Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 02, February-2017

Securing the Users' Data in Cloud Storage: A Survey

Dr. R. Kalaichelvi
Assistant Professor
College of Administrative and Financial Sciences
AMA International University Bahrain
Kingdom of Bahrain

Abstract - **Gradually becoming ubiquitous since 2007, cloud computing is an on-demand computing which evolves from grid computing, service-oriented architecture, utility computing and virtualization. Users having a Personal Computer (PC) or a Laptop with internet access can avail the cloud services at anytime, anywhere and for any number of times without any prerequisites. Virtualization is the backbone of Cloud computing and all of cloud services are virtualized. Cloud provides unlimited services provisioning to the users through the pay per use model. Due to attractive characteristics and benefits, an increasing number of users are adopting cloud services day by day. Most of the users prefer public cloud for the utility services. One of the primary uses of cloud services is the possibility to store data on cloud. Cloud has multiple data centers situated in different geographical locations where the users' data are replicated and stored. However, this feature of cloud computing brings up several security issues and challenges. Data protection is the biggest security issue in cloud. Data in the cloud storage can be hacked by unauthorized users. Attacks may be by either administrator from Cloud Service Providers (CSP) called insiders or other users of the CSP called outsiders. Securing the users' data in cloud storage is of utmost importance since cloud users are the biggest beneficiary of the cloud.**

Keywords- Utility Computing; Vertualization; Cloud Storage; Security; Cloud Service Providers.

I. INTRODUCTION

Cloud computing is an emerging powerful technology. It is an Internet-based service delivery model. According to Alvin Toffler, there are three waves of evolution in the universe, viz, i) agricultural age ii) industrial age and iii) information age [1]. There are many sub waves in all these three waves. The cloud computing is a sub wave of "information age" wave. In this modern era, using cloud computing paradigm, any organization can just plug into the cloud world, like people plug into the electrical grid. Cloud computing is a service system where numerous essential resources are accessed by many sectors such as industry, academia, medical and the government. It delivers services to public in the form of hardware, software and storage, etc. Other way, it provides Everything (X) as a Service (XaaS) where 'X' denotes software, OS, server, hardware, storage, etc [2]. It is a mixture of various computing entities, globally separated, but electronically connected.

Cloud computing consists of multi-tenancy, reliability, scalability, availability, performance, security and maintenance features. Business software, email, Banking transaction and web content management can be offered through cloud environment. The US National Institute of Standards and Technology (NIST) defines cloud as follows: "Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with a minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three delivery models, and four deployment models" [3].

The major feature of cloud computing is that it allows sharing and scalable deployment of services, as required by the users, from any location. Cloud computing saves time and money during software upgrade. Cloud services are updated by the provider, so the users are always working on the latest platform [4]. Cloud minimizes the amount of wasted computing resources and can also reduce energy consumption significantly.

With the advent of cloud computing usage, adoption of cloud storage has become very simple. It presents the users with a means for storing the data online. The users can remotely access the data at any time. Cloud computing has taken IT to a higher level by giving people of the digital world the ability to store information with bendable and measurable processing capability to cope up with the expanding need of demand and supply, whilst reducing capital expenditure. It has exhibited enormous progress in empowering high performance and quantifiable available data maintenance.

II. ESSENTIAL CHARACTERISTICS

Cloud has five essential characteristics which provide it with unique features that are unavailable with other computing [5].

On-Demand Self-Service**:** It enables users to access cloud computing resources from the Cloud Service Providers (CSP) without human intervention. Instant usage of resources and elimination of human intervention result in improved efficiencies and cost savings to both the users and the CSPs.

Broad Network Access: Cloud computing is an efficient and effective replacement for in-house data centers. High-bandwidth communication links must be available to connect to the cloud services. High-bandwidth network communication provides access to a large pool of computing resources.

