Implementation of Cloud data Integrity, Batch Auditing Verification for Cloud data Security using Algebraic Signature

Mr.D.Jayaprakash B.E., M.E., Associate Professor, Mrs.S.M.C.Subashini B.Tech., ME., Assistant Professor,
Mr.M.Prakash Kumar B.E., M.E, Assistant Professor, Ms.S.Uma B.E., PG Scholar
Department of Computer Science and Engineering, Narasu's Sarathy Instirute of Technology, Salem,Tamilnadu,India

Abstract— The Rabid development of cloud services, the cloud server processes the huge group of data with specialized connections to distribute data processing among the various servers. Client stores data on cloud server to maintain their data privacy without any security and data lose. The existing security method is called cryptography which taking more time and space to authenticate data auditing processes. The proposed method is called as Algebraic Signature to used low computation performance time and large data space for large data set. It is based on data integrity and auditing method for batch auditing method. This proposed system is used to shows that our scheme can achieve the data confidentiality and data security properties. The result of this process is supporting for data security as well as providing data dynamic operations to the user.

Keywords: Cloud Service Provider, Algebraic Signature, TPA and Batch Auditing

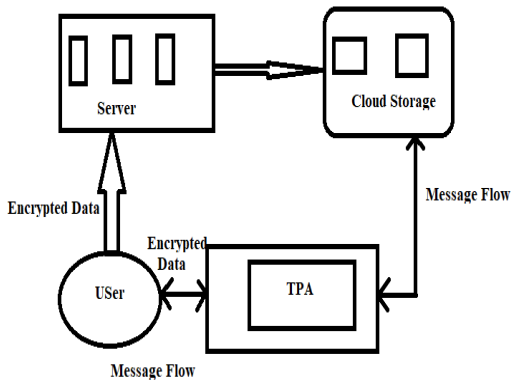
INTRODUCTION

Cloud computing uses the Novel method for a large set of distributed computing processes. Cloud computing is to make use of millions of data and its users into a single platform. The CSP is a large service provider where the data is stored. It allows operating more effectively and improving their productivity to organizations. These are the tools and applications that are integrated into the cloud server that can be accessed from anywhere by the user. To improve the data security and auditing the system use some other auditing scheme to store data by the user in CSP. Data auditing is widely used in cloud computing to deal with secured data storage with large data sets. The data batch auditing is the better process of user's data verification which can be carried out either by the user. It reduces the overhead of the client and also the client no longer needs to do the job of verification on its own.

Cloud computing is used as a huge group of servers with a large set of connections to distribute the data processing among the many servers. Nowadays in many fields people handle digital marketing for availability of resources for the clients all the time even in pandemic periods. Normally the user's data should be secure and non-leakages on the cloud computing. Data integrity batch auditing is introduced in cloud computing to deal with the securable data storage and data integrity. Data batch auditing is one of the big processes of verification of user's data which can be carried out by a Third Party Auditing. It is the protocol to make the data integrity for user's data and TPA provides to audit the user's data for both user and CSP.

Cloud computing has three entities: Data owners, CSP and TPA. Clients store data on cloud servers to maintain their data without any data loss. CSP is the largest data operations of service providers where data is stored and provides applications to the organizations. TPA is used for auditing the stored data by the user in CSP and cloud with encrypted data. A data proprietor should show this way to empower data integrity evaluating components. The data proprietor, who utilizes the TPA to check the integrity of their data, is eased from the weight of costly reviewing tasks. Although the data proprietor believes in the TPA's data checking, they can additionally be a danger to the data proprietor. Perhaps the main issue in the data review process is subsequently forestalling data spillage and protecting the security of data. An arbiter deals with the deduplication cycle inside the server, so there is no security issue. A likely strategy for tackling this issue is to scramble the entire common document prior to sending it to the cloud.

Diagram for Data Integrity Checking



SECURITY ANALYSIS

In this Security Analysis part, the security intensity and robustness is the approach by us.

Data Confidentiality

In this technique, Data Owner encodes the data and stores it in a cloud server. Despite the fact that data is encoded simply by the symmetric key, the data owner can just see the data. Cloud servers cannot provide information about data. TPA demands for scrambled information to cloud servers to actually take a look at respectability. This cloud server sends scrambled information to TPA for a data auditing check. To shielded data from an outside assailant then the cloud server has again scrambled the encoded information to the public key. Since the key size is extremely expanded then not influencing the outside assault. In this planned technique, No information about the entire key. Similar values with regards to what theyare looking for in. Henceforth, the impact assault of CS and DO's is unimaginable.

