JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

A Secure Data Dynamics and Public Auditing Scheme for Cloud Storage

Mr. M. Satish kumar[1], Ms. Jaya Madhuri[2], Mr. P. Nikhil[3]

Assistant Professor, Department of MCA, Sri Venkateswara College of Engineering and Technology, Chittoor, India[1]

MCA Student, Department of MCA, Sri Venkateswara College of Engineering and Technology, Chittoor, India[2]

MCA Student, Department of MCA, Sri Venkateswara College of Engineering and Technology, Chittoor, India[3]

Abstract: ***Cloud computing is an evolving technology that provides data storage and highly fast computing services at a very low cost. All data stored in the cloud is handled by their cloud service providers or the caretaker of the cloud. The data owner is concerned about the authenticity and reliability of the data stored in the cloud as the data owners. Data can be misappropriated or altered by any unauthorized user or person. This paper desire to suggest a secure public auditing scheme applying third party auditors to authenticate the privacy, reliability, and integrity of data stored in the cloud. This proposed auditing scheme composes the use of the AES-256 algorithm for encryption, SHA-512 for integrity check and RSA-15360 for public key encryption. And perform data dynamics operation which deals with mostly insertion, deletion, and, modification.***

Index Terms – Cloud Computing, Cloud Storage, Data Integrity, Security, Auditing etc.

1. INTRODUCTION

The global cloud computing market is anticipated to rise from $272billion in 2018 to $624billion by 2023 at a compound annual growth rate of 18%, a report from research and markets showed. Cloud computing is an advanced technology every person is used inner or outer in today's world [2]. The advance and rapidly expanding technology of cloud computing are used computation and storage. The very minimum cost is used storage and computation as a service in it. Service model provided three essential services in it: infrastructure as a service (IaaS), platform as a service (PaaS) and software as a service(SaaS)[3]. The NIST definition, "Cloud computing is a model permissive ubiquitous, convenient, on-demand network approach to a shared pool of configurable computing property(e.g. networks, servers, storage, applications, and services) that can be immediately provisioned and released with basic management effort or service provider interaction [4][6].

Cloud storage is a crucial service of cloud computing. They involve data privacy, data protection, data availability, data location, and, secure transmission which is a crucial release in cloud security. The involved in cloud challenge security are threats, data loss, degradation, outside malicious attack and multi-tenancy . The stored information of integrity is conserved for data integrity in the cloud system. The unauthorized users should not be accessed misappropriate or vary of data. Data integrity and reliability of data are faithful to preserve by the cloud computing provider. Data confidentiality is also a crucial way from a user's point of perspective therefore they store their private or confidential data in the cloud. Data confidentiality is taken to assure access control policies and authentication. The faith of cloud computing could be forward by rising cloud authenticate and data confidentiality. So the keep data on the cloud should be security, integrity, privacy, and confidentiality of crucial demands from the user perspective. A secure data storage of cloud computing is presented of a data auditing scheme. Auditing is a refinement of checking the user data which can be done by the data owner or by a TPA. The integrity of stored data on the cloud serves to maintain it. The TPA manage is split into two: one is private audibility, which allows the data owner can analyze the integrity of the data. No one has the authority to inquire about the server considering the data. Though it attains to increases verification overhead of the user. Second is public audibility, the confidentiality of the data can check by only TPA. The behalf of the client can act TPA so TPA is an entity. The verification of integrity has handled to appropriate work that all essential expertise, capabilities, knowledge and professional skill and the position of the client is also reduced by it[8]. It should be crucial that TPA should efficiently.

The cloud computing company is committed to maintaining data integrity and dependability. From a user's standpoint, data confidentiality is also important, therefore they keep their private or confidential data on the cloud. To ensure access control regulations and authentication, data confidentiality is ensured. Cloud computing's confidence might be bolstered by growing cloud authentication and data security. So, from the user's perspective, keeping data on the cloud should be about security, integrity, privacy, and confidentiality. A data auditing method is proposed for safe data storage in cloud computing. Auditing is a refinement of

user data verification that may be performed by the data owner or a TPA. The integrity of cloud-stored data helps to keep it safe. The TPA is divided into two sections: one is private audibility, which allows the data owner to examine the data's integrity. No one has the power to enquire about the server while the data is being processed. It does, however, raise the user's verification overhead. The second is public audibility; only TPA has access to the data's confidentiality. TPA can act on behalf of the customer, therefore TPA is a legal entity. The verification of integrity has been applied to suitable work, which includes all necessary experience, capabilities, knowledge, and professional ability, as well as a reduction in the client's position. It is critical that TPA audits cloud data storage rapidly and regularly without demanding a local copy of the data.

