an effect on its functionality. The applications of cloud

are accessed by end users browser of web or desktop of light weight mobile application while the user's data and business software are stored onto the servers at some remote area.

SECTION II

2.Related Work: Security cloud controls and assurance like in traditional outsourcing arrangements but since there is no common cloud computing security standard there are additional challenges associated with cloud computing. Cloud vendors implement own proprietary standards and security technologies with different security models which needs to be evaluated on their own merits. The security challenges by organizations to use cloud services are not radically different from those dependent on their own in-house managed enterprise, internal threats are present and require risk mitigation acceptance. The information security challenges that adopting organizations will need to consider either through assurance activities on the vendor or public directly through designing and implementing security control in a privately owned cloud.

Threats to information assets residing in the cloud can vary according to the cloud delivery models used by cloud user organization to which cloud computing is vulnerable. Each of the cloud computing service delivery models threats result from the attackers that can be two groups.

Internal attackers	An internal attacker has the following characteristics: • Is employed by the cloud service provider, customer or other third party provider organization supporting the operation of a cloud service • May have existing authorized access to cloud services, customer data or supporting infrastructure and applications, depending on their organizational role • Uses existing privileges to gain further access or support third parties in executing attacks against the confidentiality integrity and availability of information within the cloud service.
External attackers	An external attacker has the following characteristics: • Is not employed by the cloud service provider, customer or other third party provider organization supporting the operation of a cloud service • Has no authorized access to cloud services, customer data or supporting infrastructure and applications • Exploits technical, operational, process and social engineering vulnerabilities to attack a cloud service provider, customer or third party supporting organization to gain further access to propagate attacks against the confidentiality, integrity and availability of information within the cloud service.

Table 1 Shows the Attacks of Cloud

Internal and external attackers can be clearly differentiated capability to execute successful attacks is what differentiates them as a threat to customers and vendors, cloud environment attackers can be categorized four types random weak strong and substantial. Random weak strong substantial is based on ability to instigate a successful attack rather than threat. Attacker uses simple tools and techniques may randomly scan the internet trying to find vulnerable components deploy well known that should be easily detected. Semi attacker targeting specific servers/cloud providers by customizing existing public available tools specific targets advanced attempt to customize the attacks using available exploit tools. Well-financed and skilled groups of attackers with an internal hierarchy specializing in targeting particular applications and users of the cloud generally group will be an organized crime group specializing in large scale attacks. Strong attackers not easily detected by the organization they attack or even by the relevant law enforcement and investigative organization specializing in e-Crime or cyber security. The security risks associated with each cloud model vary and dependent on a wide range of factors including the sensitivity of information assets, cloud architectures and security control involved in a particular cloud environment.

Risk	Description
Privileged user access	Cloud providers generally have unlimited access to user data, controls are needed to address the risk of privileged user access leading to compromised customer data.
Data location and segregation	Customers may not know where their data is being stored and there may be a risk of data being stored alongside other customers' information.
Data disposal	Cloud data deletion and disposal is a risk, particularly where hardware is dynamically issued to customers based on their needs. The risk of data not being deleted from data stores, backups and physical media during de-commissioning is enhanced within the cloud.
e-investigations and Protective monitoring	The ability for cloud customers to invoke their own electronic investigations procedures within the cloud can be limited by the delivery model in use, and the access and complexity of the cloud architecture. Customers cannot effectively deploy monitoring systems on infrastructure they do not own; they must rely on the systems in use by the cloud service provider to support investigations.
Assuring cloud security	Customers cannot easily assure the security of systems that they do not directly control without using SLAs and having the right to audit security controls within their agreements.

Table 2 Shows the Risk in Cloud

Cloud provider has access to the data controls access to that data by other entities including users of the cloud and third party suppliers maintaining confidentiality of the data in the cloud and limiting privileged user access can be achieved by at least one of two approaches by the data owner encryption of the data prior to entry into the cloud to separate the ability to store the data from the ability to make use of legally enforcing the requirements of the cloud provider through contractual obligations and assurance mechanisms to ensure the confidentiality of the data is maintained to required standards.

SECTION III

3. Problem definition: Cloud computing is a traditional auditing approach from context relates specifically to crimes attacks committed over storage communication networks and information systems. Cloud computing investigators examine and interpret storage devices and aims to initiate on forensic concern in cloud computing ecosystems. Long-term goal of effort build to understand consensus on the high-priority cloud third party computing network access to shared pool of configurable computing resources including servers storage include cost savings and greater flexibility in business and consumers employ information technology. Cloud computing allows for multiple users across a large domain where cloud specific confidentiality is concern. Auditing helps organizations to assess system utilization from internal resources and external resources, due to the large number of data tags auditing protocols will incur complex storage overhead on the server.

Bases on third party auditing as an security auditor to assess system utilization from internal sources and external sources nature of expensive cloud pricing data owners are interested to use different third party services where excising TPA system is not supporting security auditing.

