International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 25 Issue 9 – AUGUST 2018.

ENSURING CLOUD DATA STORAGE SECURITY FOR PUBLIC AUDITING WITH ZERO-KNOWLEDGE SCHEME

K.SATHYA [#1] and S.SATHIYA [*2]

[#] *Assistant Professor, Dept. of Computer Science, Padmavani Arts and Science College for Women, Salem, India*

[*] *M.Phil., Research Scholar, Dept. of Computer Science, Padmavani Arts and Science College for Women, Salem, India*

***Abstract*— Cloud computing has quickly become one of the most famous catchphrase in the IT world due to its revolutionary model of computing as a service. It promises increased flexibility, scalability, and reliability, while promising decreased operational and support costs. However, many latent cloud users are hesitant to move to cloud computing on a large scale due to the unaddressed security issues present in cloud computing. In this paper, we investigate the major security issues present in cloud computing today based on a skeleton for security subsystems adopted from cloud service providers. We present the solutions proposed by other researchers, and address the potency and flaw of the solutions. Although considerable progress has been made, more research needs to be done to address the all-around security concerns that exist within cloud computing. Security issues relating to consistency, multi-tenancy, and federation must be addressed in more depth for cloud computing to overcome its security hurdles and progress towards widespread adoption.**

***Index Terms*— CSP, Integral Solutions, NIST models, Scheme**

I. INTRODUCTION

Cloud computing has become one of the most modern topics in the IT world today. Its model of computing as a resource has changed the scenery of computing as we know it, and its promises of increased flexibility, greater consistency, massive scalability, and decreased costs have enchanted businesses and individuals alike.

Cloud computing, as defined by NIST, is a model for enabling always-on, convenient, on-demand network access to a shared pool of configurable computing can be rapidly provisioned and released with nominal management effort or service provider interaction [1]. It is a new model of providing computing resources that utilizes existing technologies. At the heart of cloud computing is a datacenter that uses virtualization to isolate instances of applications or services being hosted on the "cloud". The datacenter provides cloud users the ability to hire computing resources at a rate dependent on the datacenter services being requested by the cloud user. Refer to the NIST definition of cloud computing, [1], for the core tenets of cloud computing.

In this paper, we refer to the organization providing the datacenter and related management services as the cloud provider. We refer to the organization using the cloud to host applications as the cloud service provider (CSP).

Lastly, we refer to the individuals and/or organizations using the cloud services as the cloud clients or cloud users.

NIST defines three main service models for cloud computing:

- ✓ Software as a Service (SaaS) – The cloud provider provides the cloud consumer with the capability to deploy an application on a cloud infrastructure [1].
- ✓ Platform as a Service (PaaS) – The cloud provider provides the cloud consumer with the capability to develop and deploy applications on a cloud infrastructure using tools, runtimes, and services supported by the CSP [1].
- ✓ Infrastructure as a Service (IaaS) – The cloud provider provides the cloud consumer with essentially a virtual machine. The cloud consumer has the ability to provision processing, storage, networks, etc., and to deploy and run arbitrary software supported by the operating system run by the virtual machine [1].

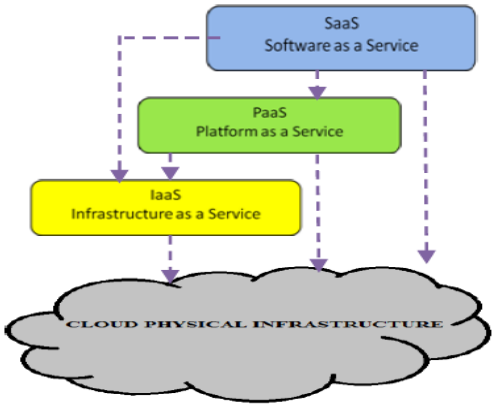

Figure 1: Cloud Service Delivery Model

NIST also defines four deployment models for cloud

computing: public, private, hybrid, and community clouds.

