International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 - 5161
©2014 INPRESSCO®, All Rights Reserved
Available at http://inpressco.com/category/ijcet

General Article

An Analysis on Cloud Data Security and Accountability

Sandip. K. Bhagat[Á*] and G.P.Bhole[Á]

[Á]Dept of Computer Engineering and IT VJTI, Mumbai Maharashtra India

Accepted 10 July 2014, Available online 01 Aug 2014, **Vol.4, No.4 (Aug 2014)**

Abstract

Cloud computing is a technology that uses the internet and central remote servers to maintain data and applications. Cloud computing allows consumers and businesses to use applications and access their personal files at any computer with internet access. As it is publicly available, the security mechanisms are of highly concern. In this paper, we have analyzed different security and application aspects of cloud computing such as confidentiality, integrity, transparency, availability, accountability, assurance. Cloud data security has many issues like users data handled remotely by many users. User should get the information about the access of his data remotely. Here we have discussed cloud data security methods like RSA based storage security system, Cloud computing data security model and Cloud information accountability framework. We have also analyzed Accountability in the cloud. Finally we have drawn conclusion about which method is most suitable for which application or type of service in the cloud.

Keywords: *Cloud Computing, Data Security, Accountability*

1. Introduction

Cloud computing is an Internet-based super-computing model, it is a new method of shared infrastructure, it can provide a variety of IT services to large pool of computer resources. In the future, the computing and data resources will gradually migrate to the Web and the computing platform can achieve supercomputing and large-capacity storage in a relaxed way, while its computational overhead is much cheaper than the current computing and storage infrastructure. With cloud computing, the users don't need to deploy a high end client computing, they can access to computing power directly from the cloud and pay according to usage (Rajeev Kanday *et al*, 2012).

Now, the people continue to launch cloud-based applications, many users are trying to enjoy the benefits of these applications, especially SME, the users want cloud computing can help information technology companies improve the efficiency and reduce the costs of operation and maintenance. However, it due to the use of off-site cloud computing resources that the users will be placed their data in off-site data center, they may lost control over their data, they do not know where the data is saved, or how these data are modify or copy (Rajeev Kanday *et al*, 2012). They are most worried about the data security since their own data that they will be as originally stored in the local control to an external cloud computing services center. Therefore, it has become a major constraining factor to ensure the cloud data safety in the development of cloud computing.

This paper addresses the cloud data security issues and its various solutions, provides the ways of data security in the cloud. The Paper also addresses the Accountability issues and its solution. This paper is useful to the various research students and cloud security researches. The Section 2 consists of the cloud computing basics and the security issues in the cloud. Section 3 contains the cloud data security models which provide the ways of cloud data security. Section 4 describes the Accountability in the cloud environment. Section 5 describes the Analysis. Section 6 addresses the conclusion and future work.

2. Cloud computing and its security issues.

A. Cloud computing

The cloud computing has three service models Cloud Software as a Service (SaaS) , Cloud Platform as a Service (PaaS)and Cloud Infrastructure as a Service (IaaS). Similarly cloud computing has four service models.(Eman M.Mohamed *et al*, 2012) Private cloud: Enterprise owned or leased, Community cloud: Shared infrastructure for specific community, Public cloud: Sold to the public, mega-scale Infrastructure, Hybrid cloud: Composition of two or more clouds. Noting here some cloud computing benefits, the cloud has Lower computer costs, improved performance, reduced software costs, instant software updates, improved document format compatibility, unlimited storage capacity, device independence, and increased data reliability. And some cloud computing drawbacks as it Requires a constant Internet connection, does not work well with low-speed connections, can be slow, features might be limited, stored data might not be secure, and stored data can be lost. Some cloud computing providers are Amazon Web Services (AWS) -include Amazon S3, Amazon EC2, Amazon Simple-DB, Amazon SQS, Amazon FPS, and others.

*Corresponding author: **Sandip. K. Bhagat**

Salesforce.com - Delivers businesses over the internet using the software as a service model. Google Apps Software- as-a-service for business email, information sharing and security. And others providers such as Microsoft Azure Services Platform, Proof-point, Sun Open Cloud Platform, Workday and etc.(Eman M.Mohamed *et al*, 2012)

B. Security issues

The benefits of cloud adoption are numerous, including improved efficiency, reduced costs and greater accessibility and flexibility. Cloud computing is one of the fasted growing segments of the IT industry. However, as more information on individuals and companies is placed in the cloud, companies must address **cloud computing security issues**. As with other major business decisions, an enterprise must evaluate the benefits and be prepared to address any risks and challenges cloud adoption brings. Moving applications to the cloud and accessing the benefits means first evaluating specific **data security issues** and **cloud security issues** (Cong Wang *et al*, 2012). When enterprises move applications from on-premise to cloud-based, challenges arise from data residency, industry compliance requirements, privacy and third party obligations concerning the treatment of sensitive data. Corporate policies or the regulations of the governing jurisdictions impact the way sensitive data is managed including where it is located, what types of data can be collected and stored and who has access to it. These issues can determine the degree to which organizations can realize the value of cloud computing. Cloud security issues fall primarily into three areas:

Data Residency: Many companies face legislation by their country of origin or the local country that the business entity is operating in, requiring certain types of data to be kept within defined geographic borders. There are specific regulations that must be followed, centered around data access, management and control.

