PROFICIENT PUBLIC VERIFICATION OF DATA RELIABILITY FOR CLOUD STORAGE WITH TWO-TIRE PROTECTION

Abstract

The cloud security is one of the important roles in cloud, here we can preserve our data into cloud storage. More and more clients would like to store their data to PCS (public cloud servers) along with the rapid development of cloud computing. Cloud storage services allow users to outsource their data to cloud servers to save local data storage costs.Multiple verification tasks from different users can be performed efficiently by the auditor and the cloud-stored data can be updated dynamically.It makes the clients check whether their outsourced data is kept intact without downloading the whole data.In our system we are using the own auditing based on the token generation. Using this key generation technique compare the key values from original keys we can find out the changes about the file. A novel public verification scheme for cloud storage using in distinguishability obfuscation, which requires a lightweight computation on the auditor and delegate most computation to the cloud.Not only stored also the content will be encrypted in the cloud server. If anyone try to hack at the cloud end is not possible to break the two different blocks. The security of our scheme under the strongest security model.They need first decrypt the files and also combine the splitted files from three different locations. This is not

possible by anyone. Anyone can download the files from the server with file owner permission. At the time of download key generated (code based key generation) and it will send to the file owner. We can download the file need to use the key for verification and some other users want to download file owner permission is necessary.

INTRODUCTION

Distributed computing has been imagined as the following creation data innovation (IT) design for undertakings, because of its extensive rundown of unparalleled preferences in the IT history: on-request self-benefit, omnipresent system get to, area self-deciding asset pooling, fast asset versatility, utilization based estimating and transference of hazard.

As a disturbing innovation with significant ramifications, distributed computing is changing the very way of how organizations utilize data innovation. One essential part of this outlook changing is that information are being brought together or outsourced to the cloud. From clients' view, including together people and IT endeavors, putting away information remotely to the cloud in an adaptable on-request technique bring appealing advantages: arrival of the weight for storage room administration, boundless information access with place autonomy, and evasion of assets expenses on equipment, programming, and staff systems of support, and so on

While distributed computing make these remuneration more engaging than any other time in recent memory, it additionally conveys new and testing security dangers to clients' outsourced information. As cloud administration suppliers (CSP) are part regulatory elements, information outsourcing is really surrendering client's last control more than the destiny of their information. As a matter of first importance, despite the fact that the frameworks beneath the

cloud are significantly more effective and dependable than individual registering gadgets, they are still before the extensive variety of both inside and outside dangers for information respectability.

1.1 .Scope of the project

As high-speed networks and ubiquitous Internet access become available in recent years, many services are provided on the Internet such that users can use them from anywhere at any time. Data robustness is a major requirement for storage systems. There have been many proposals of storing data over.

1.2 .Need for the project

As a disruptive technology with profound implications, cloud computing is transforming the very nature of how businesses use information technology. One fundamental aspect of this paradigm shifting is that data Are being centralized or outsourced to the cloud. From users' perspective, including both individuals and IT enterprises, storing data remotely to the cloud in a flexible on-demand manner brings appealing benefits: relief of the burden for storage management, universal data access with location independence, and avoidance of capital expenditure on hardware, software, and personnel maintenances, etc.

1.3 . Objective of the project

Cloud service providers (CSP) are separate administrative entities, data outsourcing is actually relinquishing user's ultimate control over the fate of their data. As a result, the correctness of the data in the cloud is being put at risk due to the following reasons. First of all, although the infrastructures under the cloud are much more powerful and reliable than personal computing devices, they are still facing the broad range of both internal and external threats for data integrity.

