Third Party Auditing System for Cloud Storage Data

NAGPURE KUNAL A.[1], BARVE MAYURESH M.[2], JADHAV NITIN B.[3]
[1] *Information Technology, S.N.D. COE & RC, Yeola, Nashik (MH), India*

Abstract- In cloud have data owners host their data on public clustered cloud servers and users can access the data from public servers from any place any location with any platform of devices. Due to the outsourcing, this reduces infra structure cost but new paradigm of data hosting service also introduces security challenges and risk of confidentiality, integrity and availability, which requires an auditing service to check the data CIA in the cloud as per the standards and policies defined by company or users requirement. CIA checking methods can only serve for static archive data and thus we cannot fully dependent on the cloud service provider audit be applied to the auditing service or report generation for annual submissions; the data in the cloud can be scalable horizontally updated or vertically updated. An efficient and secure horizontally and vertically auditing protocol is desired to convince data users that the data are correctly stored in cloud with easily available resourses. In this paper, we first design an auditing blueprint for public cloud storage systems and propose a security learning algorithm for efficient and secure auditing protocol with auto top vulnerability detection and applying patch to data security. Then, we are thinking to extend our auditing protocol to support the data scalable operations, which is efficient and secure in the random any models for using this data security auditing system to large scale data applications. Our aim is to include all new technologies in one place for data security and maintain confidentiality, integrity and availability at the public cloud storage servers.

Index Terms- TPA, Cloud Security, Auditing, Analysis, Verification.

I. INTRODUCTION

The cloud Computing is using hardware and software as computing resources to provide service through internet. Cloud computing provides various service models as platform as a service (PaaS), software as a service (SaaS), Infrastructure as a service (Iaas), storage as a service (STaaS), security as a service (SECaaS), Data as a service (DaaS) & many more. Out of this Paas, SaaS and IaaS are the most popular. Cloud computing has four models as Public cloud: though which the service is available to all public use.

Private cloud: Through which service is available to private enterprise or organization. The community Cloud: It allows us to share infrastructure among various organizations through which we can a achieve security, the compliance and jurisdiction. This can manage internally or by a third-party and hosted internally or externally. Hybrid cloud: it is a combination of public and private cloud. The cloud computing has many advantages as: we can easily upload and download the data stored in the cloud without worrying about security. We can access the data from the anywhere, any time on demand. Costs are low or pay the per usage basis. The Hardware and software resources are easily available without location independent. Major disadvantages of the cloud computing is security.

1.1 Related Work

Cloud computing is an internet based computing which enables sharing of services. Cloud computing allows users to use applications without installation any application and access their personal files and application at any computer with internet or intranet access. Many users place their data in the cloud, so correctness of data and security is a prime concern. Cloud Computing is technology for next generation Information and Software enabled work that is capable of changing the software working environment. It is interconnecting the large-scale computing resources to effectively integrate, and to computing resources as a service to users. To ensure the correctness of data, we consider the task of allowing a third party auditor (TPA), on behalf of the cloud client, to verify the integrity of the data stored in the cloud., the auditing process should bring in no new vulnerabilities towards user data privacy, and

introduce no additional online burden to user. In this paper, we propose a secure cloud storage system supporting privacy-preserving public auditing. We further extend our result to enable the TPA to perform audits for multiple users simultaneously and efficiently with RC5 Encryption Algorithm. This shows the proposed scheme is highly efficient and data modification attack, and even server colluding attacks. Here Work is focuses on RC5 Encryption Algorithm for stored data in cloud. Resulted encrypted method is secure and easy to use.

Cloud computing is a distributive computation task on the resource pool which consists of massive computers. LMS experiences with Cloud and Managed Cloud Service provider are due to numerous factors. Availability means that the services are available even when quite a number of nodes fail. Cloud services are provided by many IT companies like Google, Amazon, Microsoft, and Salesforce.com. An enterprise usually store data in local storage and then tries to protect the information from other external source. They also provide authentication at certain fixed level. To overcome this limitation, we are presenting some approaches that do not require full dependency on the external security provider. Storing the data in encrypted form is a common method of data privacy security. If a cloud system is responsible for both tasks on storage and encryption/decryption of data, the system administrators may simultaneously hold encrypted data and decryption keys. This allows them to access information without authorization and thus poses a threat to information privacy.

