JCSE International Journal of Computer Science and Engineering Open Access

Research Paper Volume-2, Issue-3 E-ISSN: 2347-2693

Improving Zero Knowledge in Cloud Storage Auditing System

B.Subasri[1*], P.Vijayalakshmi[2], P.Yurega[3] and E.Revathi[4]

[1,2,3,4] Department of Computer Science and Engineering, Anna University, Chennai- India*

www.ijcseonline.org

Received: 4 March 2014 Revised: 10 March 2014 Accepted: 22 March 2014 Published: 30 March 2014

Abstract—Usage of cloud storage user can store the data tenuously and have the benefit of on demand high quality applications and services from a shared pool of configurable computing resources without the burden of local data storage and maintenance. Utilize the random masking to guarantee that the EA would not learn any knowledge about the data content stored on the cloud server during the efficient auditing process, which not only eliminates the burden of cloud user from the tedious and possibly expensive auditing task, but also alleviates the users' fear of their outsourced data leakage

Index Term—Zero knowledge, Data storage, Public auditing, Cloud computing, Batch auditing

I. INTRODUCTION

In most of the admirable IT field cloud computing is important to developer and users. Cloud computing is most preferable platform for them. Cloud computing is an umbrella term used to refer Internet based development and services. Cloud computing is such type of computing environment where business owners outsource their computing needs including application software services to a Cloud Service Provider(CSP). Cloud storage is a service model in which data is maintained, managed and backed up remotely and made available to users over a network (typically the Internet).

In the cloud environment resources are shared among the entire server, users and individual. As a result file and data stored in the cloud become open to all. Therefore data or files of an individual can be handled by all other users of the cloud. Thus the data or files become vulnerable to attack. Cloud user don't concern about software updates, installation, antivirus and backups. Basically, a cloud storage system can be considered to be a network of distributed data centres which typically uses cloud computing technologies. Here we are considering scenarios where users may have concerns of the integrity and privacy of their data stored in the cloud storage. The potential benefits of such storage services are copy, backup, synchronization of devices and sharing files. Indeed, cloud service provider may potentially reveal users' data to auditors or adversaries during the auditing. From the perspective of protecting data privacy, this severe drawback greatly affects the security of these protocols in Cloud Computing [1]. Thus, it is also necessary to protect the data or files in the midst of unsecured processing. In order to solve this problem we need to apply security in cloud computing platforms. In our proposed security model we have tried to take into account the various security breaches as much as possible [3]

At present in part of cloud computing different security models and algorithms are applied. But, these models have failed to solve all most all the security [6, 7].

In this paper, we have proposed new security architecture for cloud computing platform. In this sculpt high ranked security algorithms are used for giving secured communication process and also Auditing process are done by External Auditor(EA) to make more integrity to data.

II. RELATED WORK

Abhishek Mohta et al [10] describe a data protection from unauthorized access and to ensure that our data are intact we proposed a scheme, which solve the problem of integrity, unauthorized access, privacy and consistency. AshishBhagat et al [11] are first considering toan 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 provide a trusted environment for cloud services.

In N. Sujan Kumar et al[4,],this work, consider the difficulty of securely outsourcing LP computation in cloud computing, and provide such a practical method design which fulfils input/output privacy, cheating flexibility, and efficiency are formalized. By unambiguously decomposing LP computation outsourcing into public LP solvers and private data, our method design is able to explore appropriate security tradeoffs via higher level LP computation than the general circuit illustration[5.6,7]. Cong Wang in this paper, for the first time formalize the problem of securely outsourcing LP computations in cloud computing ,and provide such a practical mechanism design which fulfils input/output privacy, cheating resilience, and efficiency.

III. PROBLEM STATEMENT

Corresponding: B.Subasri

Department of Computer Science and Engineering, Anna University, Chennai- India

The system and threat model:
We consider cloud storage data system involves poles apart three entities, as illustrated in Fig:1, the User U: cloud user has a large amount of data files to store in the cloud. The Cloud Server CS: cloud server which is managed by the CSP and has significant data storage and computing power (CS and CSP are the same in this paper).
The External Auditor EA: external auditor has expertise and capabilities that U and CSP don't have. EA is trusted to assess the CSP's storage security upon request from U. when user put their data on the cloud, they are facing the outsourcing data protection challenges .External auditor should audit data from the cloud, not ask copy of the data file. The user can ask external auditor to check the integrity of outsourced data..The external auditor should not create new vulnerabilities to the users.