Algebraic Signature

The Algebraic Signature is the short signature which is a type of hash function with algebraic properties. The main property of this method is the sum of the data blocks produces the same results as the signature of the sum of the corresponding blocks.The algebraic signature is that the file with the blocks f[1],f[2],f[3]……f[N] is calculated as $\mathbf{s(f)=\sum_{i=1}^{n} f.r^{i-1.}}$

Algebraic signature data blocks calculated as following way: User data file (F) will be segmented as data blocks (f_n).The user generates the secret key (K),Then the user create algebraic signature S_n of each block using Secret Key(K).The output of the data to the user like Data File Blocks(f_n) and algebraic signature(S_n).Then the converted data will be uploaded to the cloud storage and these data blocks and Signature blocks stored in the cloud storage database on the cloud server. Inside the server the linked lists are created in the database and store the logical index of datablocks and dynamic version number.This number is reference to the user data on cloud storage databases. After completing all this algebraic signature calculation the file uploaded successfully on cloud server and the notification will be sent to the user. The Algebraic Signature can be computed as Bit Strings denoted as B_1,B_2,B_3….Bn denoted as data blocks and passed as signature parameters.

$Sig_a(B_1, B_2, B_3.....Bn) = \sum_{i=1}^{n} \mathbf{B_i.a^i}$

In this equation the algebraic signature compresses the large file into a smaller string. If the user wants to change the original value of the file, the algebraic signature also will be changed. The main purpose of algebraic Signature is checking whether the remote data is stored completely on a cloud server.

The algebraic signature can be observed as the following equation: two large data files as A and B consist of n sub block which is denoted as A1, A2, A3…… An and B1, B2, B3….. Bn.

$Sig_a(A) + Sig_a(B)$

$= Sig_a(A_1, A_2, A_3..... A_n) + Sig_a(B_1, B_2, B_3.....B_n)$

$= \sum_{i=1}^{n} \mathbf{A_i.a^i} + \sum_{i=1}^{n} \mathbf{B_i.a^i}$

$= \sum_{i=1}^{n} \mathbf{(A_i+B_i).a^i}$

$= Siga(A+B)$

3. LITERATURE SURVEY:

Secure Keyword Search and Data Sharing Mechanism for Cloud Computing

The main purpose of this paper is to ensure security and the user's data is usually encrypted before it's outsourced to the cloud to avoid data losing. It is a critical task for the CSP as the users expect the cloud to conduct a quick search and return the result without lose data. To overcome these problems, here proposes a ciphertext-policy attribute-based mechanism with keyword search and data sharing for encrypted cloud data.

Provable Data Possession Scheme Based On Algebraic Signature and Linked List for Outsourced Dynamic Data on Cloud Storage

Cloud computing is apopular technology in the world of computing ,which is emerging with broad ranging effects across

IT,business,health care ,software engineering and data storage remotely. The CSP is used for storing data, sharing data and application services. The production of data is increasingly rapidly and it has the property of being updated dynamically. The dynamic data operation is used to store on cloud storage provided by Third Party Service Providers. It is used to calculate the signature for data blocks which have the computational complexity of O (N) using Algebraic Signature.

Data Security and Privacy Production for Cloud Storage: A Survey

The new development trends called Internet of Things, digital Smart city, enterprises business digital transformation and world's digital economy are at the top of the tide. The fast growth of data storage pressure drives the rapid development of the entire data storage market on account of massive data generated. By providing data storage and Management, cloud storage system becomes an indispensable part of the new area. Currently the government, enterprise and individual users are actively migrating their data to the cloud. The good performance of cloud in the digital economy, enterprise digital transformation, Internet of Things and other fields, we confirm that cloud computing and cloud storage will be the mainstream.

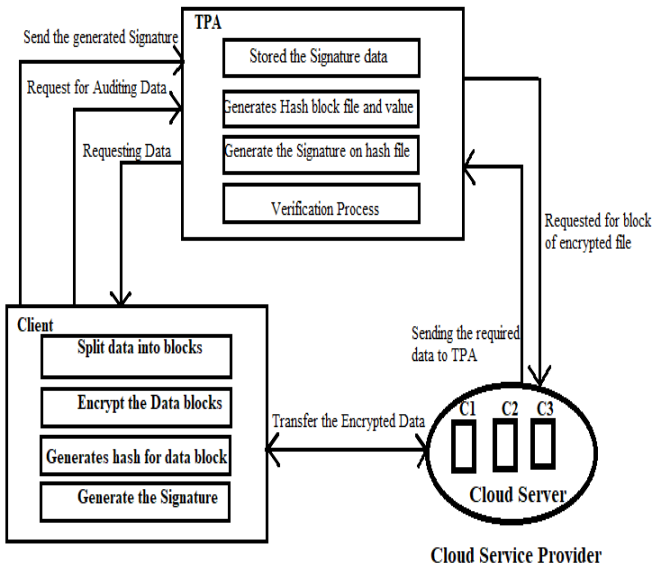
A Verifiable Semantic Searching Scheme by Optimal Matching over Encrypted Data in Public Cloud