Data Privacy: Business data often needs to be guarded and protected more stringently than non-sensitive data. The enterprise is responsible for any breaches to data and must be able ensure strict cloud security in order to protect sensitive information.

Physical and personnel security: Providers ensure that the physical machines are adequately secure and that access to these machines as well as all relevant customer data is not only restricted but that access is documented.

Security of data at data center: Organizations are skeptical about the data security because of third party vendor and multi tenancy. Choice of cryptographic and hash algorithms used, how it works at transport layer and how data protected from other tenants being the center issue.

Multi- tenancy: It is the obvious choice for the cloud vendors for scalability but large enterprises see it as a weapon to exploit their huge database.

3. Cloud Data Security

A. RSA based storage security system

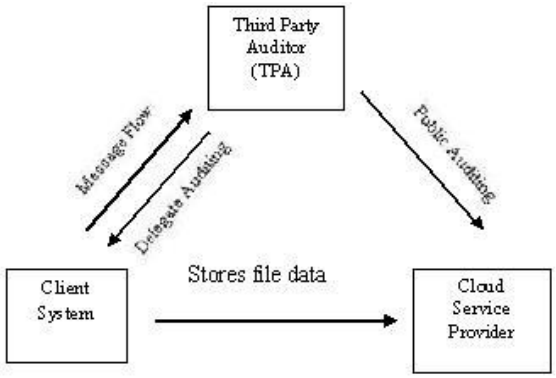

Fig.1. RSASS Data Flow Architecture(M.Venkatesh *et al*, 2012)

In the RSA based Storage Security (RSASS), there are three entities involved to carry out the overall process flow in the system (fig 1). The client generates the data and sends the file data to the remote cloud server. The remote cloud service provider stores the file data in its local data store. The client continuously monitors the stored file data in the server using the third party auditor (TPA). (M.Venkatesh *et al*, 2012)The TPA is a monitoring tool which analysis the integrity of the stored file in the server using the RSA based signature generation algorithm and report it to the client about the status of the file data. If the file is affected, any intrusion or attacks is notified to the client using proper message flow. In this paper, the security analysis of the stored file data using RSA algorithm is described.(M.Venkatesh *et al*, 2012)

Methodology

In the RSA based Storage Security system (RSASS), the security of the stored file data is continuously monitored using RSA based signature algorithm. It is based upon the concept of provable data possession (PDP) model. The PDP is a challenge and response protocol model. In the PDP model, the client using the monitoring tool, poses challenge to the cloud server and gets the proof for the challenge. The challenge is the subset of file blocks stored in the remote server and proof is the value generated for the selected subset of file blocks. The client verifies the proof that it received from the server and ensures the storage correctness of the file in the remote cloud server. RSASS consists of two phases namely setup phase and Integrity phase.(M.Venkatesh *et al*, 2012)

B. Cloud computing data security model

Data Security Model Description(Zhang Xin *et al*, 2012)
We can use the following mathematical model to describe typical cloud computing data technologies:
D s=C(name node);
Ms=S* Ds
C(.) Access to nodes, an application server of the system is denoted by name node in the formula;
D s: Block matrix of the file S;
M s : Block of data files in the data center of system;
S :File, file S in the system are represented as follows:

S={S(1),S(2),S(3),S(4), ... Sen)}, file S is a collection of n blocks of a file. Of which: S(i)nS(j)=Q,
i!=ij;i,j E 1,2,3,oo.n;
Based on basic principles of data security of cloud computing, we design security cloud cube model:
CCM DSM (Cloud Computing M ulti-dimension Date Security) in this paper, its mathematical model is indicated as follows:
D ;=C s(name node)
Ds=K.Ds'
Ms= E(S)Ds
Of which:
C s(.):Authorized application server access;
D;: File matrix in the privacy protected mode;
K: Users' secret matrix;
E(S): Encrypt the block of file S to get encrypted file vector; the security model in the following figure:

