RESEARCH ARTICLE OPEN ACCESS

Fully Homomorphic Encryption Based Outsourcing in the Cloud

P.L.Jebin [1], L.Nirmal Jega Selvi [2]
Department of Computer Science and Engineering [1]
Loyola Institute of Technology
Department of Computer Science and Engineering [2]
St. Joseph College of Engineering & Technology
Chennai - India

ABSTRACT

Cloud computing enables the customers to restrict its means of calculation to outsource large-scale computational tasks for the cloud, or an important computer processing power can easily be used in pay-per-use. However, security is the major concern that prevents the wide adoption of the calculation the outsourcing in the cloud, as well, secure outsourcing mechanisms have a great need to protect not only secret information by enabling calculations with encrypted data, and to protect customers against the malicious behaviour by validating the calculation result. Such a mechanism provides end-to- end data privacy guarantee in the cloud server and the clients. In order to achieve the practical effectiveness, proposed mechanism design explicitly encrypts the data before the outsourcing, in the cloud and allowing a third party auditor to perform the integrity of the public service verification of database on the internet. By activating fuzzy search by keyword encrypted cloud data ensures an efficient use of user data. The flexibility allows us to discover appropriate security/efficiency compromise via higher level construct of data calculations. To validate the calculation result, fully explore the homomorphism encryption calculation and calculate the necessary and sufficient conditions that correct result must satisfy.

Keywords:- FHE, symmetric, fuzzy search keyword, TPA.

I. INTRODUCTION

Cloud computing is the long dream vision of it as a utility, or cloud customers can store to distance their folders in the clouds in order to take advantage of the on-demand applications of the highest quality and services from a shared pool of configurable computing resources. Several trends are the opening of the period of Cloud computing, which is an Internet-based development and use of computer technology. The always less expensive and more powerful processors, together with the software as a service (SaaS) computing architecture, are transforming data centers into pools of computer service on a large scale. The increase in the bandwidth of the network and reliable and flexible network connections are that it is still possible that users can now subscribe services of high quality from data and software that reside only on remote data centres. Moving data in the cloud computing offers a great convenience for the users because they do not have to worry about the complexities of hardware direct management. If the Cloud computing has been envisaged as the new generation of computing architecture of the enterprise. Unlike traditional solutions, or it departments are under good, logical and physical checks of the IT staff, cloud computing moves the application software and databases for large data centers, or the management of the data and services may not be completely trustworthy. This single attribute, however, poses many new security challenges that have not been well understood. However, from the point of view of the security of the data, which has always been an important aspect of the quality of service, Cloud Computing inevitably poses new challenges to security threats for a number of reasons.

1. First of all , the cryptographic primitives for the purposes of data security protection cannot be directly adopted due to the users' control of data loss in the Cloud Computing. Therefore, the verification of the correct data storage for the cloud must be conducted without explicit knowledge of the data set. Taking into account the different types of data for each user stored in the cloud and the demand for long-term continuous assurance of their safety data, the problem of checking the accuracy of the stored data in the cloud becomes even more difficult.

2. Secondly, Cloud Computing is not only a third of data warehouse. The data stored in the cloud computing may be updated frequently by the users, including the insertion, deletion, modification, addition, reorganization, etc.

To ensure accuracy for storing dynamic updating of data is therefore of paramount importance. These techniques, which can be useful for ensuring the accuracy of storage without that users with data, cannot respond to all threats to security in the cloud data storage, since they are all focusing on a single server scenario and most of them do not consider dynamic operations on the data. As a complementary approach, researchers have also proposed distributed protocols to ensure accuracy of storage on multiple servers or of their peers. Once again, none of these regimes distributed is aware of the dynamic data operations. Accordingly, their applicability in the cloud data storage can be considerably limited.

In this Paper, focus on cloud data storage of security, which has always been an important aspect of the quality of service. To ensure the accuracy of the data of the users in the cloud, and propose an effective and flexible mechanism distributed scheme with two salient characteristics, and to oppose its predecessors. By using the token homomorphism distributed with verification of erasing of coded data, this scheme achieved the integration of storage accuracy of insurance and error of location data, that is to say, the identification of rogue server (s). Unlike most prior works, the new regime takes more secure and efficient dynamic operations on data blocks, including: data update, delete and append. The proposed scheme is very effective and to resilience against failure malicious Byzantine, modification of data, attack and even collusion attacks server.

