International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 06 Issue: 06 | June - 2022 Impact Factor: 7.185 ISSN: 2582-3930

REALTIME DATA PROVABLY SECURE FINE-GRAINED DATA ACCESS CONTROL OVER MULTIPLE CLOUD SERVERS

Mrs.S. Panneerselvi , M.E – II[nd] year, CSE, P.S.V. College Of Engineering & Technology, Krishnagiri.

Prof.B.Sakthivel, Professor, Department of Computer Science and Engineering, P.S.V. College Of Engineering & Technology, Krishnagiri.

ABSTRACT

Cloud Computing (CC) allows cloud users to have on-demand access to cloud services. Amobile cloud model helps in analyzing the information regarding the patients' records and also in extracting recommendations in healthcare applications. In mobile cloud computing, a fine- grained level access control of multi-server cloud data is a pre-requisite for successful execution of end users applications. In this paper, we propose a new scheme that provides a combined approach of fine grained access control over cloud-based multi-server data along with a provably secure mobile user authentication mechanism for the Healthcare Industry 4.0. To the best of our knowledge, the proposed scheme is the first to pursue fine-grained data access control over multiple cloud servers in a mobile cloud computing environment. The proposed scheme has been validated extensively in different heterogeneous environment where its performance was found good in comparison to other existing schemes. This project is developed C#.net as front end.

1. INTRODUCTION

The foundations of cloud computing lie in the outsourcing of computing tasks to the third party. It entails the security risks in terms of confidentiality, integrity and availability of data and service. The issue to convince the cloud clients that their data are kept intact is especially vital since the clients do not store these data locally. Remote data integrity checking is a primitive to address this issue. For the general case, when the client stores his data on multi-cloud servers, the distributed storage and integrity checking are indispensable. On the other hand, the integrity checking protocol must be efficient in order to make it suitable for capacity-limited end devices. Thus, based on distributed computation, we will study distributed remote data integrity checking model and present the corresponding concrete protocol in multi-cloud storage.

This project consider an ocean information service corporation Cor in the cloud computing environment. Cor can provide the following services: ocean measurement data, oceanenvironment monitoring data, hydrological data, marine biological data, GIS information, etc. Besides of the above services, Cor has also some private information and some public information, such as the corporation's advertisement. Cor will store these different ocean data on multiple cloud servers. Different cloud service providers have different reputation and charging standard. Of course, these cloud service providers need different charges according to the different security-levels. Usually, more secure and more expensive. Thus, Cor will select different cloud service providers to store its different data. For some sensitive ocean data, it will copy these data many times and store these copies on different cloud servers. For the private data, it will store them on the private cloud server. For the public advertisement data, it will store them on the cheap public cloud server. At last, Cor stores its whole data on the different cloud servers according to their importance and sensitivity. Of course, the storage selection will take account into the Cor's profits and losses. Thus, the distributed cloud storage is indispensable. In multi-cloud environment, distributed provable data possession is an important element to secure the remote data. In PKI (public key infrastructure), provable data possession protocol needs public key certificate istribution and management. It will incur considerable overheads since the verifier will check the certificate when it checks the remote data integrity. In addition to the heavy certificate verification, the system also suffers from the other complicated certificates management such as certificates generation, delivery, revocation, renewals, etc. In cloud computing, most verifiers only have low computation capacity. Identity-based public

key cryptography can eliminate the complicated certificate management. In order to increase the efficiency, identity-based provable data possession is more attractive. Thus, it will be very meaningful to study the ID-DPDP.

LITERATURE SURVEY

1) Scalable And Efficient Provable Data Possession Authors: Hadassa Katta, Vivek Kolla P and Raja Rao

Cloud storage has become an attractive and cost effective alternative for enterprises to outsource their valuable business data. However, there are security concerns pertaining to the integrity of data as the cloud server is treated as "untrusted". To overcome this problem many security schemes came into existence. Recently Zhu et al. presented a technique known as Provable Data Possession (PDP) for data integrity in cloud with distributed storage mechanisms. They considered multiple cloud service providers to store data in cooperative fashion. Their solution makes use of homomorphic verifiable response indeed and multi-prover zero-knowledge system for ensuring data integrity. In this paper we practically implement the PDP scheme proposed by Zhu et al. and build a prototype application to demonstrate the proof of concept. The empirical results reveal that the PDP scheme is very effective and can be used in real time multi-cloud environments.

2) Provable Data Possession at Untrusted Stores

Authors: Giuseppe Ateniese, Randal Burns and Reza Curtmola

We introduce a model for provable data possession (PDP) that allows a client that has stored data at an untrusted server to verify that the server possesses the original data without retrieving it. The model generates probabilistic proofs of possession by sampling random sets of blocks from the server, which drastically reduces I/O costs. The client maintains a constant amount of metadata to verify the proof. The challenge/response protocol transmits a small, constant amount of data, which minimizes network communication. Thus, the PDP model for remote data checking supports large data sets in widely-distributed storage systems. We present two provably-secure PDP schemes that are more efficient than previous solutions, even when compared with schemes that achieve weaker guarantees. In particular, the overhead at the server is low (or even constant), as opposed to linear in the size of the data. Experiments using our implementation verify the practicality of PDP and reveal that the performance of PDP is bounded by disk I/O and not by cryptographic computation.