LITERATURE SURVEY

TITLE 1:QUICK SYNC: IMPROVING SYNCHRONIZATION EFFICIENCY FOR MOBILE CLOUD STORAGE SERVICES

AUTHOR:Y. Cui, Z. Lai, X. Wang, N. Dai, and C. Miao

DESCRIPTION:

As a primary function of cloud storage services, data synchronization (sync) enables the client to automatically update local file changes to the remote cloud through network communications. Mobile cloud storage services have gained phenomenal success in recent few years. In this paper, we identify. For example, a minor document editing process in Dropbox may result in sync traffic 10 times that of the modification. Synchronization efficiency is determined by the speed of updating the change of client files to the cloud, and considered as one of the most important performance metrics for cloud storage services.We further implement QuickSync to support the sync operation with Dropbox and Seafile. Our extensive evaluations demonstrate that QuickSync can effectively save the sync time and reduce the significant traffic overhead for representative sync workloads.

MERITS:

- Personal cloud storage services are gaining tremendous popularity in recent years by enabling users to conveniently synchronize files across multiple devices and back up data. Services like Dropbox, Box, Seafile have proliferated and become increasingly popular, attracting many big companies such as Google, Microsoft or Apple to enter this market and offer their own cloud storage services.

DEMERITS:

- analyze and address the synchronization (sync) inefficiency problem of modern mobile cloud storage services.

- Our measurement results demonstrate that existing commercial sync services fail to make full use of available bandwidth, and generate a large amount of unnecessary sync traffic in certain circumstance even though the incremental sync is implemented.

TITLE 2: ENABLING FINE-GRAINED MULTI-KEYWORD SEARCH SUPPORTING CLASSIFIED SUB-DICTIONARIES OVER ENCRYPTED CLOUD DATA.

AUTHOR:H. Li, Y. Yang, T. H. Luan, X. Liang, L. Zhou, and X. Shen

DESCRIPTION:

Using cloud computing, individuals can store their data on remote servers and allow data access to public users through the cloud servers. As. This, however, significantly limits the usability of outsourced data due to the difficulty of searching over the encrypted data. In this paper, we address this issue by developing the fine-grained multi-keyword search schemes over encrypted cloud data. Our original contributions are three-fold. First, we introduce the relevance scores and preference factors upon keywords which enable the precise keyword search and personalized user experience. [6]. simply encrypting the data may still cause other security concerns. For instance, Google Search uses SSL (Secure Sockets Layer) to encrypt the connection between search user and Google server when private data, such as documents and emails, appear in the search results. We have investigated on the fine-grained multikeyword search (FMS) issue over encrypted cloud data, and proposed two FMS schemes. The FMS I includes both the relevance scores and the preference factors of keywords to enhance more precise search and better users' experience, respectively. The FMS II achieves secure and efficient search with practical functionality, i.e., "AND", "OR" and "NO" operations of keywords.

MERITS:

- The enhanced schemes supporting classified sub-dictionaries (FMSCS) to improve efficiency.
- the outsourced data are likely to contain sensitive privacy information, they are typically encrypted before uploaded to the cloud

DEMERTIS:

- The data encryption, however, would significantly lower the usability of data due to the difficulty of searching over the encrypted data

TITLE 3: ENABLING PUBLIC AUDITABILITY AND DATA DYNAMICS FOR STORAGE SECURITY IN CLOUD COMPUTING

AUTHOR:Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li

DESCRIPTION:

Cloud Computing has been envisioned as the next-generation architecture of IT Enterprise. This work studies the problem of ensuring the integrity of data storage in Cloud Computing. In particular, we consider the task of allowing a third party auditor (TPA), on behalf of the cloud client, to verify the integrity of the dynamic data stored in the cloud. The introduction of TPA eliminates the involvement of the client through the auditing of whether his data stored in the cloud are indeed intact, which can be important in achieving economies of scale for Cloud Computing. Although envisioned as a promising service platform for the Internet, this new data storage paradigm in “Cloud” brings about many challenging design issues which have profound influence on the security and performance of the overall system. One of the biggest concerns with cloud data storage is that of data integrity verification at untrusted servers. Although schemes. Then, clients are able to delegate the evaluation of the service performance to an independent third party auditor (TPA), without devotion of their computation resources. In the cloud, the clients themselves are unreliable

or may not be able to afford the overhead of performing frequent integrity checks.