To combat the leakage of sensitive information, the data must be encoded before the outsourcing in order to give end to end- confidentiality of data assurance in the cloud and beyond. However, the simple data encryption techniques in essence prevent cloud to perform any significant operation in the underlying data in clear text, which makes the calculation of encrypted data a very difficult problem. On the other hand, the operational details in the cloud are not sufficiently transparent to the clients. Fully homomorphism encryption (FHE) regime, explicitly encrypts the data before the outsourcing in public constraint solvers running on the cloud and allowing a third party auditor to perform the integrity of the public service verification of database on the internet. By activating fuzzy search by keyword encrypted cloud data ensures an efficient use of user data. The flexibility which allows us to explore appropriate security/efficiency compromise via higher-level abstraction of data calculations. To validate the calculation result, fully explore the homomorphic encryption calculation and calculate the necessary and sufficient conditions that correct result must satisfy. Such a result verification mechanism is extremely efficient and incurs close to zero additional cost.

II. METHODOLOGY

The proposed system has an effective outsourcing calculation of loads often contain sensitive information, such as the company financial records, research data owner, or personal health information, etc. The framework of proposed approach is shown in Fig 1. The steps involved in proposed methodology are as follows:

A. Fully homomorphic Encryption

Fully homomorphic encryption (FHE) regime, a general result of calculation secure outsourcing reg

Symmetrical or asymmetrical, but concentrate on the symmetric case. There is a fourth algorithm evaluate, which is associated with the game FE of allowed features. For any function f of FE and any ciphertexts c1; : : : ; ct with ci encrypts(pk;mi), the algorithm EvaluateE(pk; f; c1; : : : ; ct) outputs a cryptogram which encrypts f(m1; : : : ;mt) { i.e. , such that decrypts(sk; c) = f(m1; : : : ;mt). (For convenience, let us assume that f has an output. If f has k outputs, then Evaluate E outputs k cipher texts encrypt that f(m1; : : : ;mt) collectively). By focusing on the computer engineering and optimization tasks, explorer practically effective mechanisms to secure outsourcing of linear programming (LP) calculations. Linear programming is a algorithmic and calculation tool that captures the first order effects of various system parameters that must be optimized, and is essential to the optimization engineering. It has been widely used in various disciplines of engineering sciences, analyze and optimize real systems, such as packet routing, flow control, the power management of data centers, etc. because LP calculations require a significant amount of computing power and are, in general, of confidential data and propose to decompose explicitly the calculation LP outsourcing in public LP constraint solvers running on the private cloud and LP parameters belonging to the client. The flexibility of such a decomposition allows us to explore higher-level abstraction of calculations LP . To enable the secure and practice of outsourcing LP under the above model, this design of the mechanism should achieve the following security and performance guarantees.

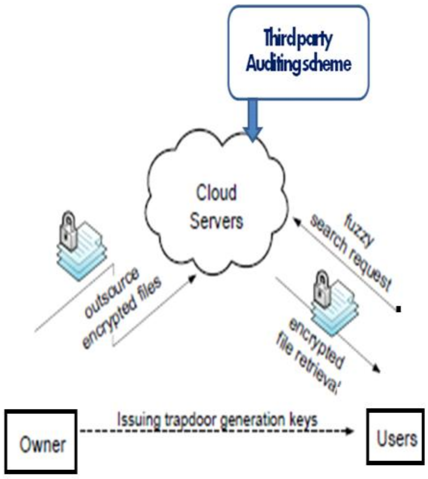
Third party Auditing scheme
Cloud Servers
outsource encrypted files
fuzzy search request
encrypted file retrieval
Owner
Issuing trapdoor generation keys
Users

Fig 1. Framework of proposed system

1) Accuracy: Any server cloud which follows faithfully the mechanism must produce an output, which can be decrypted and verified successfully by the client.