Location-Independent and Resource Pooling: Computing resources are pooled to serve multiple users using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to users' demand. Applications require resources. However, these resources can be physically located in any geographic locations and assigned as virtual components whenever they are needed. The location independence creates a perception that the users generally have no control or knowledge over the exact location of the provided resources. At the same time, this helps to specify location at a higher level of abstraction (e.g., country, state, or data center).

Scalability: It enables new nodes to be added or dropped from the network like physical servers, with limited modifications to infrastructure set up and software. Cloud architecture can scale horizontally or vertically, according to user's demand.

Measured Service: The usage of cloud resources by the users are monitored by APIs in the cloud. Users are billed automatically based on the usage of cloud resources. Cloud systems automatically control and optimize resource usage by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be transparently monitored, controlled, and reported for both the CSPs and the users of the utilized service.

III. CLOUD SERVICE MODELS

The cloud computing services are broadly divided into three categories namely, Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) [6].

Software as a Service (SaaS): The top layer provides the customer with ready to use application running on the infrastructure of service provider. The cloud service providers offer software to the clients through SaaS on demand. Users buy the rights to use and make use of an application or service that is hosted in the cloud. The necessary knowledge for the interaction between the consumer and the service provider is organized as an element of the facility in SaaS. Salesforce, DocLanding, Zoho and Workday are the examples of SaaS that are used for different purposes such as email, billing, human resource management etc.

Platform as a Service (PaaS): It is the middle layer that provides platform oriented service. PaaS is an application platform, wherein, users purchase access to the platform so that they can deploy their own software and the conventional applications with their services on the cloud. It distributes application development tools. Testing, collaborating, hosting, and managing applications are the services done by the PaaS. It conceals the details of the handling hardware. PaaS supports the construction and distribution of web based applications online. Google App Engine, LoadStorm are the examples of PaaS for running web applications and testing their performances.

Infrastructure as a Service (IaaS): The bottom layer provides infrastructure service. IaaS provides the customers the virtual devices that persuade the necessities on the needs of the customers' services and the applications such as, memory, CPU, OS and data space. IaaS presents an intermediary policy to run subjective OS and software in case of service constraints. The consumer can deploy and run software. It reduces hardware costs. License cost is reduced in all layers. Creating virtual machines, setting hosts, acquiring inter host communication are the areas covered in IaaS. Amazon S3 and FlexiScale are the best examples of IaaS for storage and maintaining virtual servers.

IV. DEPLOYMENT MODELS

Cloud is deployed in four types of deployment models as defined by NIST such as Public, Private, Community and Hybrid cloud [7, 8].

Public Cloud: This cloud infrastructure is utilized for public or large industry group; and it serves multiple tenants. This model is offered through the web applications or the online website services wherein sharing the host information or the application is possible. A third party buys this kind of cloud model and the user can use the services by paying a certain amount based on the efficacy. However, public cloud shares same infrastructure with many clients.

Private Cloud: Private cloud is mainly used by organizations for their internal usage within their firewalls which are owned and managed by the company itself. The user working for that company can alone make use of the resources available on the cloud which is bought by the owner. The user can make use of the virtualized resources for the healthy management of the same.

Hybrid Cloud: A hybrid model, as the name itself suggests, is a combination of the public and private clouds. There are various internal as well as external suppliers of the cloud. The users use private or public cloud depending on the criticality of the data transfer. Private cloud is used mainly when crucial, confidential information needs to be transferred, whereas, the public cloud is used mainly to handle large transactions smoothly at peak timings.

Community Cloud: This is a kind of substructure which is allocated to various organizations, which is normally delivered on private cloud. The advantage of using a community cloud is that the supplier can have as many numbers of clients as he gets and can charge for organizations individually.