Cloud computing is an Internet based development, in concept, it is a paradigm shift whereby details are abstracted from the users who no longer need knowledge of, expertise in, or control over the technology infrastructure that supports them. According to a 2008 IEEE paper, Cloud Computing is a paradigm in which information is permanently stored in servers on the internet and cached temporarily on clients that include desktops, entertainment centers, table computers and notebooks etc.‖ Some examples of emerging Cloud computing infrastructures are Microsoft Azure, Amazon EC2, Google App Engine, and Aneka. Cloud service providers enable users to access and use the necessary resources via the internet. To provide these resources, providers often fall back upon other providers in the cloud, hence this raises security issues in Cloud Environment as Clouds have no borders and the data can be physically located anywhere in the world. So this phenomenon raises serious issues regarding user authentication and data confidentiality. Hence it is proposed to implement a simple Data Protection framework which performs authentication, verification and encrypted data transfer, thus maintaining data confidentiality. Programming is performed using JAVA platform, Cloud environment is created using wired and wireless LAN networks. And Advanced Encryption Standard security algorithm is implemented for ensuring security framework.

In cloud computing, data is moved to a remotely located cloud server. Cloud faithfully stores the data and return back to the owner whenever needed. But there is no guarantee that data stored in the cloud is secured and not altered by the cloud or Third Party Auditor (TPA). In order to overcome the threat of integrity of data, the user must be able to use the assist of a TPA. The TPA has experience in checking integrity of the data, that clouds users does not have, and that is difficult for the owner to check. The data in the cloud should be correct, consistent, accessible and high quality. The aim of this research is twofold 1) ensuring the integrity of the data and provides the proof that data is in secured manner. 2) Providing Cryptographic key to secure the data in the cloud. The proposed approach is been implemented and the test results are promising.

Cloud computing is used to store data from various resources by the user. It is difficult for the user to store entire data within the system; therefore clouds are formed to store the user data. User can store as much large amount of the data as user wants. This data stored in the cloud must be integrated, the integrity of the data is thus has to be checked and maintain with the help of Trusted third party. Only trusted third party has the authority to check and to maintain the integrity f the data. The main approach of this paper is to check the integrity of the data stored and to maintain the security by using cryptography method.

II. EXTING SYSTEM AND COLLECT IDEA

The cloud data storage service contains 3 different entities as cloud user, The Third party auditor & cloud server / cloud provider. The cloud user is a person who stores large amount of data or files on a cloud server. The cloud server is a place where we are storing cloud data and that data will be managed by the cloud service provider. The third party auditors will do the auditing on users request for storage correctness and integrity of data.

The proposed system specifies that user can access the data on a cloud as if the local one without worrying about integrity of the data. TPA is used to check the integrity of the data. It supports the privacy preserving public auditing. It will checks the integrity of the data, The storage correctness. It supports the data dynamics & batch auditing. Major benefits of storing data on a cloud is the relief of burden for storage management, The universal data access with location independent & avoidance of capital expenditure on the hardware, software & personal maintenance.

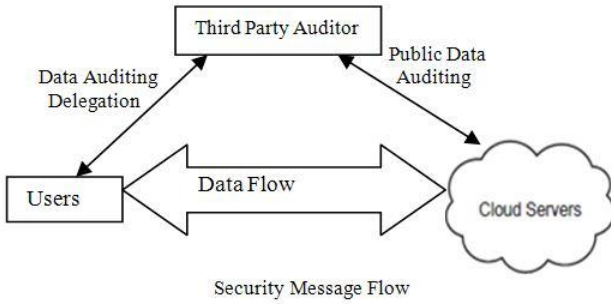

Fig : Architecture of Cloud Data storage service

In cloud, data is stored in a centralized form and managing this data and providing security is a difficult task. The TPA can read contents of data owner hence can modify. Reliability is increased as data is handled by TPA but data integrity is not achieved. It can uses encryption technique to encrypt the contents of the file. The TPA checks the integrity of the data stored on a cloud but if the TPA itself leaks the user's data. Hence the new concept comes as auditing with zero knowledge privacy where TPA will audit the users' data without seeing the contents. It uses the public key based homomorphism linear authentication (HLA) which allows TPA to perform auditing without requesting for user data. It reduces communication & the computation overhead. In this, HLA with the random masking protocol is used which does not allow TPA to learn data content.

A. Goals

[1] It allows the TPA to audit users' data without knowing data content

[2] It supports the batch auditing where multiple user requests for data auditing will be handled simultaneously.