- ✓ Private cloud – The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.
- ✓ Community cloud - The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.
- ✓ Public cloud - The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.
- ✓ Hybrid cloud - The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

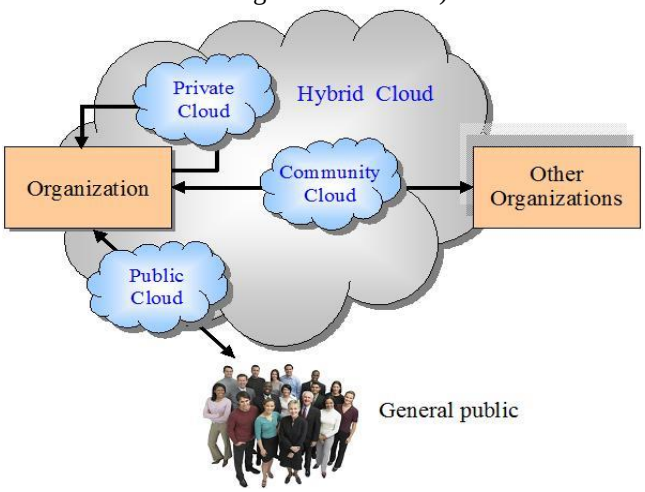

Figure 2: Cloud Service Delivery Model

One of the most appealing factors of cloud computing is its pay-as-you-go model of computing as a resource. This new model of computing has allowed businesses and organizations in need of computing power to purchase as many resources as they need without having to put forth a large capital investment in the IT infrastructure. Other advantages of cloud computing are massive scalability and increased flexibility for a relatively constant price. [2].

Despite the many advantages of cloud computing, many large enterprises are hesitant to adopt cloud computing to replace their existing IT systems. In the Cloud Computing Services Survey done by IDC IT group in 2009, over 87% of those surveyed cited security as the number one issue preventing adoption of the cloud [3]. For adoption of cloud computing to become more extensive, it is important that the security issue with cloud computing be analyzed and addressed, and proposed solutions be implemented in existing cloud offerings.

II. SCHEME FOR ANALYZING SECURITY IN THE CLOUD

Beginning in the 1980s, governmental initiatives were established around the world to define requirements for evaluating the effectiveness of security functionality built into computer systems. In 1996, initiatives from the US, Europe, and Canada were combined into a document known as the Common Criteria. The Common Criteria document was approved as a standard by the International Organization for Standardization in 1999 and has opened the way for worldwide mutual recognition of product security solutions [4].

The Common Criteria, however, serve primarily as a benchmark for security functionality in products [4]. For this reason, cloud service providers consolidated and reclassified the criteria into five functional security subsystems. We have used these subsystems as the framework within which we assess the security issues present in cloud computing and evaluate solutions proposed.

The five functional security subsystems defined by IBM are as follows:

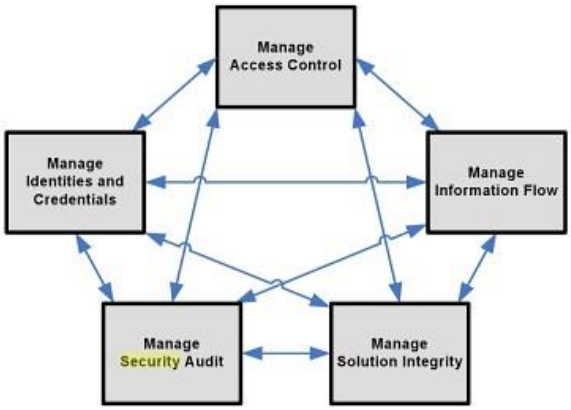

Figure 3: Security Architecture Subsystems

a. Audit and Compliance: This subsystem addresses the data collection, analysis, and archival requirements in meeting standards of proof for an IT environment. It captures, analyzes, reports, archives, and retrieves records of events and conditions during the operation of the system [4].
b. Access Control: This subsystem enforces security policies by gating access to processes and services within a computing solution via identification, authentication, and authorization [4]. In the context of cloud computing, all of these mechanisms must also be considered from the view of a federated access control system.
c. Flow Control: This subsystem enforces security policies by gating information flow and visibility and ensuring information integrity within a

computing solution [4].

