Volume 3, Issue 3, March 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Using Third Party Auditor for Cloud Data Security: A Review

Ashish Bhagat
Department Of Computer Science & Engineering
Lovely Professional University, India

Ravi Kant Sahu
School of Computer Engineering,
Lovely Professional University, India

Abstract —Cloud data security is a major concern for the client while using the cloud services provided by the service provider. There can be some security issues and conflicts between the client and the service provider. To resolve those issues, a third party can be used as an auditor. In this paper, we have analysed various mechanisms to ensure reliable data storage using cloud services. It mainly focuses on the way of providing computing resources in form of service rather than a product and utilities are provided to users over internet. The cloud is a platform where data owner remotely store their data in cloud. The main goal of cloud computing concept is to secure and protect the data which come under the property of users. The security of cloud computing environment is exclusive research area which requires further development from both academic and research communities. In the corporate world there are a huge number of clients which is accessing the data and modifying the data. In the cloud, application and services move to centralized huge data center and services and management of this data may not be trustworthy, into cloud environment the computing resources are under control of service provider and the third-party-auditor ensures the data integrity over out sourced data. Third-party-auditor not only read but also may be change the data. Therefore a mechanism should be provided to solve the problem. We examine the problem contradiction between client and CSP, new potential security scheme used to solve problem. The purpose of this paper is to bring greater clarity landscape about cloud data security and their solution at user level using encryption algorithms which ensure the data owner and client that their data are intact.

Keywords—Cloud Service Provider, Data Integrity, Encryption, Third Party Audit.

Introduction

Cloud computing has become hot issue in since 2007 and many companies used to attempt to use the cloud computing services. Typical cloud computing services are Amazon EC2 and Google's Google app engine, amazons they use the Internet to connect to external users, with the convenience, economy, high scalability and other advantages, Pick up any tech magazine or visit almost any IT website or blog and you'll be sure to see talk about cloud computing. "The computer industry is the only industry that is more fashion-driven than women's fashion," he said to a group of Oracle analysts. So let's talk about what cloud computing is and tighten up our definition and understanding of this implementation.

Cloud computing gets its name as a metaphor for the Internet. Internet is represented in the network diagrams as a cloud, the cloud icon represents "all that other stuff" that is makes the network work. It's kind of like "etc."It also typically means an area of diagram or solution that is someone else's concern, so why diagram it all out? It's probably this notion that is most applicable to the cloud computing concept. Cloud computing promises to cut capital costs and operational more importantly, let IT departments focus on strategic projects instead of keeping centralized the data centre running, as in [1].

It is up to the clients to decide the vendors, depending on how willing they are to implement secure policies and be subject to 3rd party verifications. Sales force, Amazon and Google are currently providing such services, charging clients using an on-demand policy. As in [11] references statistics that suggest one third of breaches due to laptops falling in the wrong hands and about 16% due to stolen items by employees. Storing the data in the cloud can prevent these issues altogether. Moreover, vendors can update application/OS/middleware security patches faster because of higher availability of staff and resources. The Cloud computing change Internet into a new computing platform, is a business model that achieve purchase on-demand and pay-per-use in network, has a broad development expectation. The basic point of view pattern is changing the way it is being focused over cloud. In the view of users i.e. In addition to this advantage it brings forth exclusive and challenging security threats towards user's outsourced data.

The proposed problem is multi write and problem of TPA if Third-party-auditor not only uses data but also modify the data than how data owner or user will know about this problem. Here the user has two types' keys, one of which only the owner knows called private key and another one which is known to anyone called public key. We match both the data it must be same as the sent one on the sender cannot deny that they sent it (non repudiation). The downloading of data for its integrity verification is not feasible task since it's very costly because of the transmission cost across the network.

For well organization it is very essential that cloud that allows investigation from a single party audit the outsource data to ensure data security and save the user's computation and data storage. It is very important to provide public auditing service for cloud data storage, so that the user trusts an independent third party auditor (TPA). TPA checks the integrity of data on cloud on the behalf of users, and it provides the reasonable way for users to check the validity of data in cloud. Public auditing in addition to user provides the external party to verify the correctness of stored data against external attacks it's hard to find. However these schemes, as in [7] don't involve the privacy protection of the data. It is a main disadvantage which affect the security of the protocols in cloud computing. So users who depend on only TPA for their security storage want their data to be protected from external auditors. I.e. Cloud service provider has significant storage space and computation resource to maintain the users' data. It also has expertise in building and managing distributed cloud storage servers and ability to own and operate live cloud computing systems. Users who put their large data files into cloud storage servers can relieve burden of storage and computation. At the same time, it is important for users to ensure that their data are being stored correctly and security check. Users should be equipped with certain security means so that they can make sure their data is safe. Cloud service provider always online & assumed to have abundant storage capacity and computation power. The third party auditor is invariably online, too. It makes every data access be in control.