2) Soundness: No cloud server can generate incorrect output which cannot be decrypted and verified successfully by the client with non-negligible probability.

3) Input/output privacy: no sensitive information from the client of private data can be derived by the cloud server .
In this framework, the process of cloud server can be represented by the algorithm ProofGen and the process on the client can be organized in three algorithms (Keygen.ProbEnc, ResultDec).

• Keygen(1k) → {K}. It is a randomized trial key generation algorithm which takes a security system parameter k, and returns a secret key K that is subsequently used by the client to encrypt the target LP problem.

• ProbEnc(K,_) → {_K}. This algorithm encrypts the input tuple _ in _K with the secret key K. Depending on the problem transformation, the input encrypted _K has the same form as _, and thus defines the problem to solve in the cloud.

• ProofGen(_K) → { (y) }. This algorithm improves a generic solver which solves the problem _K to produce both output y and a proof . The output y later decrypts to x, and is subsequently used by the client to verify the accuracy of the y or x.

• ResultDec (K,_, y) → {x,⊥}. This algorithm may choose to verify either y or x via the evidence . In any case, a correct output x is produced by decrypting y using the secret K. The algorithm outputs ⊥ when validation fails, indicating that the cloud server was not performing the computation faithfully.

B. Third Party Audit System

An auditing structure for cloud storage systems and an effective protection of the private life preserves the audit protocol. The verification protocol that supports the data dynamic operations, which is efficient and safe demonstrable way in the random oracle model. The verification protocol to support batch auditing for both multiple owners and multiple clouds, without use of trusted organizer. It reduces the calculation cost of the auditor. In this section, introduces SSOP (secure storage outsourcing protocols) which includes SShP(Secure Sharing based Protocol), SCoP(Secure Coding based Protocol) and SEnP(Secure Encryption based Protocol) to overcome the security vulnerabilities existing in resilient storage outsourcing schemes. These are ensuring the confidentiality and integrity of user data during the loading and storage. After that, make analysis of the confidence of security protocols. The safety analysis demonstrated the protocols can achieve secure storage outsourcing in the cloud computing and resist against different attacks.

C. Fuzzy search by keyword

Fuzzy search by keyword encrypted cloud data, which should be explored for effective use of data in the Cloud. Fuzzy search by keyword aims to accommodate several typos and representation of inconsistencies in different user input search for acceptable use of the system and overall user search experience, while protecting the privacy keyword. In order to further improve the range of secure cloud the use of data services. The concept of fuzzy search naturally supports correspondence search, a basic and prevailing instrument which is widely used in research of information.

This architecture is composed of three entities: owner of data, user and cloud server. Under the cloud paradigm, the owner of the data can represent either the person or the customer of the company, which is based on the cloud server remote data storage and maintenance, and therefore is exempt from the charge of construction and maintenance of storage facilities. Suppose that data owner is a collection of n data files C = (F1; F2; : : : ; FN) to be stored in the cloud server, or a predefined set of keywords in separate C is denoted as W = fw1 ;w2; : :: ;wpg. To keep confidential data from unauthorized entities, cryptographic methods must be applied to the data collection C by the owner before the outsourcing, so that the confidentiality of data can be assured in the cloud and beyond. The simple enumeration method in constructing fuzzy key-word sets would introduce large storage complexities, which greatly affect the usability.

For example, the following is the listing variants after a substitution operation on the first character of keyword CASTLE:{AASTLE, BASTLE, DASTLE, YASTLE, ZASTLE}. Wildcard – Based Technique, Gram - Based Technique,Symbol – Based Trie – traverse Search Scheme are introduced

1. Wildcard – Based Technique:

In the above straightforward approach, all the variants of the keywords have to be listed even if an operation is performed at the same position. Based on the above observation, we proposed to use an wildcard to denote edit operations at the same position. The wildcard-based fuzzy set edits distance to solve the problems.