d. Identity and Credential Management: This subsystem creates and manages identity and permission objects that describe access rights information across networks and among the subsystems, platforms, and processes, in a computing solution [4]. It may be required to adhere to legal criteria for creation and maintenance of credential objects.
e. Solution Integrity: This subsystem addresses the requirement for reliable and proper operation of a computing solution [4].

III. INVESTIGATION OF ISSUES AND LATENT SOLUTIONS INSIDE CLOUD COMPUTING SECURITY

A. *Review and Agreement*

Cloud computing raises issues regarding compliance with existing IT laws and regulations and with the division of compliance responsibilities.

- Compliance with laws and regulations

Regulations written for IT security require that an organization using IT solutions provide certain audit functionality. However, with cloud computing, organizations use services provided by a third-party. Existing regulations do not take into account the audit responsibility of a third-party service provider [5].

The division of audit responsibilities required for regulatory compliance must be clearly delineated in the contracts and service-level agreements (SLAs) between an organization and the cloud provider.

In order to comply with audit regulations, an organization defines security policies and implements them using an appropriate infrastructure. The policies defined by an organization may impose more stringent requirements than those imposed by regulations. It falls on the customer of the cloud services to bridge any gap between the audit functionality provided by the CSP and the audit mechanisms required for compliance [5].

The CSA states that the SLA between the cloud consumer and provider should include a Right to Audit clause, which addresses audit rights as required by the cloud consumer to ensure compliance with regulations and organization-specific security policies [5].

Even though a general approach to involve legal has been described by the CSA, no formal APIs or frameworks for integration of multiple audit systems have been defined. Additionally, there are no specific standards or models that define the separation of responsibilities between CSP and cloud service consumer.

B. *Admission control*

Admission management is one of the toughest issues facing cloud computing security [5]. One of the fundamental differences between traditional computing and cloud computing is the distributed nature of cloud computing. Within cloud computing, access management must therefore be considered from a federated sense, where an identity and access management solution is utilized across multiple cloud services and potentially multiple CSPs.

Admission control can be separated into the following functions:

- Authentication

An organization can utilize cloud services across multiple CSPs, and can use these services as an extension of its internal, potentially non-cloud services. It is possible for different cloud services to use different identity and credential providers, which are likely different from the providers used by the organization for its internal applications. The credential management system used by the organization must be consolidated or integrated with those used by the cloud services [5].

The CSA suggests authenticating users via the consumer's existing identity provider and using federation to establish trust with the CSP [5]. It also suggests using a user-centric authentication method, such as OpenID, to allow a single set of credentials to be used for multiple services [5].

Use of an existing identity provider or a user-centric authentication method reduces complexity and allows for reuse of existing systems. If done using standardized federation service, it also increases the potential for seamless authentication with multiple different types of cloud services. The CSA states that in general, CSPs and consumers should give preference to open standards, which provide greater transparency and hence the ability to more thoroughly evaluate the security of the approach taken.

- Authorization

Requirements for user profile and access control policy vary depending on whether the cloud user is a member of an organization, such as an enterprise, or as an individual. Access control requirements include establishing trusted user profile and policy information, using it to control access within the cloud service, and doing this in an auditable way [5].

Once authentication is done, resources can be authorized locally within the CSP. Many of the authorization mechanisms that are used in traditional computing environments can be utilized in a cloud setting.

- Federated sign-on

A federation is a group of two or more organizations that have agreed upon standards for operation [6]. Federations allow multiple, disparate entities to be treated in the same way. In cloud computing, federated sign-on plays a vital role in enabling organizations to authenticate their users of cloud services using their chosen identity provider.