V. CLOUD COMPUTING SYSTEM ARCHITECTURE

The current cloud computing system consists of three layers: software layer, platform layer and infrastructure layer. The software layer provides the interfaces for users to use CSPs' applications running on a cloud infrastructure. The platform layer provides the operating environment for the software to run using system resources. The infrastructure layer provides the hardware resources for computing, storage and networks [9]. A cloud is structured in seven layers on the basis of Cloud Security Alliance: 1) Facility Layer, 2) Network Layer, 3) Hardware Layer, 4) OS Layer, 5) Middleware Layer, 6) Application Layer and

7)The User Layer [10, 11]. The CSPs or the cloud users can manage these layers. The cloud computing architecture with these layers is shown in Fig. 3.

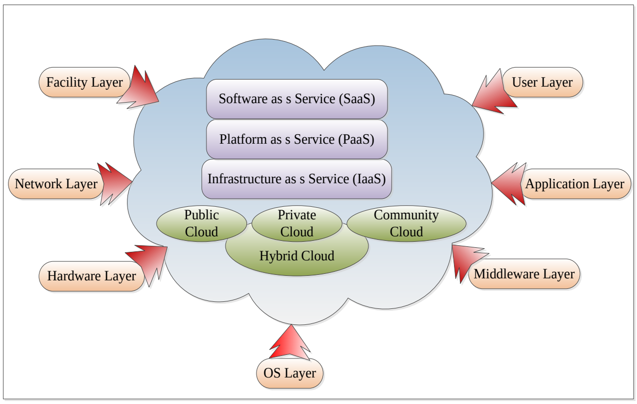

Fig. 3. Current Cloud Computing Architecture

VI. NEED FOR CLOUD STORAGE

One of the full-fledged cloud services provided by cloud computing is cloud storage. Originally, the cloud service providers that offer remote storage service were called as Storage Service Providers (SSPs). Cloud Storage is becoming an increasingly popular paradigm through which cloud service providers offer a service known as "Database as a Service" (DaaS) where users' data are stored and maintained [12].

The main advantages of cloud storage are:

- Significant cost savings and service benefits, and,
- Higher availability and better protection effectiveness than in-house operation.

The cloud storage allows the cloud users to store the users' incredible amount of data in the database server. Then, the cloud service providers monitor and maintain the data and provide maximum availability and efficient recovery of data.

Cloud users may be public, start-ups or well established businesses [13]. The cloud users could be of two types: Data Owner (DO) and Data User (DU). If the DOs and DUs are same, the data storage and retrieval from the cloud are relatively easy. While, if the DOs and the DUs are different, i.e. the DUs are the employees of the same organization, but are located in a different location, then the data storage and data access need different mechanisms, as they need permission to access the cloud stored data. Fig. 1 and Fig. 2 represent the above mentioned mechanisms.

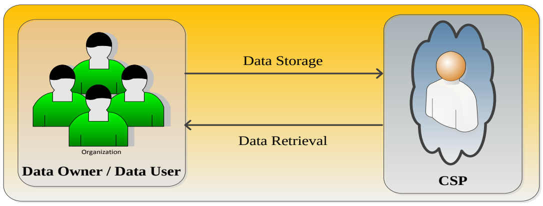

Fig. 1. Cloud Storage – Data Owners and Data Users are same

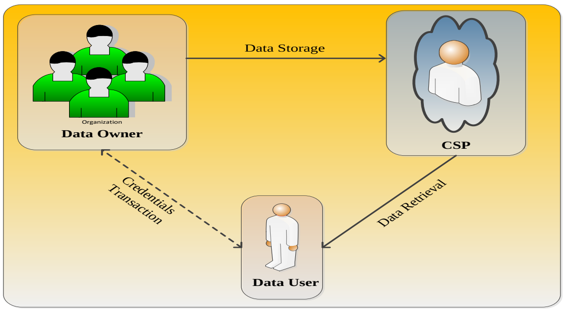

Fig. 2. Cloud Storage – Data Owners and Data Users are Different

The cloud storage paradigm helps the cloud users to store their highly sensitive data in remotely located servers. Nevertheless, the DOs lose control on their own data. Besides, the DUs have no power over the data in cloud storage. As cloud may not be a trusted domain, there can be risks of data confidentiality. There is a possibility of unacceptable use of data that may be made by the CSP itself. The traditional access control techniques may prevent data access by external users, but not by internal administrators.