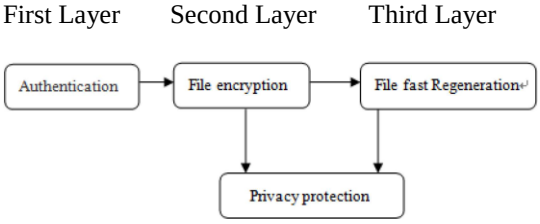

Fig. 2 Data security model Layered Architecture(Zhang Xin *et al*, 2012)

The model uses a hierarchical defending architecture with three layers. Every layer has its own responsibilities and is combined with each other to ensure data security in the cloud.
First layer: in charge of users' authentication, confers the appropriate digital certificates to users, manage users' permissions;
Second layer: in charge of encrypting users' data, and protects users' privacy by some means.
Third layer: fast recovers users' data and is the last layer of the system used to protect user data.(Zhang Xin *et al*, 2012)

The model adopts a multi-dimension architecture of three - layer defense. First of all, user authentication is required to ensure that user data cannot be tampered. Users who pass the authentication can make relative operation on the user data, such as addition, modification, deletion. If the unauthorized user use illegal means to deceive the authentication system, the file entered the system encrypt and privacy defense levels. In this layer, user data is encrypted. If key has been got by the intruder.(Zhang Xin *et al*, 2012) The user data cannot be got valid information even it is obtained through function of privacy protection. It is very important for commercial users of the cloud computing to protect their business secrets. The last is the file quick regeneration layer, user data can get maximum regeneration even it is damaged through rapid Regeneration algorithm in this layer. Each layer accomplishes its own job and combines with others to ensure data security in the cloud computing.

C. Cloud Information Accountability (CIA) Framework for Data Security and Accountability

The overall CIA framework, combining data, users, logger and harmonizer is sketched in Fig. 3. At the beginning, each user creates a pair of public and private keys based on Identity-Based Encryption (step 1 in Fig. 3). This IBE scheme is a Weil-pairing-based IBE scheme, which protects us against one of the most prevalent attacks to our architecture as described in Section. Using the generated key, the user will create a logger component which is a JAR file, to store its data items.

The JAR file includes a set of simple access control rules specifying whether and how the cloud servers, and possibly other data stakeholders (users, companies) are authorized to access the content itself. Then, he sends the JAR file to the cloud service provider that he subscribes to. To authenticate the CSP to the JAR (steps 3-5 in Fig. 3), we use OpenSSL based certificates, wherein a trusted certificate authority certifies the CSP. In the event that the access is requested by a user, we employ SAML-based authentication, wherein a trusted identity provider issues certificates verifying the user's identity based on his username.(Smitha Sundareswaran *et al*, 2012)

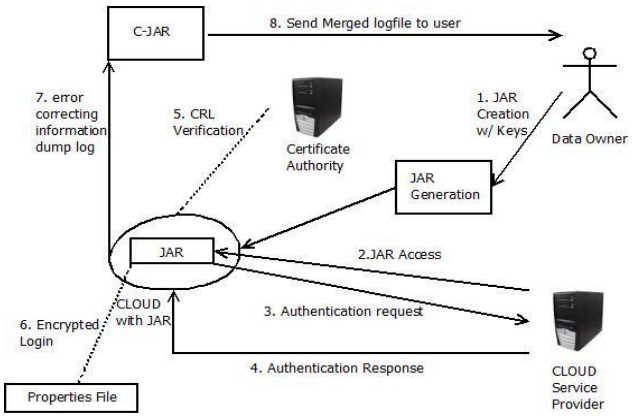

Fig 3: Overview of the cloud information accountability framework.

Once the authentication succeeds, the service provider (or the user) will be allowed to access the data enclosed in the JAR. Depending on the configuration settings defined at the time of creation, the JAR will provide usage control associated with logging, or will provide only logging functionality. As for the logging, each time there is an access to the data, the JAR will automatically generate a log record, encrypt it using the public key distributed by the data owner, and store it along with the data (step 6 in Fig. 3). The encryption of the log file prevents unauthorized changes to the file by attackers. The data owner could opt to reuse the same key pair for all JARs or create different key pairs for separate JARs. Using separate keys can enhance the security (detailed discussion is in Section) without introducing any overhead except in the initialization phase. In addition, some error correction information will be sent to the log harmonizer to handle possible log file corruption (step 7 in Fig. 3). To ensure trustworthiness of the logs, each record is signed by the entity accessing the content. Further, individual records are hashed together to create a chain structure, able to quickly detect possible errors or missing records. The

encrypted log files can later be decrypted and their integrity verified. They can be accessed by the data owner or other authorized stakeholders at any time for auditing purposes with the aid of the log harmonizer (step 8 in Fig. 3).(Smitha Sundareswaran *et al*, 2012)