This paper is organized in five sections. After this introduction, in Section II, literature survey discussed of the paper, section III about the System Analysis, Section IV about System Design, as well as the novel feature of the proposed method. Finally, Sections V provide the the conclusion and future scope of the paper.

2. LITARATURE SURVEY

Literature survey is the most important step in software development process. Before developing the tool it is necessary to determine the time factor, economy and company strength. Once these things are satisfied, ten next steps are to determine which operating system and language can be used for developing the tool. Once the programmers start building the tool the programmers need lot of external support. This support can be obtained from senior programmers, from book or from websites. Before building the system the above consideration are taken into account for developing the proposed system.

[1] J Agarkhed, R Ashalatha-"An efficient auditing scheme for data storage security in cloud".2017[ICCPCT].

An on-demand computing in which data is stored in a remote manner and provision of services is from a pool of resources of computing that is shared is known as Cloud computing. The cloud computing fulfills the need of store and oversee show. Though to get to and secure information, numerous exceptional advancements like parallel and guide diminish strategies are accessible. The burden of usage from maintenance and storage of native data is eliminated and the owner additionally benefits from elimination of the responsibility of security and storage .In order to ensure modification of the accuracy of the on-demand data and its due verification on the cloud owners' behalf, a methodology that is innovative is needed. The encryption and file split up is done using a novel secure cryptography hashing algorithm. Once the data is uploaded the user is provided with a private and public key for trustworthy retrieval of the data file. Those keys are generated using a proposed modified RSA cryptosystem algorithm. A multilevel hash tree algorithm is used to efficiently audit the data file occasionally. The implementation and therefore the results show the potency and efficiency of the proposed algorithm compared to the existing algorithm.

[2] B.L Adokshaja, and S.J.Saritha,"Third Party Public Auditing on Cloud Storage using the Cryptographic Algorithm"ICECDS-2017.

Cloud storage is one of the service provided by Cloud computing in which data is maintained, managed, backed up remotely and made available to users over a network (typically the Internet). The user is concerned about the integrity of data stored in the cloud as the user's data can be attacked or modified by outside attacker. Therefore, a new concept called data auditing is introduced which check the integrity of data with the help of an entity called Third Party Auditor (TPA). The purpose of this work is to develop an auditing scheme which is secure, efficient to use and possess the capabilities such as privacy preserving, public auditing, maintaining the data integrity along with confidentiality. Thus the new auditing scheme has been developed by considering all these requirements. It consist of three entities: data owner, TPA and cloud server. The data owner performs various operations such as splitting the file to blocks, encrypting them, generating a hash value for each, concatenating it and generating a signature on it. The TPA performs the main role of data integrity check. It performs activities like generating hash value for encrypted blocks received from cloud server, concatenating them and generates signature on it. It later compares both the signatures to verify whether the data stored on cloud is tampered or not. It verifies the integrity of data on demand of the users. The cloud server is used only to save the encrypted blocks of data. This proposed auditing scheme makes use of AES algorithm for encryption, SHA-2 for integrity check and RSA signature for digital signature calculation.

[3] IK Meenakshi and Sudha George. Cloud Server Storage Security using TPA.International Journal of Advanced Research in Computer Science and Technology (IJARCST) ISSN: 2347-9817, 2014.

In cloud computing, data is moved to a remotely located cloud server. Cloud server faithfully stores the data and return back to the owner whenever needed. Many users place their data in the cloud and so data integrity is very important issue in cloud storage. After moving the data to the cloud, owner hopes that their data and applications are in secured manner. But that hope may fail sometimes that is the owner's data may be altered or deleted. In this scenario, the user must download the data in order to validate it.

[4] Cong Wong, Sherman S M Chow, Qian Wang, KuiRen, and Wen jing Lou. "Privacy Preserving Public Auditing for Secure Cloud Storage". IEEE Transactions on Computers, Volume 62, ISSUE 2, February 2013.

Using cloud storage, users can remotely store their data and enjoy the on-demand high-quality applications and services from a shared pool of configurable computing resources, without the burden of local data storage and maintenance. However, the fact that users no longer have physical possession of the outsourced data makes the data

integrity protection in cloud computing a formidable task, especially for users with constrained computing resources. Moreover, users should be able to just use the cloud storage as if it is local, without worrying about the need to verify its integrity. Thus, enabling public auditability for cloud storage is of critical importance so that users can resort to a third-party auditor (TPA) to check the integrity of outsourced data and be worry free. To securely introduce an effective TPA, the auditing process should bring in no new vulnerabilities toward 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. Extensive security and performance analysis show the proposed schemes are provably secure and highly efficient. Our preliminary experiment conducted on Amazon EC2 instance further demonstrates the fast performance of the design.