Cloud Software as a Service (SaaS). The capability provided to consumer is to use provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email). The consumer does not manage or control the underlying cloud infrastructure including network, servers, storage, or even individual application capabilities, with possible exception of limited user-specific application configuration settings. TPA eliminates the involvement of client through auditing of whether his data stored in cloud are indeed intact, which can important in achieving economies of scale for Cloud Computing third party auditor who will audit the data of data owner or client so that it will let off the burden of management of data of data owner. Released audit report would not only help owners to evaluate the risk of their subscribed cloud data services, but also be beneficial for cloud service provider to improve their cloud based service platform, as in [7].This public auditor will help to data owner that his data are safe in cloud with the use of TPA, management of data will be easy and less burdening to data owner but without encryption of data, how data owner will ensure that his data are in a safe hand.

Two or more user is using the data any time than consistency of data is important because any time anyone unwanted person can use data and change or modify the data or delete data. If any user two or more is using a data, user one is reading a data while one is writing a data than it may

Be wrong read by one user. So to resolve the data inconsistency becomes an important task of the data owner.

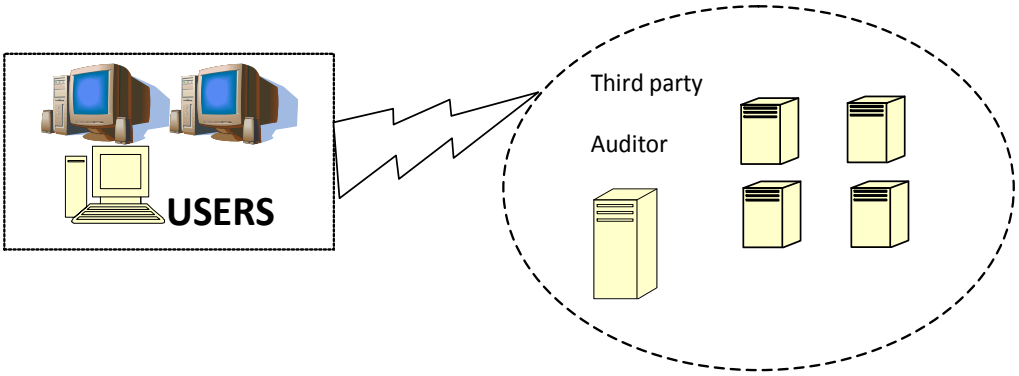

Fig. 1 Cloud Architecture

Review of Literature

As in [6] proposed the issue of cloud computing security in high-speed Railway which provide the security and Issue of cloud computing security such as virtualization security and traffic monitoring between virtual machines. Propose a cloud computing reference framework. By building a Cloud test bed that simulates the information system of China Railway and running Railway applications and data in this test bed. The architecture of Cloud test bed for China Railway as shown in Fig. 1 below. To solve the problem of cloud computing security, create a comprehensive cloud computing security framework is

Proposed their solutions for against cloud security problems there are several traditional solutions to mitigate security problems that exist in Internet environment, as a cloud infrastructure, but nature of cloud causes some security problem that they are especially exist in cloud environment, as in [9]. In the other hand, there is also traditional countermeasure against popular Internet security problems that may be usable in cloud but some of them must be improved or changed to work effectively in it.