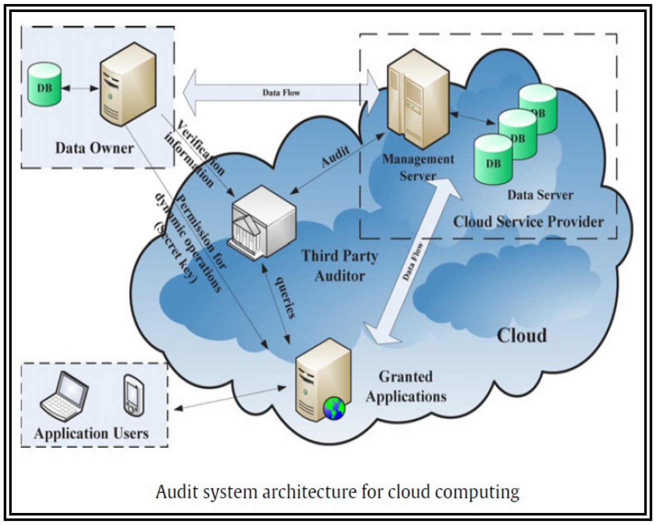

Fig1: Audit system

Architecture
From fig1, we describe audit system architecture. To enable Zero Knowledge auditing for cloud data storage under therefore mentioned model, our protocol design should achieve the following security and performance guarantee:

Public Auditing: to allow EA to verify the precision data which are hoard in the cloud storage system , but without retrieving the copy of entire data.

Batch Auditing: to enable EA secure and efficient manner capability to cope with multiple delegation from possibly different large number of users simultaneously.

Storage correctness: to ensure that there exists nocheating cloud server that can pass the EA's audit without indeed storing users' data intact.

Zero knowledge auditing:
The EA should not reveal any content of data which are placed in cloud storage system. So we improving zero knowledge auditing process

IV. EXISTING SYSTEM AND ITS CHALLENGES

In the Existing method, Linear Programming in cloud computing for practical outsourcing brings new and challenging security threats towards user's outsourced data. This paper used LP computation techniques but data is not encrypted and stored in CSP. So user data are revealed by EA during Auditing process. In Yan Zhu used [8] a quantified new audit approach based on probabilistic queries and periodic verification, as well as an optimization method of parameters of cloud audit services. This approach greatly reduces the workload on the storage Servers, while still achieves the detection of server's misbehavior with a high probability.

By referring different existing system, we have described some suggested requirements for public auditing services and the state of threat that fulfils them. Further challenging issues remain to be supported and resolved.

- What will happen if the data owner and TPA are unreliable? In this case the auditing result should identify the data correctness as well as it should be able to determine which entity is responsible for the problem like owner, TPA or cloud server[12]. So systems accountability should be achieved.
- Performance is another important aspect in cloud computing data storage security and its integrity for any physical system.
- Cloud data storage provides dynamic and scalable storage services. It also allows easy on-demand file sharing on cloud. The challenge in this case is that legacy users, who access data and it can also modify the owner's data in the cloud[13]. So major challenge is dynamics support for public auditing services while maintaining system runtime.
- To securely launch an effective third party auditor (TPA), the following two essential requirements should be met;
- *TPA should be able to efficiently audit the cloud data storage without demanding the local copy of data, and introduce no additional on-line burden to the cloud user.*
- *The third party auditing process should bring in no new vulnerabilities towards user data privacy.*
- Therefore our system protocols provide Confidentiality, Integrity.

V. PROPOSED SYSTEM AND IMPLEMENTATION

In this paper, for improving zero knowledge auditing process , we utilize a cryptographic technique, for verifying the integrity of data without retrieving it at an untrust server; can be used to realize audit services[2]. It with random mask technique to achieve a privacy-preserving public auditing system for cloud data storage security while keeping all above requirements in mind. To support efficient Handling of multiple auditing tasks, we further explore the technique of bilinear aggregate signature to extend our main result into a multi-user setting, where EA can perform multiple auditing tasks simultaneously. Extensive security and performance analysis shows the proposed schemes are provably secure and highly efficient. We also show how to extent our main scheme to support batch auditing for EA upon delegations from multi users. EA should not reveal the content of the data from the users and also does not allow even CSP to view the data. The proposed security model one time random access key has been used for authenticating the user [11]. The key is used to keep the user account secure and secret from the unauthorized user.