3.1. Cloud Evolution: The data need to archive in secure organizations to integrate storage, to manage the use of their data from creation of end, the opportunity to store all our data in the world wide. The storages are provided and maintained by the third party through the world wide represents in the figure offers a complex pool of storage was available for use. With three significant attributes access via web services on a non-persistent network connection availability of very large quantities of storage and pay for the rapid scalability.

Cloud storage based on traditional network storage and hosted storage benefit of cloud storage is the access of data from application to application. Cloud storage providers provide storage varying from fewer amounts of data to the complete database of an organization subscriber can pay to the cloud storage provider for what are using and how much are transferring to the cloud storage.

Figure 2 Represents the cloud storage provider

Cloud storage subscriber copies the data into one of the data server of the cloud storage provider that copy data will be made available to all the other data servers of the cloud storage provider featuring redundancy in the availability ensures that the data of the subscriber is secure even anything went wrong.

Advantage of cloud storage: No need to invest any storage devices and technical expert to maintain the storage backup replication and importantly disaster management.

Allowing other to access data will result with collaborative working style instead of individual work.

3.2. Cloud storage Reference Model: The cloud storage is due to some of the same attributes that define other cloud services pay as you the illusion of infinite capacity and the simplicity of management is important that any interface for cloud storage support these attributes while allowing for a multitude of business cases and offerings long. The model created by storage networking industry association shows multiple types of cloud data storage interfaces able to support legacy and new applications interface allow storage to be provided on demand from a pool of resources. The capacity is drawn from a pool of storage capacity provided by storage services are applied to individual data elements as determined by the data system metadata, metadata specifies the data requirements on the basis of individual data elements on groups of data elements. Cloud data management interface is the functional interface that applications will use to create retrieve update and delete elements from the cloud as part of the interface the client will be able to discover the capabilities of the cloud storage offering and use this interface to manage containers and the data is placed. Metadata can be set in container and data elements through the interface expected the interface will be able to be implemented by the majority f existing cloud storage offerings with and adapter to their existing propriety interface by implementing the interface.

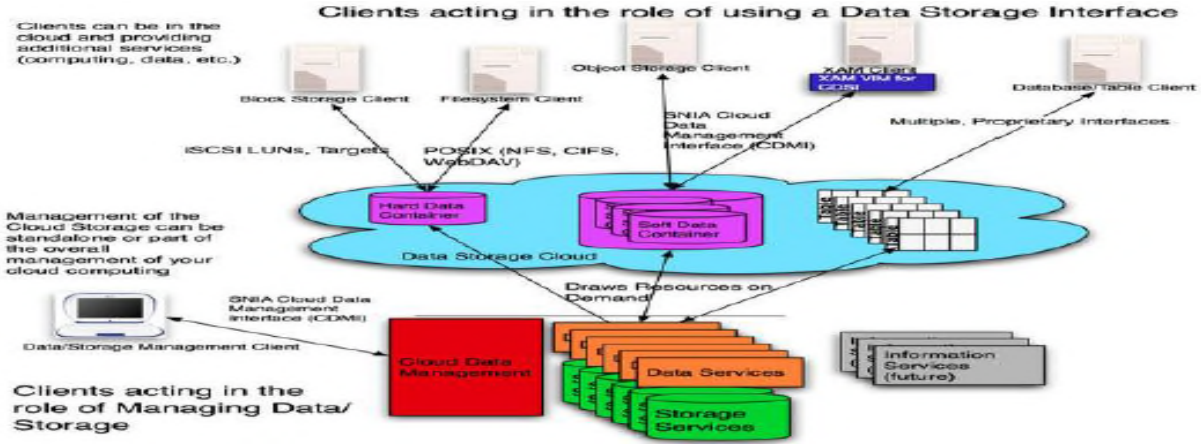

Figure 3 Cloud application programming

The interface administrative application to manage containers accounts security access monitoring billing information and even for storage that is accessible by other protocols, underlying storage and data services are exposed so that clients can understand the offering. Cloud storage application programming interface is a method for access to and utilization of a cloud storage system, most common kinds are representation state transfer although there are others which are based on simple object access protocol. All these application programming interface are associated with establishing request for service the internet widely recognized as an approach to quality scalable API design, the most important features of REST is a stateless architecture that everything needed to complete the request to the storage cloud is contained in the request so that session between the request and the storage cloud is contained in the request so that session between the requestor and the storage cloud is not required.

SECTION IV

4.1. Storage Provider in cloud: Storage Provider in cloud computing bring many challenging design issues has performed influence on the security of overall system. When many users are using data any time then consistency of data is more important because unauthorized person can use data and it can change or edit data or delete the data. If two users are using data user one is writing a data while other is reading data then it may lead to inconsistency, so resolving the data inconsistency becomes an important task of data owner, Third party Audit can be used as an intermediate party between the user and the cloud service provider, TPA not only use data but also edit data than data owner or user will know the problem and is multi write problem is important issue. to improve security check the integrity of data found out the problem which is security issues and third party auditor service and to manage this data using third party audit that provide the security and also some key security.