MERITS:

- with private auditability can achieve higher scheme efficiency, public auditability allows anyone, not just the client (data owner), to challenge the cloud server for correctness of data storage while keeping no private information

DEMERITS:

- It moves the application software and databases to the centralized large data centres, where the management of the data and services may not be fully trustworthy.
- This unique paradigm brings about many new security challenges, which have not been well understood

TITLE 4: REMOTE DATA AUDITING IN CLOUD COMPUTING ENVIRONMENTS: A SURVEY, TAXONOMY, AND OPEN ISSUES

AUTHOR: M. Sookhak, A. Gani, H. Talebian, A. Akhunzada, S. U. Khan, R. Buyya, and A. Y. Zomaya

DESCRIPTION:

Handling of Big Data and cloud computing are the two important prime concerns which have become more and more popular in recent years. In this paper, we Distributed File System is a client-based application which permits its users to access, process and modify the data which is stored on a remote server as if it existed on their local systems. Centralized cache management is a mechanism which significantly improves the Query response time of the file system. It allows users to specify paths to be cached in main memory by HDFS. In this, the NameNode will communicate with its DataNodes that have analyzed the evolution of distributed file systems, their origin, specialty and their development. We started our discussion with the analysis of Network File

system and Andrew File System. We have also discussed the detailed architectures of GFS and HDFS, the two most significant distributed file systems of their time capable enough to handle the Big Data Management. A comparative study between both GFS and HDFS has been done which has resulted in the occurrence of some similarities as well as differences between both GFS and HDFS.

MERITS:

- Due to tremendous hike in data production, the need for the efficient processing, transaction storage or retrieval, and management of the structured and unstructured data have become one of the important issues of the IT industry.

- Have the requested files on their disks, and instruct them to cache the blocks in off-heap caches to improve the efficiency by directly providing the cached path for the same request by the other remote user.

DEMERITS:

- Examine the concept of evolution of various distributed file systems, advantages, and limitations with respect to the cloud computing paradigm.

TITLE 5: PROVABLE DATA POSSESSION AT UNTRUSTED STORES

AUTHOR: G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song

DESCRIPTION:

In recent years, cloud computing has gradually become the mainstream of Internet services. When cloud computing environments become more perfect, the business and user will be an enormous amount of data stored However, when the data is stored in the cloud storage device, a long time, enterprises and users inevitably will have security concerns, fearing that the information is

actually stored in the cloud is still in the storage device or too long without access to, has long been the cloud server removed or destroyed. Therefore, this scheme goal to research and design for data storage cloud computing environments that are proved. Therefore, how to backup data files in the user not the case, found an efficient and securely ways of good information to perform periodically verification, allowing users to know his information file is stored securely on the server,. From the above, the user data files stored on the server in the cloud, in order to know whether the server actually storing data files, users will be timely made to the server a number of challenges (Challenge), so that the server that the use of the archives were stored in the cloud does to the user ease. Shows the first user data files stored on the server, shows the server certificate data to the user actually stored on the server. In the literature, proposed a data storage proved Provable Data Possession (PDP) system, which applies to of cloud in an untrusted storage server, based on RSA of main plant with state verify that the label is used to check the integrity of the data stored in the cloud, which allows unlimited number of storage server authentication, and also provides a public authentication method, but also the use of asymmetric-key system and the data must be calculated in each block encryption and tags the action, making it a relatively large amount of computation. Compared to the literature of PDP protocol, the literature for the previous method proposed by PDP extension of a new dynamic storage technology, because, in this new method uses

MERITS:

- The symmetric cryptography to encrypt, making information storage, bandwidth and computational smaller, more efficient.
- In the remote cloud storage devices, hoping to achieve random access, data collection, reduce costs, and facilitate the sharing of other services.