For example, for the keyword CASTLE with the pre-set edit distance 1, its wildcard based fuzzy keyword set can be constructed as SCASTLE, 1 = {CASTLE, *CASTLE,*ASTLE, C*ASTLE, C*STLE, CASTL*E, CASTL*, CASTLE*}.

2. Gram – Based Technique

Another efficient technique for constructing fuzzy set is based on grams. The gram of a string is a **substring** that can be used as a signature for efficient approximate search. While gram has been widely used for constructing inverted list for approximate string search, we use gram for the matching purpose. We propose to utilize the fact that any primitive edit operation will affect at most one specific character of the keyword, leaving all the remaining characters untouched. In other words, the relative order of the remaining characters after the primitive operations is always kept the same as it is before the operations. For example, the gram-based fuzzy set SCASTLE, 1 for keyword CASTLE can be constructed as {CASTLE, CSTLE, CATLE, CASLE, CASTE, CASTL, and ASTLE}.

3. Symbol – Based Trie – traverse Search Scheme

To enhance the search efficiency, now propose a symbol-based trie-traverse search scheme, where a multi-way tree is constructed for storing the fuzzy keyword set over a finite symbol set. The key idea behind this construction is that all trapdoors sharing a common prefix may have common nodes. The root is associated with an empty set and the symbols in a trapdoor can be recovered in a search from the root to the leaf that ends the trapdoor. All fuzzy words in the trie can be found by a depth-first search.

d.Trapdoor Generation

To initialize the service, owner of data will distribute request for research (flap) generation sk keys to authorized users, as partners in a collaboration team or employees in the company. Here, assume that the authorization between the owner of the data and the users is appropriate. Research solidly the set of files for a keyword w, an authorized user uses the flap generation key sk to generate a request for research Tw = f(sk; w) via a one-way function f(_), and of the present on the cloud, which then executes the search on the data file collection C without decryption and sends all encrypted files containing the specific keyword w, denoted FIDw. For high-level system and usability research user flexibility, fuzzy search by keyword must be enabled in the cloud the use of service data: Fuzzy search by keyword supports various user input search and/or by typing habits by integrating the two minor typos and format of inconsistencies. Cloud Server expects to return the corresponding files when users' search entries correspond exactly the predefined keywords or the nearest possible corresponding files based on keyword similarity metrics, when exact match fails.

III. RESULT AND DISCUSSION

This scheme used public key based Homomorphic. The tags in the audit of a data file, thus providing public verifiability. This method has less overhead than their previous system and allows us to block updates, deletions, and added to the stored file, which has also been supported in our work. However, their scheme is concentrated on a single server scenario and does not address small data corruptions, leaving the distributed scenario and the data of error recovery problem unexplored. Ensure that the data possession of multiple replicas in the distributed storage system. They have extended the PDP system to cover multiple replicas without coding each replica separately, providing guarantees that multiple copies of data are effectively maintained.

The methodology proposed for the building base generic fuzzy keyword set can be correctly applied to the asymmetric case for tolerating the errors and/or representation the inconsistencies. However, further research should be conducted to investigate specific solutions to expect better performance in research for the public key based fuzzy search on turnover data in cloud. Following the current research on the safety and effective cloud the use of data, another promising research task is the exploration of several key words search semantics. Given the large number of data files and the corresponding keywords, there is a natural demand for users to refine the targeted data files by providing more relevant information. Thus, the support of semantic search, which takes into account jointly of the keywords, the sequence of keywords, and even the complex natural language semantics to produce relevant search results, is a necessity, and can be an interesting research work to be fully explored.

Finally, an important vein of research resides with the support to secure file collection update. In Cloud Computing, outsourcing of data may be changing frequently due to updates by clouds the customers. Here an update can be either a document Adding or deleting. The proposed approaches for fuzzy search and similarity search are all based on the activity of the art SSE, or updates to indexes are not supported in an effective manner. Building updateable searchable index while preserving the benefits of existing SSE can be difficult.