[3] It will provides the security and increases performance through this system.

B. Design Goals

[1] Public audit ability: Allows the third party auditor to check data correctness without accessing local data.

[2] Storage Correctness: Data stored on a cloud is as it. No data modification is done.

[3] Privacy preserving: The TPA can't read the users' data during the auditing phase.

[4] Batch Auditing: The Multiple users auditing request is handled simultaneously.

[5]Light Weight: The Less communication and computation overhead during the auditing phase.

C. Batch Auditing

It also supports batch auditing through which efficiency is the improved. It allows TPA to perform multiple auditing task simultaneously and it reduces communication and computation cost. Through this scheme, we can identify the invalid response. It uses bilinear signature (BLS proposed by Boneh, Lynn and Shacham) to achieve the batch auditing. The System performance will be faster.

D. Data Dynamics

It also supports data dynamics where user can frequently update the data stored on a cloud. It supports block level operation of insertion, deletion and modification. Author of proposed scheme which support simultaneous public Audibility and data dynamics. It uses Merkle Hash Tree (MHT) which works only on encrypted data. It uses MHT for block tag authentication.

III. PROPOSED METHODOLOGY

Those section is presents The public auditing scheme which provides a complete outsourcing solution of data not only the data itself, but also its integrity checking. We start from an overview of our public auditing system and discuss two straightforward schemes and their demerits. We present our main scheme and show how to extent our main scheme to support batch auditing for the TPA upon delegations from multiple users. Then, we discuss how to generalize our privacy-preserving public auditing scheme and its support of data dynamics.

3.1 Definitions and Framework

We are following the similar definition of previously proposed schemes in the context of remote data integrity checking and adapt the framework for our privacy-preserving public auditing system.

A public auditing scheme consists of four algorithms (KeyGen, SigGen, GenProof, Verify Proof). The KeyGen is a key generation algorithm that is run by the user to setup the scheme. The SigGen is used by the user to generate verification metadata, which consist of MAC, signatures, or other related the information that will be used for auditing. The GenProof is run by the cloud server to generate a proof of data storage correctness, while the VerifyProof is run by the TPA to audit the proof from the cloud server.

IEEE Transactions on Knowledge and Data of Engineering, (Volume: 62, Issue: 2) Feb 2013 4 Running a public auditing system consists of the two phases, Setup and Audit:

[1] Setup: User initializes the public and secret parameters of the system by executing KeyGen, and pre-processes the data file F by using SigGen to generate the verification metadata. User then stores the data file F and the verification metadata at the cloud server, and deletes its local copy. As the part of pre-processing, User may alter the data file F by expanding it or including additional metadata to be stored at server.

[2]Audit: The TPA issues an audit message or challenge to the cloud server to make sure that the cloud server has retained the data file F properly at the time of an audit. Cloud server will derive a response message from a function of the stored data file F and its verification metadata by executing the GenProof. TPA then verifies the response via Verify Proof.

IV. CONCLUSIONS

In this paper, we propose a privacy-preserving public auditing system for data storage security in the Cloud Computing. Utilize a homomorphism linear authenticator and random masking to guarantee that the TPA would not learn any knowledge about the data content stored on the cloud server during the efficient auditing process, which not only eliminates a burden of cloud user from the tedious and possibly expensive auditing task, but also the alleviates the users' fear of their outsourced data leakage. We achieved zero knowledge privacy through random masking technique. It supports batch auditing where TPA will handle multiple users request at the same time which reduces communication and computation overhead. It uses bilinear signature to achieve batch auditing. Also supports data dynamics.

V. ACKNOWLEDGEMENT

We would particularly like to thank Prof. B. A. Abhale for stimulating discussion that we had and also we thank for his valuable suggestions.

REFERENCES

[1] C wang, Sherman S. M. Chow, Q. Wang, K Ren and W. Lou, "Privacy-Preserving Public Auditing for Secure Cloud Storage", IEEE Transaction on Computers I, vol. 62, no. 2, pp.362-375 , February 2013.

[2] P. Mell and T. Grance, "Draft NIST working definition of cloud computing," Referenced on June. 3rd, 2009 Online at http://csrc.nist.gov/groups/ SNS/cloud-computing/index.html, 2009.

[3] Tejashree Paigude, Prof. T. A. Chavan "A survey on Privacy Preserving Public Auditing for Data Storage Security" http://www.international journ alssrg. org