DEMERITS:

- This data storage is cloud computing environment is an important security issue.
- resulting in businesses and users in the future can't access or restore the data files

TITLE 6: ENGINEERING SEARCHABLE ENCRYPTION OF MOBILE CLOUD NETWORKS: WHEN QOE MEETS QOP

AUTHOR: H. Li, D. Liu, Y. Dai, and T. H. Luan

DESCRIPTION:

The mobile cloud computing applications, data outsourcing, such as iCloud, is fundamental, which outsources a mobile user's data to external cloud servers and accordingly provides a scalable and "always on" approach for public data access. With although encryption increases the quality of protection (QoP) of data outsourcing, it significantly reduces data usability and thus harms the mobile user's quality of experience (QoE).Mobile applications, such as social networking, healthcare, and media streaming, have already become an integral part of our daily lives. However, weak processing rate, and limited local storage, have significantly impeded the improvement of mobile service utilities. This article investigates the QoE and QoP balancing of data outsourcing by developing a flexible and fine-grained searchable encryption scheme over outsourced data. In the remainder of this article we first overview the searchable encryption technique in mobile cloud networks from the perspective of system definition and modelling. Then we identify the key influencing factors of QoE and QoP in searchable encryption and the state-of-the-art research.

MERITS:

- Mobile cloud computing can effectively address the resource limitations of mobile devices, and is therefore essential to enable extensive resource consuming mobile computing and communication applications.

DEMERITS:

- Mobile cloud computing, by integrating cloud computing in mobile networks, has been recognized as a key technique to provide mobile users with more diversified and flexible services.

- the inherent limitations of mobile devices including low battery life,

TITLE 7: AN EFFICIENT AND SECURE DYNAMIC AUDITING PROTOCOL FOR DATA STORAGE IN CLOUD COMPUTING

AUTHOR: Kan Yang, Xiaohua Jia

DESCRIPTION:

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 cloudIt protects the data privacy against the auditor by combining the cryptography method with the bilinearity property of bilinear paring, rather than using the mask technique. Thus, our multi-cloud batch auditing protocol does not require any additional organizer. Our batch auditing protocol can also support the batch auditing for multiple owners. Furthermore,thus. 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.

MERITS:

- Our auditing scheme incurs less communication cost and less computation cost of the auditor by moving the computing loads of auditing from the auditor to the server, which greatly improves the

auditing performance and can be applied to large scale cloud storage systems.

- an efficient and secure dynamic auditing protocol is desired to convince data owners that the data are correctly stored in the cloud

DEMERITS:

- 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.

TITLE 8: PRIVACY-PRESERVING PUBLIC AUDITING FOR DATA STORAGE SECURITY IN CLOUD COMPUTING

AUTHOR: Cong Wang, Qian Wang, and Kui Ren, Wenjing Lou

DESCRIPTION:

In this paper, we utilize and uniquely combine the public key based homomorphic authenticator with random masking to achieve the privacy-preserving public cloud data auditing system, which meets all above requirements, we further explore the technique of bilinear aggregate signature to extend our main result into a multi-user setting, where TPA can perform multiple auditing tasks simultaneously. In this paper, we propose a privacy-preserving public auditing system for data storage security in Cloud Computing. We utilize the homomorphism authenticator and random masking to guarantee that TPA would not learn any knowledge about the data content stored on the cloud server during the efficient auditing process,. Considering TPA may concurrently handle multiple audit sessions from different users for their outsourced data files, we further extend our privacy-preserving public auditing protocol into a multi-user setting, where TPA can perform the multiple auditing tasks in a batch manner.

MERITS:

- Extensive security and performance analysis shows the proposed schemes are provably secure and highly efficient.
- To support efficient handling of multiple auditing tasks

DEMERITS:

- 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

TITLE 9: SCALABLE AND EFFICIENT PROVABLE DATA POSSESSION

AUTHOR: Giuseppe Ateniese, Roberto Di Pietro, Luigi V. Mancini, and Gene Tsudik

DESCRIPTION:

The main issue is how too frequently, the storage server is assumed to be untrusted in terms of both security and reliability. (In other words, it might maliciously or accidentally erase hosted data; it might also relegate it to slow or off-line storage.) The problem is exacerbated by the client being a small computing device with limited resources. In this paper, we construct a highly efficient and provably secure PDP technique based entirely on symmetric key cryptography, while not requiring any bulk encryption. We developed and presented a step-by-step design of a very light-weight and provably secure PDP scheme. It surpasses prior work on several counts, including storage, bandwidth and computation overheads as well as the support for dynamic operations. However, since it is based upon symmetric key cryptography, it is unsuitable for public (third-party) verification. A natural solution to this would be a hybrid scheme combining elements of and our scheme. To summarize, the work described in this paper represents an important step forward towards practical

PDP techniques. We expect that the salient features of our scheme make it attractive for realistic applications.