But the user defined key can be compromised. To overcome this difficulty one time random access key is used in the proposed security model. Thus whenever a user login in the system, he/she will be provided with a new key for using it in the next login. This is usually provided by the CSP. This key will be generated randomly. Each time a new key is created for a user, the previous key for that user will be expired. New key will be updated for that particular user. A single key will be used for login only once. The password will be sent to the users authorized mail account. Therefore at a same time a check to determine the validity of the user is also performed. As a result only authorized user with a valid mail account will be able to connect to the cloud system. By this system, existence of unauthorized user or a user with an invalid mail account will be pointed out.

In the proposed model AES encryption algorithm is used for making the confident data storage. When a file is uploaded by a user the system server encrypts the file using AES encryption algorithm. In the security model 128 bit key is used for AES encryption. 192 bit or 256 bit can also be used for this purpose. Here the 128 bit key is generated randomly by the system server [9]. A single key is used only once. That particular key is used for encrypting and decrypting a file of a user for that instance. This key is not further used in any instance later. The key is kept in the database table of the system server along with the user account name.

In this model, the encryption key for a particular file of a particular user is only known to the users. The encrypted file is stored in the cloud server. For this, the key as well as the encrypted file is hidden from the unauthorized person. In the cloud storage system, external auditor will audit the encrypted files which are sent from the user. The major advantage is that, auditor should not reveal the content of data due to the encryption process

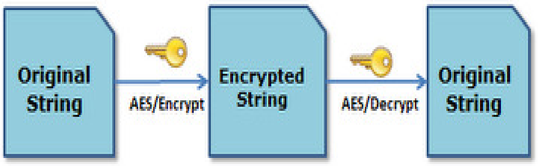

Fig2: AES Encryption/decryption

An algorithm is developed, which is used for inserting the file in the cloud server and in the database table where the encrypted file is kept. In the cloud server, the file is inserted by maintaining the sequence.Therefore, AES remains the preferred encryption standard for governments, banks and high security systems around the world.Symmetric key encryption/decryption uses a secret key during the process[5]. A String encrypted with a secret key cannot be decrypted using another secret key. This is more effective if both the parties keep the key secret.

Modules:
Client

External Auditor

Cloud Service Provider

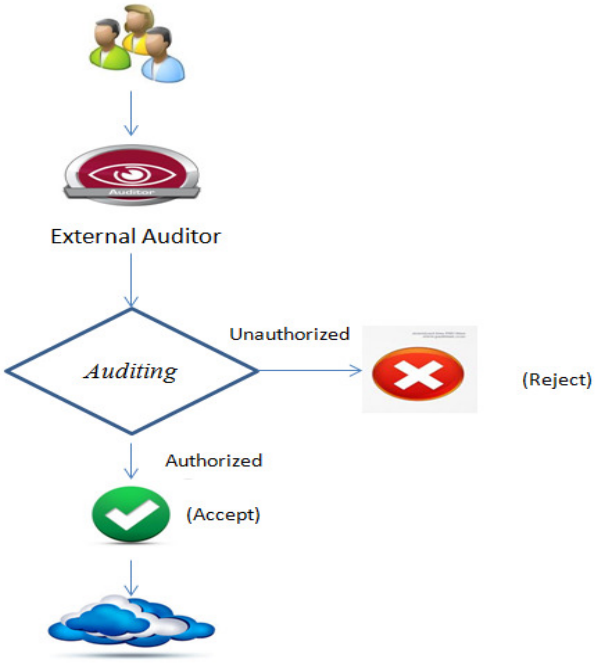

Fig3: Flow diagram for modules

Client: User is a client, in cloud storage system. Cloud storage system has multiple users. So security is not efficient. So we are improving the security in our proposed system. First, Client login the page. After login CSP generates the Temporary Random Access Key to the User. This key sends to the user's appropriate mail-id. Using this access key User can upload or download their appropriate files [14]. User can upload file and send file to cloud storage, then file can be stored in cloud system

External Auditor: External Auditor login the page .CSP provides the Temporary Random Access Key to EA's Mail-Id. Using this access key EA verifies the User's file. During the auditing process EA check whether the user is authorized person or unauthorized person. The user is authorized person means EA allows the particular user for upload/download their file to CSP. Suppose the person is unauthorized person means EA should not allow the particular user.