Semantic Searching over the encrypted data is a very crucial task. So to provide retrieval service to client data and search results and be flexible. This paper provides a secure verifiable semantic searching scheme. For semantic optimal matching on ciphertext, we formulate word transportation problems to calculate the minimum word transportation cost as the similarity between queries and documents and propose a secure transformation to transform word Transportation problems into Random Linear Programming problems to obtain the encrypted Minimum Word Transportation Cost. For verifiability the duality theorem of Linear Programming to design a verification mechanism using the intermediate data produced in the matching process to verify the correctness of search results.

TPA Auditing scheme for Cloud Storage

Cloud Computing is the service provider by Cloud Servers in which data is maintained,managed,backed up remotely and available to users data over a large network. The user is concerned about the security of data stored in the cloud as the user's data can be attacked or modified or leaked by outside attackers. Therefore the concept called data auditing is introduced which checks the integrity of user's data with the help of an entity called TPA. The main purpose of this concept is to develop an integrity auditing scheme which is secure, efficient to use and possesses the capabilities such as privacy preserving, public auditing and maintaining the user's data integrity along with confidentiality. Thus the TPA auditing scheme has been developed by considering all these requirements. It consists of three entities which are Data Owner, TPA and Cloud Server. The auditing scheme makes use of AES algorithm for encryption, SHA-2 for Integrity check and RSA signature for digital signature calculation.

4. SYSTEM ARCHITECTURE:



4. EXISTING SYSTEM:

The current framework utilizes the irregular example method and homomorphic direct authenticators to plan a PDP conspiracy, which permits the data evaluator to confirm the integrity of cloud data without downloading the entire data from the cloud server. In the proposed conspiracy, the blunder adjusting codes and the spot-checking method are used to guarantee the irretrievability and the integrity of the data put away in the cloud. The current framework executes private unquestionable status and public evidence by utilizing pseudorandom capacity and BLS signature. To help client associations, including data change, inclusion and erasure, built a unique data integrity inspecting plan by taking advantage of the file hash tables. In open data integrity evaluating, The TPA may determine the substance of client's data by testing similar data blocks rehashed times. To ensure the data protection took advantage of the irregular veiling procedure to develop the principal public data integrity examining plan supporting security saving. To mitigate the client's calculation weight of authenticator age, a data integrity evaluating plan utilizes in notice ability obscurity strategy, which diminishes the overhead for creating data authenticators.

5. PROPOSED METHODOLOGY

This proposed system is an algebraic signature based Novel technology with data integrity and auditing scheme that ensures the cloud server data integrity and data confidentiality with batch auditing. The main advantage of this scheme is that it can also support data dynamics by using many cloud servers. It proposes the monitoring of data access patterns by profiling user's data behaviour to determine the defect when a malicious occurs insider illegitimately accesses someone's documents in cloud servers. Decoy documents stored in the cloud alongside the user's real unauthorized data access or exposures are verified with data integrity challenge questions for instance. The malicious that is third party attacker is unknown with unrelated information in order to collapse the user's real data from the cloud storage server. Such preventive attacks that rely on disinformation technology could provide unprecedented levels of security in the cloud along with social networks. The results of the experiments suggest that user profiles are accurate enough to detect unauthorized cloud access on the cloud server. When such unauthorized access is deleted from the cloud one can respond by presenting the user with a challenge questions to validate whether the access was indeed authorized similar to how we used decoy in a local data file setting with multimedia data to validate the alerts issued by the user file search and access data behaviour by the TPA. Some researchers have proposed PDP for checking whether a remote cloud server stores data files correctly.PDP allows a user to check a part of their data and it is unnecessary to retrieve all the data to the user's side. The cloud server will help to compute a storage proof for users to avoid data collision. In further studies on data integrity checking, POR has been proposed by various researchers to check whether the remote servers possess a user's data. To improve the quality of the data checking to avoid servers from obtaining sensitive information during the integrity checking process, the researchers have resorted to TPA to realize the data integrity checking, which is defined as cloud data auditing. We call page P a String of l symbols pi and l=0, 2 ...l-1.In our Scheme, the symbols are elements of a Galois Field, GF (2^f) for us; f=8, f=16 basically. We assume that l<2^f-1. Let $\alpha=\alpha_1.....\alpha_n$ be a vector data of different zero and non zero elements of the Galois Field(GF). We call α n-symbol signature base or simply the base. The n-symbol P signature or N signature or simply based on α is vector.