If an organization uses multiple cloud services, it could suffer from the difficulty of having to authenticate multiple times during a single session for different cloud services. The Cloud Computing Use Cases Discussion Group suggests that the multiple sign-on problem can be solved by using a federated identity system. The federated identity system would have a trusted authority common to multiple CSPs, and provide single or reduced sign-on through the common authority [7].

C. *Flow control*

Information flow control is central to interactions between the CSP and cloud consumer, since in most cases, information is exchanged over the Internet, an unsecured and uncontrollable medium. Flow control also deals with the

security of data as it travels through the data lifecycle within the CSP – creation, storage, use, sharing, archiving, and destruction.

A cloud is shared by multiple service consumers, and by their very nature, cloud architectures are not static and must allow flexibility and change. Securing the flow of data across the cloud service consumer and providers and across the various components within a CSP becomes challenging and requires extensions of mechanisms used in more static environments of today.

Flow control can be separated into the following functions:

- Secure exchange of data:

Since most cloud services are accessed over the Internet, an unsecured domain, there is the utmost need to encrypt credentials while they are in transit [5]. Even within the cloud provider's internal network, encryption and secure communication are essential, as the information passes between countless, disparate components through network domains with unknown security, and these network domains are shared with other organizations of unknown reputability. Controls should be put in place at multiple levels of the network stack. At the application layer, Shipping Chen et. al. [8] suggest using application-specific encryption techniques to ensure adequate security of the data for the particular application. At the transport layer, Xiao Zhang et. al. [9] suggest using standard cryptographic protocols, such as SSL and TLS. At the network layer, Chen et. al. [8] suggest using network-layer controls, such as VPN tunneling, to provide easy-to-implement, secure connection with a CSP.

- Data security lifecycle

The data security lifecycle tracks the phases through which data goes from creation to destruction. It is composed of the six phases given below. Refer to [5] and [10] for descriptions of these phases.

Build phase: As soon as data is created, it can be tampered with. It could be improperly classified or have access rights changed by intruders, resulting in loss of control over the data [10]. The CSA suggests that organizations use data labeling and classification techniques, such as user tagging of data, to mitigate the improper classification of data [5].

Store phase: Because CSPs are third-parties, the complete security of CSP systems is unknown, so data must be protected from unauthorized access, tampering by network intruders, and leakage [10]. Due to the multi-tenant nature of cloud computing, controls must be put in place to compensate for the additional security risks inherent to the commingling of data.

In order to prevent legal issues based on the physical location of data, the CSA suggests that the cloud consumer stipulate its ability to know the geographical location of its data in the SLA and ensure that the SLA include a clause requiring advance notification of situations in which storage may be seized or data may be subpoenaed [5].

Use and Share phase: During the use phase, which includes transmission between CSP and consumer and data processing, the confidentiality of sensitive data must be protected from mixing with network traffic with other cloud consumers. If the data is shared between multiple users or organizations, the CSP must ensure data integrity and consistency. The CSP must also protect all of its cloud service consumers from malicious activities from its other consumers [10].

Record phase: As with the storage phase, data must be protected against unauthorized access by intruders, and from malicious co-tenants of the cloud infrastructure. In addition, data backup and recovery schemes must be in place to prevent data loss or premature destruction [5].For data in a live production database, the CSA suggests using at-rest encryption – having the CSP encrypt the data before storage [5]. For data that will be archived, it recommends that the cloud consumer perform the encryption locally before sending the data to the CSP to decrease the ability of a malicious CSP or co-tenant from accessing archived data [5].

Demolish phase: Data persistence is the biggest challenges present in the destroy phase. For data to be completely destroyed, it must be erased, rendered unrecoverable, and as appropriate, physically discarded [5].The CSA suggests a plethora of techniques to be used by CSPs to ensure that data is completely destroyed, including disk wiping, physical data destruction techniques, such as degaussing, and crypto-shredding [5].