MERITS:

- Efficiently and securely verify that a storage server is faithfully storing its client's (potentially very large) outsourced data.
- Very low cost and support for dynamic outsourced data

DEMERITS:

- Prior work has addressed this problem using either public key cryptography or requiring the client to outsource its data in encrypted form.

TITLE 10: HIDING SECRETS IN SOFTWARE: A CRYPTOGRAPHIC APPROACH TO PROGRAM OBFUSCATION

AUTHOR:Sanjam Garg, Craig Gentry, Shai Halevi, Mariana Raykova, Amit Sahai, and Brent Waters

DESCRIPTION:

In this article, we describe some rigorous cryptographic answers to these quasi-philosophical questions. We also discuss our recent "candidate indistinguishability obfuscation" scheme and its implications. However, it is a recurring theme in security engineering that resistance to one set of attacks is no guarantee that a system cannot be broken by other means. And so, many of these obfuscation schemes have been followed by corresponding schemes for deobfuscation. We described a candidate indistinguishability obfuscation scheme, and some of the exciting applications it makes possible. However,

MERITS:

- a lot remains to be done—to base obfuscation on well-established assumptions, to build a practical scheme to truly understand what

obfuscation means—before cryptographic obfuscation can move from being a proof of concept to a widely-deployed privacy enhancing technology.

DEMERITS:

- Previous work on obfuscation has focused on making code resistant/unintelligible to particular attacks, such as known techniques for static and dynamic analysis

2.1 EXISTING SYSTEM

- In public cloud environment, most clients upload their data to PCS and check their remote data's integrity by Internet. When the client is an individual manager, some practical problems will happen.
- The computation overhead of verification by the auditor linearly increases with the size of the verified data set.
- Here third party public auditing scheme for the regenerating-code-based cloud storage. To solve the regeneration problem of failed authenticators in the absence of data owners, if these data cannot be processed just in time, the manager will face the loss of economic interest.
- In order to prevent the case happening, the manager has to delegate the proxy to process its data. In PKI (public key infrastructure), remote data integrity checking protocol will perform the certificate management.
- When the manager delegates some entities to perform the remote data integrity checking, it will incur considerable overheads since the verifier will check the certificate when it checks the remote data integrity.

2.1.1 Disadvantage of Existing System:

- The cryptographic techniques for the purpose of data security protection cannot be directly user's control.
- Therefore, verification of correct data storage in the cloud must be conducted without explicit knowledge of the whole data.
- Considering various kinds of data for each user stored in the cloud and the demand of long term continuous assurance of their data safety, the problem of verifying correctness of data storage in the cloud becomes even more challenging.
- This is not just a third party data warehouse. The data stored in the cloud may be often updated by the users.

2.2 PROPOSED SYSTEM

- An efficient distributed scheme with data in the cloud is been made. Here we are using the erasure code technique for distribute the data to cloud locations and access the data from cloud.
- User can register and login into their account. Provided an option to store, share and access the data from cloud storage. Here we are using the double ensured scheme for storing data into the cloud.
- First is your data or file splited into multiple parts and it will store into different cloud server locations. Each and every file generates the key-code for auditing.