Cloud Service Provider: CSP manages the significant data storage and also provides lot of cloud services to user. It provides data storage service and has enough storage spaces and computation resources. The user gives their data to CSP. The whole data is controlled by CSP.CSP only allows the verified file [10]. All files are verified by EA. The user uploads or downloads their file from CSP at anywhere, any place and any time. The important advantage of CSP is it takes the automatic periodic backups for user's data. There is no data loss in CSP.

From below table, we know about algorithm for auditing data. Here the process between user of cloud storage and auditor are described. From the auditing process we gain the zero knowledge of auditor. It becomes more security to cloud user for their files.

ALGORITHM FOR AUDITING DATA

TABLE1: ALGORITHM FOR AUDITING

Client Side	EA Auditing
1. Client request to upload/download the file from CSP. 3. Client authenticates EA by his password. 5.Client encrypts/decrypts the file by applying AES algorithm 6. Client upload/download the file to CSP through EA.	2. EA ask client for authentication just like login page. 4. Verify password if correct EA allow the client to upload/download the file from CSP. Else move to step2. 7. EA performs the auditing process for a particular file according to file size, id etc. 8. If file details are correct means they accept the file for upload/download.

VI. CONCLUSION AND FUTURE ENHANCEMENT

In this paper, we propose a zero knowledge auditing in cloud storage which provide integrity protection to customer's essential data. This paper supports file upload/download process effectively and also supports public verifiability. We utilize the cryptographic algorithm(AES) and random access key generator to guarantee that EA would not learn any knowledge about the data content stored on the cloud server during the efficient auditing process. Its also alleviates the users' fear of their outsourced data leakage. In future, we want to work between users and cloud service provider, user to user and also extend the performance of the security communication

REFERENCES

[1]. M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A. Konwinski, G. Lee, D.A. Patterson, A. Rabkin, I. Stoica, and M.Zaharia, "A View of Cloud Computing," Comm. ACM, vol. 53, no. 4,

[2]. YashpalKadam, "Security Issues in Cloud Computing A Transparent View", International Journal of Computer Science Emerging Technology, Vol-2 No 5 October, 2011 , 316-322

[3]. K.S.Suresh M.Tech#1 Prof K.V. Prasad #2Asst. Professor Principal Department of CSE, MLRIT Security Issues and security algorithms in cloud computing

[4]. LIET, Hyderabad, India, Assoc. Professor, LIET, Hyderabad, India Linear programming in cloud computing for Practical outsourcing

[5]. RohitBhadauria, RituparnaChaki, NabenduChaki, SugataSanyal, "A Survey on Security Issues in Cloud Computing", 2011

[6]. Cloud computing: benefits ,risks and recommendation for information security Nelson Gonzalez1*, Charles Miers1,4, Fernando Red´ıgolo1, Marcos Simpl´ıcio1, Tereza Carvalho1, Mats N¨aslund2 and MakanPourzandia

[7]. cloud computing security NGONGANG GUY MOLLET

[8]. YanZhua,b, HongxinHuc, Gail-JoonAhnc, Stephen S. Yauc."Efficient audit service outsourcing for data integrity in clouds".In "The Journal of Systems and Software 85 (2012) 1083– 1095".

[9]. JoanDaemen, Vincent Rijmen, "Announcing the ADVANCED ENCRYPTION STANDARD (AES)", Federal Information Processing Standards Publication 197, November 26, 2001

[10]. AbhishekMohta , Ravi Kant Sahu,Lalit Kumar Awasthi Robust Data Security for Cloud while using Third Party Auditor

[11]. Using Third Party Auditor for Cloud Data Security: A Review .AshishBhagat Ravi Kant Sahu

[12]. A Newer User Authentication, File encryption and Distributed Server Based Cloud Computing security architecture KawserWazed Nafi1,2, TonnyShekha Kar2, SayedAnisul Hoque3, Dr. M. M. A Hashem4

[13]. Mladen A. Vouk, "Cloud Computing – Issues, Research and Implementations", Journal of Computing and Information Technology - CIT 16, 2008, 4, 235–246

[14]. Cloud Security Alliance, "Security guidance for critical areas of focus in cloud computing," 2009, online at http://www.cloudsecurityalliance.org115.G. Ateniese et al., ―Scalable and Efficient Provable Data Possession, Proc. Secure Comm _08, Sept. 2008.