D. Identity/credentials (management)

Within cloud computing, identity and credential management entails provisioning, deprovisioning, and management of identity objects and the ability to define an identity provider that accepts a user's credentials (a user ID and password, a certificate, etc.) and returns a signed security token that identifies that user. Service providers that trust the identity provider can use that token to grant appropriate access to the user, even though the service provider has no knowledge of the user [7].

An organization may use multiple cloud services from multiple cloud providers. Identity must be managed at all of these services, which may use different identity objects and identity management systems.

In addition, provisioning and deprovisioning of identities for an organization's IT system is traditionally done manually and infrequently. With cloud computing, access to services changes more rapidly than it would in a traditional IT application, so provisioning and deprovisioning of identities must be dynamic.

Federated identity management allows an organization to rapidly manage access to multiple cloud services from a single repository. An organization can maintain a mapping of master identity objects to identities used by multiple applications within the organization's IT system. Cloud customers should modify or extend these repositories of identity data so that they encompass applications and processes in the cloud [5].

Currently, CSPs provide custom connectors for communication of identity and access control objects. The capabilities currently provided by CSPs are inadequate for enterprise consumers. Custom connectors unique to cloud providers increase management complexity, and are not flexible, dynamic, scalable, or extensible [5].

Researchers at IBM Research – China [11] suggest using a brokered trust model, where a third-party broker server is used to establish the trust with a cloud service user. The business agreement between the CSP and the identity broker allows the CSP to place trust in the broker, allowing it to act

as an agent for the CSP to establish trust with other parties, such as organizations using cloud services [11]. The organizations can then take advantage of their own identity federation services to relay credential information for authentication with the cloud service.

Such an approach reduces the CSP's cost of establishing multiple trust relationships with multiple service users. It also pushes complexity to the trust broker, which can support more forms of federated identities. From the consumer's perspective, if multiple CSPs utilize same trust broker, establishing trust with multiple different types of services can be done by establishing trust with single trust broker.

E. Solution integrity

Within the realm of cloud computing, solution integrity refers to the ability of the cloud provider to ensure the reliable and correct operation of the cloud system in support of meeting its legal obligations, e.g., SLAs, and any technical standards to which it conforms. This encompasses protecting data while it is on the cloud premises, both cryptographically and physically; preventing intrusion and attack and responding swiftly to attacks such that damage is limited; preventing faults and failures of the system and recovering from them quickly to prevent extended periods of service outage; and protection of cloud tenants from the activities of other cloud tenants, both direct and indirect.

- Incident response and remediation

Even though solutions are run by the cloud provider, cloud providers have an obligation to both their customers and to regulators in the event of a breach or other incident. In the cloud environment, the cloud consumer must have enough information and visibility into the cloud provider's system to be able to provide reports to regulators and to their own customers.

The CSA suggests that cloud customers clearly define and indicate to cloud providers what they consider serious events, and what they simply consider incidents [5]. For example, a cloud consumer may consider a data breach to be a serious incident, whereas an intrusion detection alert may just be an event that should be investigated.

- Fault acceptance and failure recovery

For a CSP, one of the most devastating occurrences can be an outage of service due to a failure of the cloud system. For example, Amazon's EC2 service went down in April 2011, taking with it a multitude of other popular websites that use EC2 to host their services. Amazon Web Services suffered a huge blow from this outage. CSPs must ensure that zones of service are isolated to prevent mass outages, and have rapid failure recovery mechanisms in place to counteract outages.

The CSA recommends that cloud customers inspect cloud provider disaster recovery and business continuity plans to ensure that they are sufficient for the cloud customer's fault tolerance level [5].

IV. CONCLUSIONS AND FUTURE WORK

Cloud computing is an extension of existing techniques for computing systems. As such, existing security techniques can be applied within individual components of cloud computing. However, because of the inherent features of cloud computing, such as resource pooling and multitenancy, rapid elasticity, broad network access, and on-demand self-service, existing security techniques are not in themselves adequate to deal with cloud security risks.