[5] KanYang,XiaohuaJia."An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing, IEEE Transaction on (1- 10), 2012.

In cloud computing, data owners host their data on cloud servers and users (data consumers) can access the data from cloud servers. Due to the data outsourcing, however, this new paradigm of data hosting service also introduces new security challenges, which requires an independent auditing service to check the data integrity in the cloud. Some existing remote integrity checking methods can only serve for static archive data and, thus, cannot be applied to the auditing service since the data in the cloud can be dynamically updated. Thus, an efficient and secure dynamic auditing protocol is desired to convince data owners that the data are correctly stored in the cloud. In this paper, we first design an auditing framework for cloud storage systems and propose an efficient and privacy-preserving auditing protocol. Then, we extend our auditing protocol to support the data dynamic operations, which is efficient and provably secure in the random oracle model. We further extend our auditing protocol to support batch auditing for both multiple owners and multiple clouds, without using any trusted organizer. The analysis and simulation results show that our proposed auditing protocols are secure and efficient, especially it reduce the computation cost of the auditor.

3. SYSTEM ANALYSIS

A. Existing System

All data stored in the cloud is handled by their cloud service providers or the caretaker of the cloud. The data owner is concerned about the authenticity and reliability of the data stored in the cloud as the data owners. Data can be misappropriated or altered by any unauthorized user or person.

Dis-advantages

- Data Privacy problem
- Low efficiency
- Providing low security
- Performance is low

B. Proposed System

This proposed auditing scheme composes the use of the AES-256 algorithm for encryption, SHA-512 for integrity check and RSA-15360 for publickey encryption. And perform data dynamics operation which deals with mostly insertion, deletion, and, modification.

It is necessary to develop a reliable auditing technique and perform data dynamics operations. There is no information regarding the auditing process sent on to a third-party auditor. It operates on the basis of a communication model. It employs the algorithms AES256, RSA15360, and SHA512. AES256 is a widely used and well accepted encryption and decryption method. It operates with a 128-bit input block size and a 256-bit key size[16]. As a result, it has a total of 2256 potential key combinations, which is a 78-digit number. It generates the number of astronomically in the observable universe in an exponential manner. It is regarded as one of the most powerful algorithms available.

Advantages

- Improving Data Privacy
- Providing more Security to the Data
- High efficiency
- Confidentiality and privacy

4. SYSTEM DESIGN

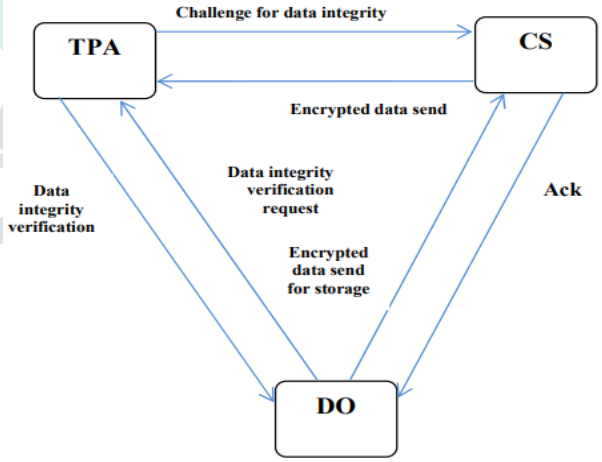

Figure 1: Communication Model

Our protocol design should fulfil the following security and performance requirements to allow privacy-preserving public auditing for cloud data storage under the aforementioned scenario.

- **Public auditability:** to allow TPA to check the integrity of cloud data on demand without having to download a copy of the entire data or putting additional strain on cloud users' internet connections.

- **Storage integrity:** to ensure that no cheating cloud server may pass the TPA's audit without actually storing users' data intact.
- **Privacy-preserving:** the TPA must not be able to deduce the content of users' data from the information gathered during the auditing process.
- **Batch auditing:** to enable TPA to handle numerous auditing delegations from a potentially large number of different users at the same time in a secure and efficient manner.
- **Lightweight:** to allow TPA to conduct audits with the least amount of transmission and processing.