IV. CONCLUSION

This system has investigated on the problem of the security of the data in the cloud data storage, which is essentially a distributed storage system. To ensure the accuracy of the data of the users in the clouds data storage, has proposed a flexible and effective mechanism distributed scheme with explicit dynamic data support, including block update, delete, and add. The owners rely on erasure correction code in the distribution of the file preparation to provide a redundancy parity vectors and ensure the reliability of the data. By using the token homomorphic distributed with verification of erasure coded data, this scheme achieved the integration of storage insurance accuracy and error of location data, that is to say, when the data corruption has been detected during storage of verification based on the distributed servers, we can almost guarantee the simultaneous identification of the rogue server(s).

Through detailed security and performance analysis, this scheme is very effective and resilient to Byzantine failure malicious, modification of data, attack and even collusion attacks server. . The most promising, that it regarded as a model in which public verifiability is applied. Public verifiability, supported in TPA allows you to undertake an audit of the cloud of data storage without the demanding users, feasibility or resources.

The storage of data security in the Cloud Computing, a region full of challenges and of paramount importance, is still in its infancy, and many research problems are not yet identified. Envision several possible directions for future research in this area.

REFERENCES

[1] Cong Wang, Kui Ren, Jia Wang and Qian Wang, Member, IEEE,"Harnessing the Cloud for Securely Outsourcing Large-Scale Systems of Linear Equations" IEEE transactions on parallel and distributed systems, vol. 24, no. 6, june 2013.

[2] Cong Wang, Qian Wang, and Kui Ren Department of ECE.Illinois Institute of Technology," Towards Secure and Effective Utilization over Encrypted Cloud Data" 2011 31st International Conference on Distributed Computing Systems Workshops.

[3] Cong Wang Ning , CAD, Kui Ren, Wenjing Lou, "enabling secure and efficient class search by keyword on the outsourced Cloud data". ieee transactions on parallel and distributed systems, vol. 23, No. 8, August 2012.

[4] C. Wang, K. Ren, J. Wang, and K. Mahendra Raje Urs,"The mastery of the cloud to correctly solve Large-Scale systems of linear equations", Proc. 31E Int'l Conf. Distributed Computing Systems (ICDCS), pp. 549-558, 2011.

[5] MR. Armbrust et al. , "A view of Cloud Computing ", Comm. ACM,vol. 53, No. 4, PP. 50-58, April 2010.

[6] Ji Soo Park , Ki Jung Yi and Jong Hyuk Park SSP-MCloud. A study on the safety Service Protocol for Mobile Smartphone centered on Cloud Computing. Lecture Notes in electrical engineering, 2012, 107 (1)165-172.

[7] Wei Ren, Linchen Yu,Ren ,Gao Feng Xiong. Lightweight and compromise resilient storage outsourcing withDistributed SecureAccessibility Mo bile in Cloud Computing.T. Singha Science and Technology , 2011, 16 (5): 520-528.

[8] C. Wang, N. Cao, J. Li, K. Ren, and W. Lou, "Secure class Search by keyword encrypted via the cloud Data," Proc. IEEE 30th Int'lconf. Distributed Computing Systems (ICDCS ' 10), 2010.

[9] P. Mell and T. Guy Angelloz, "Draft nist working definition of cloud computing , "reference on January 23rd, 2010.

[10] C. Gentry, "Computing arbitrary functions of encrypted data, "Common.ACM, vol. 53, No. 3, PP. 97-105, 2010.

[11] Sun Microsystems, Inc. , "bring the customers trust in cloud computing with transparent security ", 2009.

[12] Mr. J. Atallah, K. N. Pantazopoulos, J. R. Rice and E. H. Spafford, "secure outsourcing of scientific calculations," advances in computers,vol. 54, PP. 216-272, 2001.

[13] S. Hohenberger and A. Lysyanskaya, "How securely outsource cryptographic calculations," in Proc. of CPTS, 2005, pp. 264-282.

[14] Mr. J. Atallah and J. Li, "secure outsourcing of these comparisons , "Int'l J. Inf. Sec., vol. 4, No. 4, PP. 277-287, 2005.

[15] D. Benjamin and M. J. Atallah, "Private and cheating-free outsourcing of algebraic calculations," in Proc. of Int'l Conf. on privacy, security and trust (PST), 2008, pp. 240-245.