VII. DATA MANAGEMENT IN CLOUD STORAGE

The data storage and data management are crucial aspects for enterprises [14]. As these responsibilities are a burden to the enterprises, they are interested in getting the benefits from the cloud paradigm, for outsourcing their data via internet. The service offered by cloud computing is used to store and manage data. This is referred to as Database as a Service (DaaS) [15]. DaaS is one of the most important applications of SaaS delivery model. DaaS model provides many benefits to enterprises as it saves the cost of database administration, and offers reliable storage.

Once the data is stored on cloud, the DOs are disconnected from their data. However, the Data Base Administrators (DBAs) of the DaaS model manage the enterprises' data. The DBAs of CSP have the responsibilities, such as, database backup, database restoration, database recovery in the case of data crash and also to achieve performance and fine-tuning of the database [16]. This state may lead to unauthorized access of data by the DBAs of CSP themselves, as the DOs have no control of the cloud stored data. Additionally, the multi-tenancy feature of cloud allows multiple users to use the computational resources of same CSP. Hence, there are possibilities that the other users can access the data illegally. Due to these factors, despite the attractiveness of the DaaS model, it is not successful [17].

VIII. NEED FOR DATA SECURITY IN CLOUD STORAGE

Security of data in cloud is a challenge and is of supreme importance as many flaws and concerns are yet to be identified. Data protection is a crucial security issue for most of the enterprises [18]. The management of the data and services [19] may not be fully trustworthy and the enterprises do not have any control on the data, since the data centers are remotely located. Moreover, data are stored in a multitenant environment. The common security concerns are: 1. Data Security, 2. Software Interfaces Security, 3. User Access Control and 4. Data Separation. Since, data in cloud computing is placed in the hands of third parties, ensuring the data security is of great importance. Given the large number of issues concerning data security, many organizations need clear answers regarding data security before migrating to the cloud. The users' data confidentiality and integrity are maintained by providing data security which is an important quality of service in cloud computing. Data security in network, host and application levels has become a vital part of cloud storage [20]. The data in cloud can be in any of the forms as shown in Fig. 4 [21]:

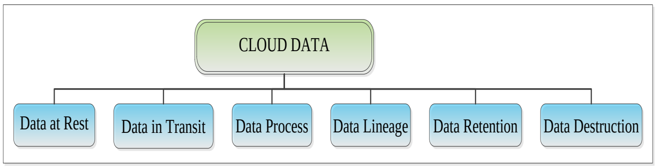

Fig. 4. Cloud Data Forms

Hence**,** data security of all the above mentioned forms is the most vital factor to be considered. Users' Data at Rest which stored on the physical storage should not be modified. Encrypting the data may be the solution for this, but in case of PaaS and SaaS models, encryption of data is not always feasible and hence the probability of unauthorized access is very high. Furthermore, data must be secured while transferring between servers. It should not be viewed or changed by other users. So, it requires an appropriate encryption algorithm, as well as, a secure protocol. Also, Users' data should not be viewed or changed by other user at runtime. Finally, data lineage deals with maintaining the origin and custody of data in order to prevent tampering and to assure the integrity of data. However, this is a time-consuming job. Trying to provide accurate reporting on data lineage for public cloud services is not possible.