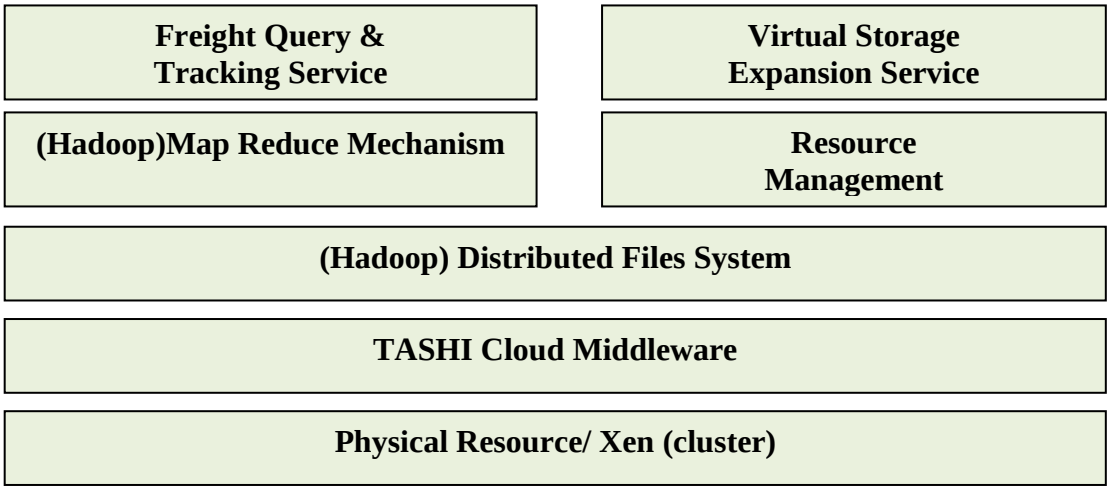

Fig. 2 Cloud Architecture for china railway that test bad

A. Access Control

Access control mechanisms are tools to ensure authorized user can access and to prevent unauthorized access to information systems.

The following are six control statements should be consider ensuring proper access control management as in [2].

1. The Access to information.
2. Manage user access rights.
3. Encourage good access practices.
4. Control access to the operating systems.
5. Control access to network services.
6. Control access to applications and systems.

In [8] in this proposed the problem can be generalized as how can the client find an efficient way to perform periodical integrity verifications without the local copy of data files, as in [2]. If any two users or more users are using a data, one is writing a data while one is reading a data than it may be wrong read by 1 user, so to resolve data inconsistency is become an important task of the data owner and another problem how to trust on TAP is not calculated. If TPA become intruder and pass information of data or deleting a data than how owner know about this problem are not solved. Integrity and consistency.

Proposed scheme in this *vm*, Advanced Encryption Standard (AES) are used where client encrypt and decrypt the file. In this virtual machine, this mechanism solves the problem of unauthorized access of data. In this suggested scheme that can be used for integrity and consistency of data.

In this [9] in this proposed the third party auditor ensures data integrity over out sourced data and proposed digital signature method to protect the privacy and integrity and integrity of outsourced data in cloud environment. TPA check the integrity of data on cloud on the behalf of users, in this solve the previous problem in Enabling public verifiability and data dynamics for storage security in cloud computing and privacy-preserving audit and extraction of digital contents.

They generally cannot help recovery for two reasons as in [4].First, as mismatch between the stored value and computed value of checksums just means that one of them was modified, but it does not provide information about which

of them is legitimate, as in [7]. Stored checksums are also likely to be modified or corrupted. Second, checksums are generally computed using a one-way hash function and data cannot be reconstructed given a checksum value.

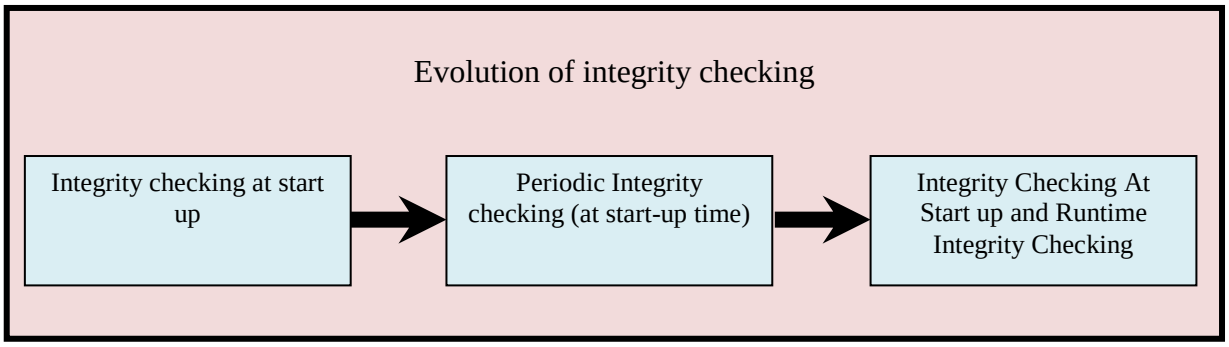

Fig. 3 Evolution of integrity checking

I. Problem Formulation

New data storage paradigm in cloud computing bring about many challenging design issues which has profound influence on the performance and security of overall system.

When two or more users are using data any time then consistency of data is more important because unauthorised person can use data and it can change or modify data or delete the data. If two or more 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, so TPA can be used as an intermediate party between the user and the Cloud Service Provider. An another problem of TPA not only use data but also modify data than how data owner or user will know about this problem and another problem is multi-write problem is important issue.