- Then second is each and every splited file will encrypt before store into different locations. The shared users can edit the file in the cloud with file owner's permission. That file eligible of own public auditing.
- Search and download the files, at the time of download user should use the security key. As an authentication success it will be decrypt and combine to get the original data from cloud.
- Moreover, we design a novel public verifiable authenticator, which is generated by a couple of keys and can be regenerated using partial keys.
- Thus, our scheme can completely release data owners from online burden. In addition, we randomize the encode coefficients with a pseudorandom function to preserve data privacy.
- Extensive security analysis shows that our scheme is provable secure under random oracle model and experimental evaluation indicates that our scheme is highly efficient and can be feasibly integrated into the regenerating code- based cloud storage.

2.2.1 Advantages of Proposed System*:*

- Compared to a lot of its predecessors, which only provide binary results about the storage state across the distributed servers, the challenge-response protocol in our work more provides the localization of data error.
- Unlike most prior works used for ensuring remote data integrity, the new scheme supports secure and efficient dynamic operations on data blocks, including: update, delete and append.
- Extensive protection and act analysis demonstrate that the proposed scheme is extremely efficient and resilient beside Byzantine failure, malicious data modification attack, and even server colluding attacks

SYSTEM REQUIRMENTS

3.1 Hardware Requirements

Processor	:	Pentium Dual Core 2.3 GHz
Hard Disk	:	250 GB or Higher
Ram	:	1 GB (Min)

3.2. Software Requirements

Operating System	:	Windows XP or Higher
Languages used	:	Java (JSP, Servlet), HTML
Tools	:	JDK 1.7, Net Beans 7.0.1, SQLyog
Backend	:	My SQL

\

CONCLUSION

A privacy-preserving public auditing system for data storage security in cloud computing. We utilize the 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 the burden of cloud user from the tedious and possibly expensive auditing task, but also alleviates the users' fear of their outsourced data leakage. Considering TPA may concurrently handle multiple audit sessions from different users for their outsourced data files, we further extend our privacy-preserving public auditing protocol into a multiuser setting, where the TPA can perform multiple auditing tasks in a batch manner for better efficiency.

REFERENCE:

1. Y. Cui, Z. Lai, X. Wang, N. Dai, and C. Miao, "Quicksync: Improving synchronization efficiency for mobile cloud storage services," in Proceedings of MobiCom. ACM, 2015, pp. 592–603.

2. H. Li, Y. Yang, T. H. Luan, X. Liang, L. Zhou, and X. Shen, "Enabling fine-grained multi-keyword search supporting classified sub-dictionaries over encrypted cloud data," IEEE Transactions on Dependable and Secure Computing, vol. 13, no. 3, pp. 312–325, 2016.

3. Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, "Enabling public auditability and data dynamics for storage security in cloud computing," IEEE Transactions on Parallel and Distributed Systems, vol. 22, no. 5, pp. 847–859, 2011.

4. M. Sookhak, A. Gani, H. Talebian, A. Akhunzada, S. U. Khan, R. Buyya, and A. Y. Zomaya, "Remote data auditing in cloud computing

environments: A survey, taxonomy, and open issues," ACM Computing Surveys, vol. 47, no. 4, 2015.

5. G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable data possession at untrusted stores," in Proceedings of CCS. ACM, 2007, pp. 598–609.

6. H. Li, D. Liu, Y. Dai, and T. H. Luan, "Engineering searchable encryption of mobile cloud networks: When qoe meets qop," IEEE Wireless Communications, vol. 22, no. 4, pp. 74–80, 2015.

7. K. Yang and X. Jia, "An efficient and secure dynamic auditing protocol for data storage in cloud computing," IEEE Transactions on Parallel and Distributed Systems, vol. 24, no. 9, pp. 1717–1726, 2013.

8. C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for data storage security in cloud computing," in Proceedings of INFOCOM. IEEE, 2010, pp. 19.

9. G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik, "Scalable and efficient provable data possession," in Proceedings of SecureComm. ACM, 2008.

10. S. Garg, C. Gentry, S. Halevi, M. Raykova, A. Sahai, and B. Waters, "Hiding secrets in software: A cryptographic approach to program obfuscation," Communications of The ACM, vol. 59, no. 5, pp. 113– 120, 2016.