IX. SECURITY REQUIREMENTS FOR CLOUD STORAGE

Cloud service providers should supply data security measures in order to gain the users' trust [22]. Though the CSPs offer security actions, there are possibilities that the cloud users expect to have other security mechanisms to protect their data [23]. As the CSPs can access the data stored in their servers, misuse the data for their gain, it can result in a great loss to the data owners. Additionally, DUs store the data in a virtual environment in cloud; they do not know who is managing their data. Hence, the users are very much worried about the safety of the cloud-stored data. The users of cloud can be public or businesses which process sensitive information. So, the degree of security also varies with types of cloud users. The data of public sources may not require a high degree of security [24]. On the other hand, businesses, banks, other financial establishments or governments require a high level of security for their sensitive data in cloud. As a result, to ensure security, the users must take proactive measures to secure their data. In order to have a secured cloud system, the following aspects of security parameters are considered for data protection:

1. AUTHENTICATION

Authentication is a method of guaranteeing the users' identity. The potency of an authentication mechanism can be assessed on many things. It depends on what the user knows, possesses and has. Authentication is the process of verifying and validating the user's possession or the testimonial. There are many schemes that are projected for user authentication like textual password, graphical password, one time password, finger print, retina scan etc.

2. AUTHORIZATION

Authorization determines the privileges of users. Authorization is the process of allocating the degree of access to services and resources by clients. It is the process of providing clients permission to access the services based on defined access policies from cloud services providers. This decision is made after authenticating the identity of users. When considering an authentication system for a particular application, it is crucial to understand the type of identifier required to provide a certain level of authorization.

3. CONFIDENTIALITY

Confidentiality is an attribute that keeps the information of the users across the cloud concealed so that even privacy for each user is ensured. Data confidentiality is a measure of the capacity of any scheme to protect its data. Confidentiality is very much required when the data stored on cloud should not be read by unauthorized users. Hence, the data should not be sent in an intelligible format. A loss of confidentiality results in the unauthorized disclosure of information. Cryptographic technique is the solution to ensure the confidentiality of cloud-stored data.

4. INTEGRITY

Integrity is ensuring that the data presented are true and valid. It also includes guarding against improper data modification. A loss of integrity is identified by unauthorized modification, insertion, or destruction of information. One way of ensuring data integrity is using simple checksums which prevent an attacker from forging or replaying messages.

5. NON-REPUDIATION

Non-repudiation is a process of ensuring that a traceable legal record is kept and has not been changed by a malicious entity. A loss on non-repudiation would result in the questioning of the transaction that has occurred. A simple example of non-repudiation is signing a contract. The signers cannot claim that they did not agree a contract, because there is an evidence that they did agree.

X. CONCLUSION

The unique and attractive features of cloud computing have been fueling the integration of cloud storage in the enterprises. The mixture of pay-as-you-go with on-demand elastic operation of cloud makes the transition of on-premises storage to off-premises storage. The cloud storage reduces the capital expenditure and operational expenditure of users, as the users delegate the responsibilities to the cloud environment. Regardless of it benefits, it has many security concerns and issues. Hence, it is necessary to propose a new security framework to protect the outsourced data in public cloud storage environment.

REFERENCES

[1] Tim Mather, Subra Kumaraswamy and Shahed Latif, 2009. Data Security and Storage. In: Cloud Security and Privacy - An Enterprise Perspective on Risks and Compliance, O'Reilly Media, Inc., 61-71.

[2] Dawei Sun, Guiran Chang, Lina Sun and Xingwei Wang, 2011. Surveying and Analyzing Security, Privacy and Trust Issues in Cloud Computing Environments. Elsevier Journal of Advanced in Control Engineering and Information Science, Procedia Engineering. 2852-2856.

[3] NIST, 2012. Cloud Computing. http://www.nist.gov/itl/cloud/. Accessed Jan 2017.

[4] Armbrust M, Fox A, Griffith R, Joseph A. D, Katz R. H, Konwinski A, Lee G, Patterson D. A, Rabkin A, Stoica I. and Zaharia M., 2009. Above the clouds: A Berkeley View of Cloud Computing. EECS Department, University of California, Berkeley, Technical Report. 1-23.

[5] M.Malathi, 2011. Cloud Computing Concepts, 2Electronics Computer Technology (ICECT), IEEE, 236-239.

[6] R. Kalaichelvi, S. Shanmuga Priya, and L. Arockiam. Research challenges and security issues in cloud computing. *International Journal of Computational Intelligence and Information Security*, 2012, 3(3), pp.42-48.