Machine means of software as a service. In this we use a new algorithm to improve the security check the integrity of data. We find out the problem which is security issues and third party auditor services and to manage this data using TAP that provide the security and also some key security

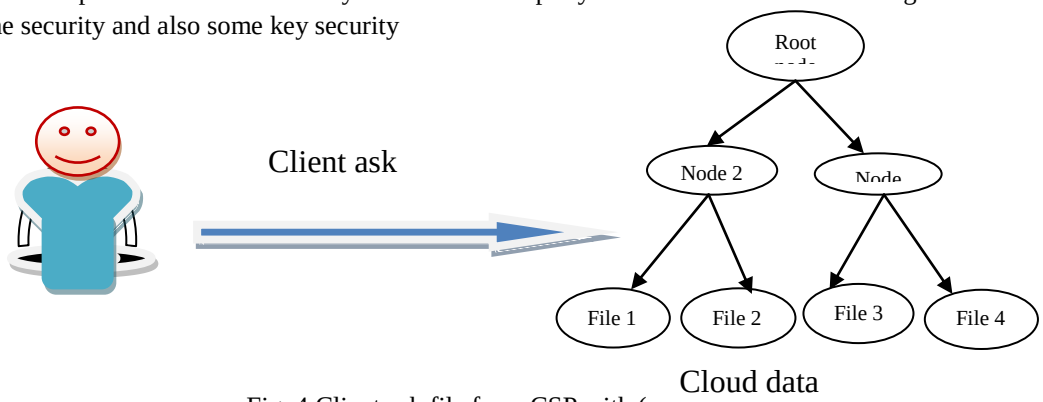

Fig. 4 Client ask file from CSP with (v

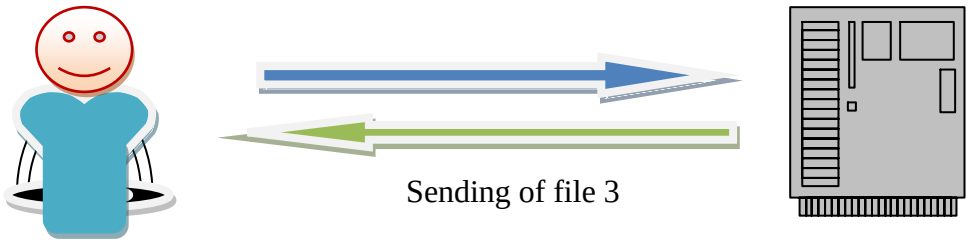

Fig. 5 CSP send file to Client

II. Research Methodology

We use this methodology to getting results and show the work of client, CSP and TPA.