3) Dynamic Provable Data Possession

Authors: C. Chris Erway, Alptekin Kupcii, Charalampos Papamanthou and Roberto Tamassia

As storage-outsourcing services and resource-sharing networks have become popular, the problem of efficiently proving the integrity of data stored at untrusted servers has received increased attention. In the provable data possession (PDP) model, the client preprocesses the dataand then sends it to an untrusted server for storage, while keeping a small amount of meta-data. The client later asks the server to prove that the stored data has not been tampered with or deleted (without downloading the actual data). However, the original PDP scheme applies only to static (or append-only) files. We present a definitional framework and efficient constructions for dynamic provable data possession (DPDP), which extends the PDP model to support provable updates to stored data. We use a new version of authenticated dictionaries based on rank information. The price of dynamic updates is a performance

change from O(1) to O(log n) (or O(nọ log n)), for a file consisting of n blocks, while maintaining the same (or better, respectively) probability of misbehavior detection. Our experiments show that this slowdown is very low in practice (e.g., 415KB proof size and 30ms computational overhead for a 1GB file). We also show how to apply our DPDP scheme to outsourced file systems and version control systems (e.g., CVS).

4) Provable Possession and Replication of Data over Cloud Servers Authors: Ayad F.Barsoum and M.Anwar Hasan

Cloud Computing (CC) is an emerging computing paradigm that can potentially offer a number of important advantages. One of the fundamental advantages of CC is pay-as-you-go pricing model, where customers pay only according to their usage of the services. Currently, data generation is outpacing users' storage availability, thus there is an increasing need to outsource such huge amount of data. Outsourcing data to a remote Cloud Service Provider (CSP) is a growing trend for numerous customers and organizations alleviating the burden of local data storage and maintenance. Moreover, customers rely on the data replication provided by the CSP to guarantee the availability and durability of their data. Therefore, Cloud Service Providers (CSPs) provide storage infrastructure and web services interface that can be used to store and retrieve an unlimited amount of data with fees metered in GB/month. The mechanisms used for data replication vary according to the nature of the data; more copies are needed for critical data that cannot easily be reproduced. This critical data should be replicated on multiple servers

across multiple data centers. On the other hand, non-critical, reproducible data are stored at reduced levels f redundancy. The pricing model is related to the replication strategy. Therefore, it is of crucial importance to customers to have a strong evidence that they actually get the service they pay for. Moreover, they need to verify that all their data copies are not being tampered with or partially deleted over time. Consequently, the problem of Provable Data Possession (PDP) has been considered in many research papers. Unfortunately, previous PDP schemes focus on a single copy of the data and provide no guarantee that the CSP stores multiple copies of customers' data. In this paper we address this challenging issue and propose Efficient Multi- Copy Provable Data Possession (EMC-PDP) protocols. We prove the security of our protocols against colluding servers. Through extensive performance analysis and experimental results, we demonstrate the efficiency of our protocols.

5) Proofs of Retrievability for Large Files Authors: Ari Juels and Burton S. Kaliski Jr

In this paper, we define and explore proofs of retrievability (PORs). A POR scheme enables an archive or back-up service (prover) to produce a concise proof that a user (verifier) can retrieve atarget file F, that is, that the archive retains and reliably transmits file data sufficient for the user to recover F in its entirety. A POR may be viewed as a kind of cryptographic proof of knowledge(POK), but one specially designed to handle a large file (or bitstring) F. We explore POR protocols here in which the communication costs, number of memory accesses for the prover, and storage requirements of the user (verifier) are small parameters essentially independent of the length of F. In addition to proposing new, practical POR constructions, we explore implementation considerations and optimizations that bear on previously explored, related schemes. In a POR, unlike a POK, neither the prover nor the verifier need actually have knowledge of F. PORs give rise to a new and unusual security definition whose formulation is another contribution of our work.

We view PORs as an important tool for semi-trusted online archives. Existing cryptographic techniques help users ensure the privacy and integrity of files they retrieve. It is also natural, however, for users to want to verify that archives do not delete or modify files prior to retrieval.

3. SYSTEM STUDY

3. 1 EXISTING SYSTEM

The foundations of cloud computing lie in the outsourcing of computing tasks to the third party. It entails the security risks in terms of confidentiality, integrity and availability of data and service. The issue to convince the cloud clients that their data are kept intact is especially vital since the clients do not store these data locally. Remote data integrity checking is a primitive to address this issue. For the general case, when the client stores his data on multi-cloud servers, the distributed storage and integrity checking are indispensable. On the other hand, the integrity checking protocol must be efficient in order to make it suitable for capacity-limited end devices. Thus, based on distributed computation, we will study distributed remote data integrity checking model and present the corresponding concrete protocol in multi-cloud storage.