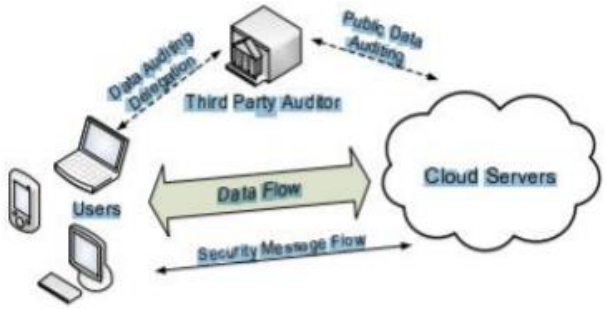

Fig.2: Architecture Diagram

We propose combining the homomorphic linear authenticator with the random masking approach to provide privacy-preserving public auditing. The linear combination of sampled blocks in the server's response is disguised by randomness generated by the server in our protocol. With random masking, the TPA no longer has all of the required information to construct a proper group of linear equations and, as a result, it is unable to deduce the user's data content, regardless of how many linear combinations of the same set of file blocks are gathered. However, even in the presence of randomness, the correctness validation of the block authenticator pairs may be done in a novel method that will be demonstrated shortly. To provide public auditability to the auditing protocol, we employ a public keybased HLA in our architecture. We utilise the HLA suggested in, which is based on the Boneh, Lynn, and Shacham short signature method (hence referred to as BLS signature).

5. CONCLUSION

A secure auditing method is to store the data on the cloud in a secure manner. The prospective take the AES-256 algorithm, RSA-15360, and SHA-512 algorithm to assure that TPA cannot knowledge about data toward the robustness auditing scheme. We propose a data dynamics operation with mostly deal insertion, deletion and, modification.

Future Scope

In the future, we would like to perform a batch auditing method of data.

REFERENCES

[1] The global cloud computing market report 2019.
[2] J Agarkhed, R Ashalatha-"An efficient auditing scheme for data storage security in cloud".2017[ICCPCT].
[3]. SK Saroj, G Noida,SKChauhan, AK Sharma "Threshold cryptography based data security in cloud computing".S Vats-2015.
[4] Mell, Peter, and Tim Grance.The NIST definition of cloud computing(2011).
[5]]P.Mell and T.Grance,"The NIST definition of cloud computing",National Institute of Standards and Technology,Tech. Rep.,2009.
[6].SwapnaliMorea, SangitaChaudhari,"Third Party Public Auditing Scheme for Cloud Storage ",International Journal of Prpcedia Computer Science ,Volume 79,pp.69-76,2016.
[7] Zissis, Dimitrios, and DimitriosLekkas. Addressing cloud computing security issues. Future Generation computer systems 28.3(2012):583-592.
[8] B.L Adokshaja, and S.J.Saritha,"Third Party Public Auditing on Cloud Storage using the Cryptographic Algorithm"ICECDS-2017.
[9]Cong Wang, Sherman SM Chow, Qian Wang, KuiRen, and WenjingLou."Privacy Preserving Public Auditing for Secure Cloud Storage.http://eprint.iacr.org/2009/579.pdf.
[10] Cong Wong, Sherman S M Chow, Qian Wang, KuiRen, and Wen jing Lou."Privacy Preserving Public Auditing for Secure Cloud Storage". IEEE Transactions on Computers, Volume 62, ISSUE 2, February 2013.
[11]AbhishekMohta, Ravi Kant Sahu, Lalit Kumar. "Robust Data Security for Cloud while using Third Party Auditor". International journal of advanced research in CSE (IJARCSE), Volume 2, Issue 2, February 2012.
[12]IK Meenakshi and Sudha George.Cloud Server Storage Security using TPA.International Journal of Advanced Research in Computer Science and Technology (IJARCST) ISSN: 2347-9817, 2014.
[13] Qian Wang, Cong Wang, KuiRen, and Wenjing Lou, and Jin Li. Enabling Public Auditability and Data Dynamics for Security in Cloud Computing. Parallel and Distributed Systems,IEEE Transactions on,22(5):847-859,2011.
[14] KanYang,XiaohuaJia."An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing, IEEE Transaction on (1- 10), 2012.
[15] W.Stalling,"Cryptography and network security,"LPE Sixth Edition,ISBN-978-013-335-4690. [16] Kerry Maletsky,"RSA vs ECC comparison for embedded system"Atmel8951.
[17] MeilianaSumagita,ImamRiadi,"Analysis of secure hash algorithm(SHA) 512 for encryption process on web based application"IJCSDF-7(4):373- 381.