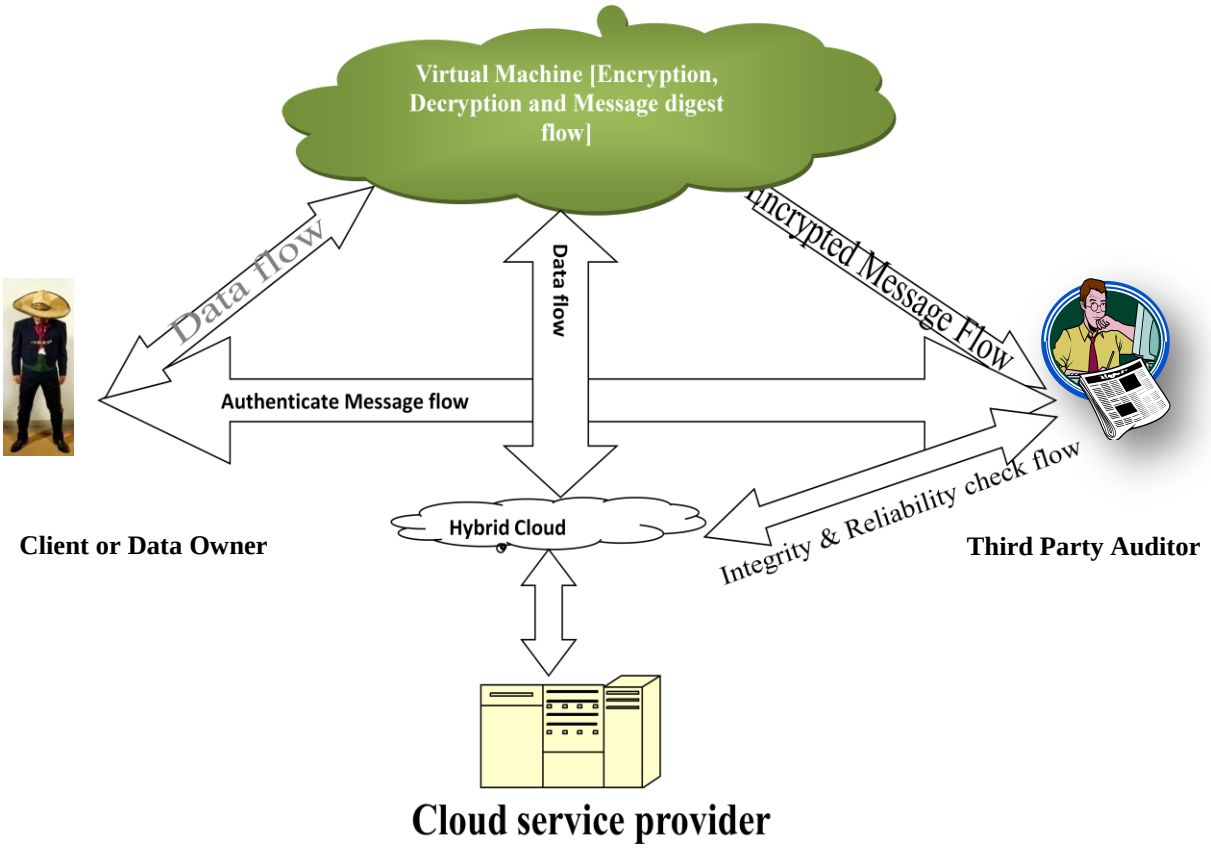

Fig. 6 Architecture for Client TPA and Service provider

TABLE I.
Authors and papers detail description

TITLE	AUTHOR	YEAR	DESCRIPTION
Robust Data Integration while using TPA for Cloud Data Storage Services	Ravi Kant Sahu, Abhishek Mohta and L. K. Awasthi	2012	Third party is used to store the encrypted data using AES encryption algorithm.
Third Party Auditing For Secure Data Storage in Cloud Through Digital Signature Using RSA	Govinda V and Gurunathaprasad H. Sathshkumar	2012	In this Third party is used to store the encrypted data using private and public key in RSA algorithm.
The issue of cloud computing security in high-speed Railway	Xiang Tan Bo Ai.	2011	Developed virtual firewall for the issues of traffic between the VM and monitor the traffic between VM.
The cloud computing security threats and responses	Sabahi Farzad (2011)	2011	Summarize reliability, availability and security issues for cloud computing using access control managements.

In cloud computing, security is most important task. Cloud computing entrusts services with users data, software and computation on a published application programming interface over a network. Cloud provides a platform for many types of services. It has a considerable overlap with software as a service (SaaS), as in [5] End users access cloud based applications through a web browser or a light weight desktop or a mobile app while the business software and data are stored on servers at a remote location. Cloud application providers strive to give same or better service and performance than if the software programs were installed. When we talk about cloud Security, maintaining data integrity is one of the most important and difficult task. When we talk about cloud users, they are using cloud services provided by the cloud provider, as in [5] and again, in the case of maintaining integrity of the data, so we cannot trust the service provider to handle the data, as he himself can modify the original data and the integrity may be lost. If a smart hacker hacks the cloud server and steals the data and modifies it then in some cases this modification is not even identified by the cloud provider. So, in this case, we take the help of a trusted third party auditor to check for the integrity of our data.

This third party auditor takes care of our data and makes sure that data integrity is maintained. We view the procedure of integrity checking as a key's proficiency within software, platform, and infrastructure security focus area of our cloud architecture. Our vision for helping assure ongoing system integrity in a virtualized environment includes an evolution of integrity checking competences, as in [5] Each phase, in this evolution relies on secure start up enabled and provides an increasing level of assurance and. This evolution begins with one-time integrity checks at system or hypervisor start up,

V. Conclusion

Cloud data security is an important aspect for the client while using cloud services. Third Party Auditor can be used to ensure the security and integrity of data. Third party auditor can be a trusted third party to resolve the conflicts between the cloud service provider and the client. Various schemes are proposed by authors over the years to provide a trusted environment for cloud services. Encryption and Decryption algorithms are used to provide the security to user while using third party auditor. This paper provides an abstract view of different schemes proposed in recent past for cloud data security using third party auditor. Most of the authors have proposed schemes which rely on encrypting the data using some encryption algorithm and make third party auditor store a message digest or encrypted copy of the same data that is stored with the service provider. The third party is used to resolve any kind of conflicts between service provider and client.

References

[1] 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. 5.

[3] Cong Wang and Kui Ren and Wenjing Lou and Jin Li,"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.

[6] 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,.

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

[8] 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.

[9]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.

[10] P. Mell and t. Grance "Draft Nist Working Definition of Cloud Computing", 2009.

[11] Elinor Mills, "Cloud Computing Security Forecast: Clear Skies", 2009.