Cloud providers exist in the market today, so the cloud paradigm has already overcome its initial security hurdles and moved from theory into reality. However, current cloud providers have provided extremely proprietary solutions for dealing with security issues. Execution of a single business process requires the participation of multiple, interoperating providers and consumers. In addition, for cloud computing to be used in a wide scale and really deliver on its promised benefits of elasticity, scalability, flexibility, and economies of scale, the focus of security needs to shift towards devising techniques to enable federation of security functions that are used today.

Further, the federation should allow the cloud consumers to commission and decommission services from various CSPs with flexibility and agility. Finally, interest research problems will arise when we consider cloud computing security together with classical quality-of-serve issues [12,13] and distributed computing issues [14] in a network-wide scope where cloud (storage) systems are implemented in a distributed manner.

Due to multitenancy, there is a need to logically isolate the data, computing, manageability, and audit ability of users co-tenant on the same physical infrastructure at an individual component level, across architectural layers, and across multiple providers. Hence, security mechanisms and approaches that enable the abovementioned isolation in a standardized way need more scrutiny in the future.

REFERENCES

[1] National Institute of Standards and Technology, NIST Definition of Cloud Computing, Sept 2011.
[2] Armbrust, M. et. al., (2009), "Above the clouds: A Berkeley view of Cloud Computing", UC Berkeley EECS, Feb 2013.
[3] Ramgovind, S.; Eloff, M.M.; Smith, E., "The management of security in Cloud computing," Information Security for South Africa, 2010 , vol., no., pp.1-7, 2-4 Aug. 2014.
[4] IBM Corporation, Enterprise Security Architecture Using IBM Tivoli Security Solutions, Aug 2007.
[5] Cloud Security Alliance, Security Guidance for Critical Areas of Focus in Cloud Computing V2.1, 2009.
[6] "Federated identity management." Internet: http://en.wikipedia.org/wiki/Federated_identity_ management, [Dec. 16, 2011].
[7] Cloud Computing Use Case Discussion Group, Cloud Computing Use Cases Whitepaper v4.0, July 2010.
[8] Shiping Chen; Nepal, S.; Ren Liu, "Secure Connectivity for Intra-cloud and Inter-cloud Communication," Parallel Processing Workshops (ICPPW), 2011 40th International Conference on , vol., no., pp.154-159, 13-16 Sept. 2011.
[9] Xiao Zhang; Hong-tao Du; Jian-quan Chen; Yi Lin; Lei-jie Zeng, "Ensure Data Security in Cloud Storage," Network Computing and Information Security (NCIS), 2011 International Conference on , vol.1, no., pp.284-287, 14-15 May 2011.
[10] Xiaojun Yu; Qiaoyan Wen, "A View about Cloud Data Security from Data Life Cycle," Computational Intelligence and Software Engineering (CiSE), 2010 International Conference on , vol., no., pp.1-4, 10-12 Dec. 2010.
[11] He Yuan Huang; Bin Wang; Xiao Xi Liu; Jing Min Xu, "Identity Federation Broker for Service Cloud," Service Sciences (ICSS), 2010 International Conference on , vol., no., pp.115-120, 13-14 May 2010.
[12] Shigang Chen, Meongchul Song, Sartaj Sahni, Two Techniques for Fast Computation of Constrained Shortest Paths, IEEE/ACM Transactions on Networking, vol. 16, no. 1, pp. 105-115, February 2008.

[13] King-Shan Lui, Klara Nahrstedt, Shigang Chen, Hierarchical QoS Routing in Delay-Bandwidth Sensitive Networks, in Proc. of IEEE Conference onLocal Area Networks (LCN'2000), pp. 579-588, Tampa, FL, November 2000.

[14] Shigang Chen, Yi Deng, Attie Paul, Wei Sun, Optimal Deadlock Detection in Distributed Systems Based on Locally Constructed Wait-for Graphs, in Proc. of 16th IEEE International Conference on Distributed Computing Systems (ICDCS'96),HongKong,May1996.