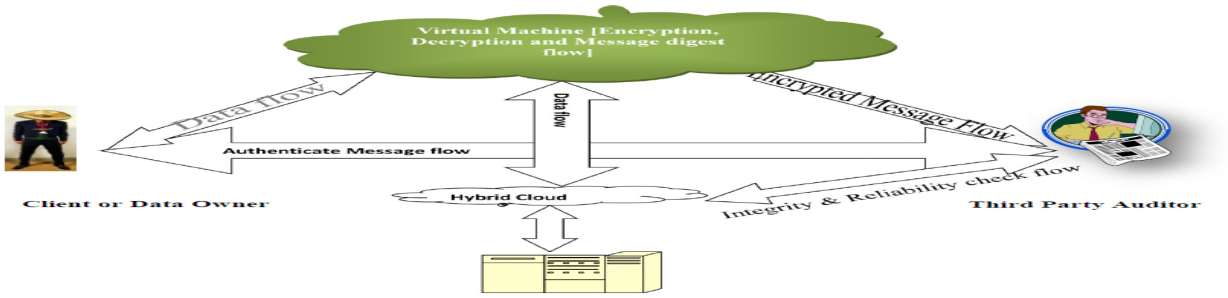

Figure 4 Shows the Third Party Auditor

Trust the cloud services with users data software computation on a published application programming interface over a network, cloud service providers a framework for several types of services that overlap with software as service and end users access cloud based applications through a web browser or a lit weight desktop or a mobile app while the business software data are stored on servers at a remote location. Cloud applications give same performance than if the software program were installed when we talk about cloud security maintaining data integrity is one of the most important task, when we talk about cloud users they are using cloud services provided by the cloud provider as in the case of maintaining integrity of the data, so we cannot trust the service provider to handle the data as he can edit the original data and the integrity may be lost. If the smart attack hacks the cloud servers and steals the data and modifies the modification not even identified by the cloud provider we take the help of trusted third party auditor to check for the integrity of our data. Auditor takes care of our data and makes sure that

data integrity is maintained the procedure of integrity checking as a key proficiency within software platform and infrastructure security focus area of our cloud architecture for helping assure system integrity in a virtualized environment includes an evolution of architecture.

4.2. Information Technology Auditing: Cloud computing is stated by National Institute of Standards and Technology for enabling on-demand network access to a shared pool of configurable convenient computing resources which can rapid growth released with minimal management effort or service provider interaction.

Private Cloud storage designed for hidden market like business and also provides security for their sensitive data typically on location where all processes and operations are managed internal. Third party can provide the same service off-site used entirely by the organization control.

CONCLUSION V

Cloud data security is effective storage device for client while using their business on cloud environment. Third party audit in cloud used to ensure the security and integrity of data trusted third party to resolve the conflicts between the cloud service provider and the client. We have many algorithms to protects against threats such as Encryption and Decryption but the third party auditor is abstract view of different schemes proposed for cloud data security, most of the authors have auditors store a message digest or encrypted copy of the same data that is stored with the service provider and resolve the conflicts between service provide and business people.

Reference

[1] Cong Wang and Kui Ren and Wenjing Lou and JinLi,"Toward Publicly Auditable Secure Cloud Data Storage Services" in IEEE, 2010. [4] M.Ashah and R. swaminathan and m.baker"Privacy-Preserving Audit And Extraction of Digital Contents", 2011. [5] H. Shacham and B. Waters "Compact Proofs of Retrivability" in proc. of asiascrypt, 2008.

[2] Elsenpeter Robert, Anthony T.Velte and Toby J.Velte, Cloud Computing a Practical Approach 2010. [2] Qian Wang and Cong Wang and Kui Ren, Wenjing Lou, Jin Li "Enabling Public Auditability And Data Dynamics For Storage Security in Cloud Computing" in IEEE transactions on parallel and distributed systems, 2011, vol. 22, no.

[3] Xiang Tan and Bo Ai "The Issue of Cloud Computing Security in High-Speed Railway" international confer. on electronic and mechanical engi. And information technology, 2011. Beijing p.r china,.

[4] FarzadSabahi,"Cloud Computing Security Threats and Responses" ,IEEE confer. 2011, 978-1-61284-486-2/111

[5] Ravi Kant Sahu and Abhishek Mohta, L.K. Awasthi "Robust Data Integration While Using Third Party Auditor For Cloud Data Storage Services", conf. IJARCSSE, 2012, Volume 2, Issue 2,ISSN: 2277 128X.

[6]Govinda V, and Gurunathaprasad, H Sathshkumar,"Third Party Auditing For Security Data Storage in cloud through digital signature using RSA" IJASATR, 2012, issue 2,vol-4, Issn 2249-9954.

[7] Cloud Standards Customer Council. Practical Guide to Cloud Service Agreements. http://cloud-council.org/resource-hub.htm#cscc-practical-guide-SLAs

[8] Cloud Standards Customer Council. Cloud Security Standards: What to Expect & Negotiate. http://cloud-council.org/resource-hub.htm#cloud-security-standards-what-to-expect-what-to-negotiate.Creeger, M. (2009).