$$\mathbf{Sig_\alpha\ (P) =(sig_{\alpha 1}\ (P),\ sig_{\alpha 2}\ (P) \ldots sig_{\alpha n}\ (P)\ )}$$

Here, for each α,

Sig_α (P) denotes = $\mathbf{Sig\alpha(P) = \sum_{i=0}^{l-1} Pi\ \alpha\hat{}i}$

The generalization of **$Sig_{\alpha,n}$** scheme to a base process using a non primitive data that is α does not seem of practical interest. We now prove our intuitive claim with respect to the collision probability of **$Sig_{\alpha,n}$** and naturally **of $Sig\alpha^2_{,n}$ with n<=2.**

COCLUSION AND FUTURE ENHANCEMENT

The proposed data dynamics can provide data, deletion, insertion and update on cloud servers. From fast forward to today, storage remains a main service that cloud servers provide to users. Because of the special nature of cloud computing, traditional security solutions cannot be directly applied to it. The cloud may conceal the risks to the users and reserve computing resources as much as possible. To ensure the security of the data, a common method is to encrypt the data and outsource the encrypted data to the cloud. Generally the cloud is a public cloud, which means that there are no limitations on access by users and devices can access the cloud therefore the cloud application system should include an access control mechanism. Certain schemes focus on attribute-based cryptography in the design of cloud access control protocols which effectively ensures that the user can satisfy the attribute data security wise. Inspired by and the algebraic signature is introduced in designing the auditing scheme for cloud computing to reduce the overhead of the computation. The algebraic signature is more efficient in remote data integrity checking without losing data. Because we use both cloud computing with big data technologies. Therefore massive amounts of data transactions are happening on the cloud computing for organizations for remote data transactions in a secured manner.

REFERENCE:

1.C. Ge, W. Susilo, Z. Liu, J. Xia, P. Szalachowski and L. Fang, "Secure Keyword Search and Data Sharing Mechanism for Cloud Computing," in *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 6, pp. 2787-2800, 1 Nov.-Dec. 2021, doi: 10.1109/TDSC.2020.2963978.

2. P. Yang, N. Xiong and J. Ren, "Data Security and Privacy Protection for Cloud Storage: A Survey," in IEEE Access, vol. 8, pp. 131723-131740, 2020, doi: 10.1109/ACCESS.2020.3009876.

3. W. Yang and Y. Zhu, "A Verifiable Semantic Searching Scheme by Optimal Matching Over Encrypted Data in Public Cloud," in *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 100-115, 2021, doi: 10.1109/TIFS.2020.3001728.

4. SmitaChaudhari and Gandharba Swain, "Efficient and Secure Group based Collusion Resistant Public Auditing Scheme for Cloud Storage" International Journal of Advanced Computer Science and Applications(IJACSA), 12(3), 2021. http://dx.doi.org/10.14569/IJACSA.2021.0120356

5.SEzhilArasu, B Gowri, and S Ananthi. Privacy-Preserving Public Auditing in cloud using HMAC Algorithm. *International Journal of Recent Technology and Engineering (IJRTE)* ISSN: 2277, 3878, 2013.

6. Abbdal, Salah H., Hai Jin, DeqingZou and Ali A. Yassen. "Secure Third Party Auditor for Ensuring Data Integrity in Cloud Storage." *2014 IEEE*

11th Intl Conf on Ubiquitous Intelligence and Computing and 2014 IEEE 11th Intl Conf on Autonomic and Trusted Computing and 2014 IEEE 14th Intl Conf on Scalable Computing and Communications and Its Associated Workshops (2014): 510-517.

7. Li, Ling et al. “Study on the third-party audit in cloud storage service.” *2011 International Conference on Cloud and Service Computing* (2011): 220-227.

8. W. Li, X. Li, J. Gao and H. Wang, "Design of Secure Authenticated Key Management Protocol for Cloud Computing Environments" in IEEE Transactions on Dependable and Secure Computing, vol. 18, no. 03, pp. 1276-1290, 2021.

doi: 10.1109/TDSC.2019.2909890

9. A. d. Santos, T. I. Syed, M. C. Naldi, R. J. G. B. Campello and J. Sander, "Hierarchical Density-Based Clustering Using MapReduce," in *IEEE Transactions on Big Data*, vol. 7, no. 1, pp. 102-114, 1 March 2021, doi: 10.1109/TBDATA.2019.2907624.

10. K. Gai, M. Qiu and H. Zhao, "Privacy-Preserving Data Encryption Strategy for Big Data in Mobile Cloud Computing," in *IEEE Transactions on Big Data*, vol. 7, no. 4, pp. 678-688, 1 Oct. 2021, doi: 1109/TBDATA.2017.2705807.