[7] Peter Mell and Tim Grance, 2011. The NIST Definition of Cloud Computing Technical Report-800-145, Version 15, National Institute of Standards & Technology, Gaithersburg, MD, United States.

[8] R. Kalaichelvi and L. Arockiam, 2013. Secure and Robust Cloud Storage with Cryptography and Access Control. Elixir International Journal. 56: 13481-13484

[9] Arijit Ukil, Debasish Jana and Ajanta De Sarkar, 2013. A Security Framework in Cloud Computing Infrastructure. International Journal of Network Security & Its Applications. 5 (5): 11-24.

[10] Jonathan, 2011. Monitoring Cloud computing by layer part 1. Security & Privacy, IEEE. 9 (2): 66-68.

[11] Jonathan, 2011. Monitoring Cloud computing by layer part 2. Security & Privacy, IEEE. 9 (3): 52-55.

[12] Carlo Curino, Evan P. C. Jones, Raluca Ada Popa and Nirmesh Malviya, 2011. Relational Cloud: A Database-as-a-Service for the Cloud. Proceedings of Biennial Conference on Innovative Data Systems Research. 235-240.

[13] Fatima Trindade Neves, Fernando Cruz Marta, Ana Maria Ramalho Correia and Miguel de Castro Neto, 2011. The Adoption of Cloud Computing by SMEs: Identifying and Coping with External Factors. Proceedings of International Conference of the Portuguese Association of Information Systems - The Information Management in the age of Cloud Computing. 1-11.

[14] Waleed Al Shehri, 2013. Cloud Database Database as a Service. International Journal of Database Management Systems. 5 (2): 1-12.

[15] Carlo Curino, Evan P. C. Jones, Raluca Ada Popa and Nirmesh Malviya, 2011. Relational Cloud: A Database-as-a-Service for the Cloud. Proceedings of Biennial Conference on Innovative Data Systems Research. 235-240.

[16] Ramakrishnan Raghu, Gehrke Johannes, 2003. Database Management Systems. McGraw-Hill Higher Education, 3rd Edition (en). 282.

[17] Pardeep Sharma, Sandeep K. Sood, and Sumeet Kaur, 2011. Security Issues in Cloud Computing. High Performance Architecture and Grid Computing Communications in Computer and Information Science. 169: 36-45.

[18] Raman Chawla and Kirti Nagpal, 2013. Data Security Issues & Requirements in Cloud Computing. International Journal of Computing Science and Communication Technologies. 5 (2): 883-886.

[19] Bhardwaj, A. and V. Kumar, 2011. Cloud security assessment and identity management. Computer and Information Technology (ICCIT), IEEE, 14th International Conference, Dhaka. 387-392.

[20] Shucheng Yu, Wenjing Lou, and Kui Ren, 2012. Data Security in Cloud Computing. Handbook on Securing Cyber-Physical Critical Infrastructure, Chapter 15, Elsevier, Morgan Kaufmann Publisher. 389-410.

[21] R. Kalaichelvi and L. Arockiam, 2014. Enhanced User Access Control Architecture for Cloud Storage. International Journal of Advanced Research in Computer Science and Software Engineering. 4(3): 1111-1116.

[22] Hyun-Suk Yu, Yvette E. Gelogo and Kyung Jung Kim, 2012. Securing Data Storage in Cloud Computing. Journal of security Engineering. 9 (3): 251-260.

[23] Masayuki Okuhara, Telsuo Shiozaki and Tukuya Suzuki, 2010. Security Architecture for Cloud Computing. FUJITSU Science and Technology Journal. 46 (4): 397-402.

[24] R. Kalaichelvi and L.Arockiam, 2015. EnBloAES: A Unified Framework to Preserve Confidentiality of Data in Public Cloud Storage. Indian Journal of Science and Technology. 8(19): 1-8.