As discussed in Section, our proposed framework prevents various attacks such as detecting illegal copies of users' data. Note that our work is different from traditional logging methods which use encryption to protect log files. With only encryption, their logging mechanisms are neither automatic nor distributed. They require the data to stay within the boundaries of the centralized system for the logging to be possible, which is however not suitable in the cloud.(Smitha Sundareswaran *et al*, 2012)

4. Accountability

Cloud computing involves certain risks which may make the access of data by the clients and unsafe tasks. Neither the client who puts his/her data on the cloud nor the cloud service provider can be held responsible for any kind of casualty In the system. At least one of them has to be held accountable to resolve the disputes if they arise. Thus the body which has to be held responsible for these accidents has to have a strong identity and it has to have a provision of storing transactions and when needed, auditing the same. To achieve this, a record of data manipulations has to be maintained which can be checked any time against a set of policies that are supposed to govern them.

For example if a person performs an action A, then that action can be scrutinized to see whether the person has done something wrong and can be thus held accountable. To achieve accountability in the cloud, we must make sure that we are able to trace even the smallest of activities taking place in the cloud, back to the person or entity who did it, so that the same can be held responsible for any kind of hazard. Whenever an activity is started and processed, an evidence/record of the same be simultaneously maintained for reviewing. The evidence should have sufficient information so that the activity can be justifiably traced and examined. This examination should be pursued continuously so that aptness of the action is assessed. Accountability is a big challenge because of the following reasons.

1) Misc configured machines may provide incorrect computation results.
2) Allocation of insufficient resources to the customers which may eventually lead to degradation of the performance of the customer services.
3) Releasing a virus by third party which may cause pilferage of the valuable data.
4) The inability of the cloud to provide data to the customer at the desired point of time or the loss of the data by the cloud. An accountable system must incorporate the under listed features/provisions to addressed the above mentioned challenges –

1) Each message should have a unique identity that can be linked to a node.
2) The system must have a secure record that is saved so that no entry can be deleted, or in any way tampered with.
3) The record should be continuously audited for faultfinding.
4) If a problem appears, the system should be able to determine the culprit so that the third party may judge accordingly.

5. Analysis

We studied all the above explained methods of the data security and Accountability. The method RSA Based Storage Security System addresses the Data Accountability by using Third Party Auditor.(M.Venkatesh *et al*, 2012)

Table 1: Analysis of cloud security methods

Method	Addresses Issues	Achieved Through
RSA Based Storage Security System	Accountability	Third Party Auditor.
Cloud Computing Data Security Model	Data Security	File Encryption.
Cloud Information Accountability (CIA) Framework	Data Security and Accountability.	JAR creation, File Encryption, Certificate Authority, Log generation

The method cloud computing data security model addresses data security by using file encryption at senders end and file description at recipient end.(Zhang Xin *et al*, 2012) Cloud Information Accountability (CIA) Framework addresses both the issues data security and the cloud data Accountability. All are achieved through JAR creation, File Encryption, Certificate Authority, Log generation.(Smitha Sundareswaran *et al*, 2012)

Conclusion

The Data security is very important and expensive in the cloud. We have discussed various cloud data security issues and the various methods to handle that issues. We have also addressed cloud accountability need and studied the methods to achieve cloud accountability. Services in which Data security is more important it is better to use Cloud computing Data Security Model or Cloud Information Accountability Framework. The Services in which Data access information is important it is better to use RSA based storage security system or Cloud Information Accountability Framework. If both the issues are important then it is good to use Cloud Information Accountability Framework.

References

Smitha Sundareswaran, Anna C. Squicciarini (July/August 2012), Ensuring Distributed Accountability for Data Sharing in the Cloud, IEEE transactions on dependable and secure computing, vol. 9, NO. 4.

Rajeev Kanday (2012), A Survey on Cloud Computing Security, 978-0-7695-4817-3/12 IEEE

RAN Shuanglin (2012), Data Security Policy In The Cloud Computing, The 7th International Conference on Computer Science & Education (ICCSE 2012).

Eman M.Mohamed, Hatem S. Abdelkader (2012), Enhanced Data Security Model for Cloud Computing, The 8th International Conference on INFOrmatics and Systems (INFOS2012)

Cong Wang, Qian Wang, and Kui Ren, Wenjing Lou (2009), Ensuring Data Storage Security in Cloud Computing, 978-1-4244-3876-1/09 IEEE

M.Venkatesh, M.R.Sumalatha, Mr.C.SelvaKumar (2012), Improving Public Auditability, Data Possession in Data Storage Security for Cloud Computing, ISBN: 978-1-4673-1601-9/12 IEEE

Zhang Xin, Lai Song-qing, Liu Nai-wen (2012), Research on Cloud Computing Data Security Model Based on Multi-dimension , 978-1-4673-2108-2112 IEEE