3.1.1 DRAWBACKS OF EXISTING SYSTEM

- Data checking in more complex using multi servers.
- Needed large storage space.
- In sufficient data loss.

3.2 PROPOSED SYSTEM

In identity-based public key cryptography, this paper focuses on distributed provable datapossession in multi-cloud storage. The protocol can be made efficient by eliminating the certificate management. We propose the new remote data integrity checking model: ID-DPDP. The system model and security model are formally proposed. Then, based on the bilinear pairings, the concrete ID-DPDP protocol is designed. In the random oracle model, our ID-DPDP protocol is provably secure. On the other hand, our protocol is more flexible besides the high efficiency. Based on the client's authorization, the proposed ID-DPDP protocol can realize private verification, delegated verification and public verification.

3.2.1 ADVANTAGES OF THE PROPOSED SYSTEM

- It has more significant storage space.
- It provides secure public data's.

- Using Private Key generation.

3.3 MODULES DESCRIPTION1.Cloud Module :

In this module, we create a local Cloud and provide priced abundant storage services. The users can upload their data in the cloud. We develop this module, where the cloud storage can be made secure. However, the cloud is not fully trusted by users since the CSPs are very likely to be outside of the cloud users' trusted domain. Similar to we assume that the cloud server is honest but curious. That is, the cloud server will not maliciously delete or modify user data due to the protection of data auditing schemes, but will try to learn the content of the stored data and the identities of cloud users.

2. Register Module:

In this module, we have to create users to allocate files by block tag pairs to combiner.thw work of registered users are to create a valid file then to store it in a cloud server. User also called as Client.

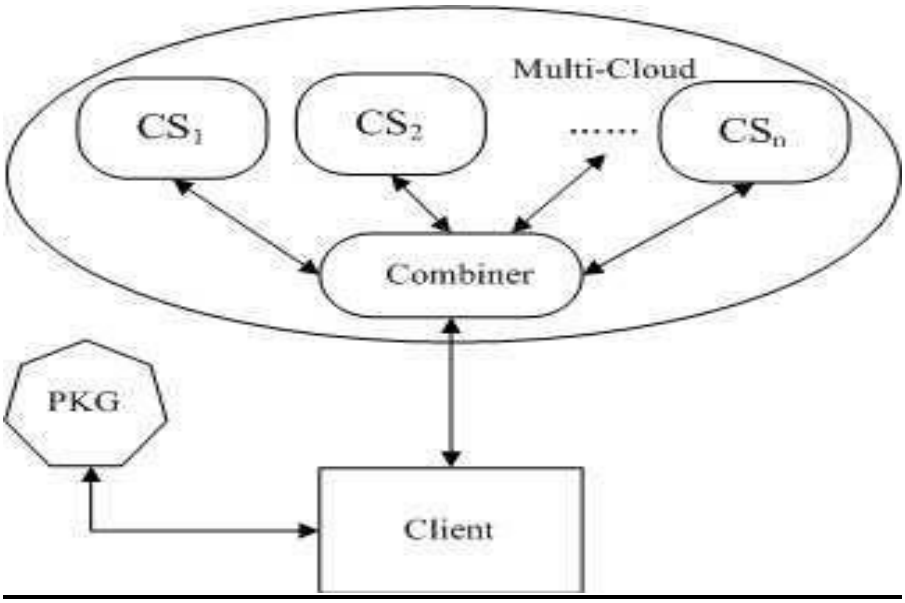
Client: an entity, which has massive data to be stored on the multi-cloud for maintenance and computation, can be either individual consumer or corporation.

3. Client Key Segregation module:

In this module, we will allocate a random key which will be accessible only by the client.*PKG* (Private Key Generator): an entity, when receiving the identity, it outputs the corresponding private key. While registering a client it will automatically send through secure channel.

4. SYSTEM DESIGN

4.1 SYSTEM ARCHITECTURE



5. CONCLUSION

In multi-cloud storage, this paper formalizes the ID-DPDP system model and security model. At the same time, we propose the first ID-DPDP protocol which is provably secure under the assumption that the CDH problem is hard. Besides of the elimination of certificate management, our ID-DPDP protocol has also flexibility and high efficiency. At the same time, the proposed ID-DPDP protocol can realize private verification, delegated verification and publicverification based on the client's authorization.

The system has been designed, developed and implemented after tedious testing and debugging the goals of the system have reached in such a manner that the system is flexible for any change in the near future. The coding has been done cautiously so that any developer can follow the program easily with the knowledge of the convections followed hence it is easy to be maintained. Testing has been completed and a third person, with little knowledge of coding, tested the system for user friendliness and simplicity.

This system satisfies all the requirements of the company and the application is developed by advanced software ASP.Net which is widely used in all applications. This project mainly focus flat registration for any customer or dealer any ware of India. Flat buying and selling very easily.

REFERENCES:

[1] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, ``Public key encryption with keyword search," in Proc. Eurocrypt, 2004, pp. 506_522.

[2] R. Bost, ``6o'o&: Forward secure searchable encryption," in Proc. ACM CCS, 2016, pp. 1143_1154.

[3] R. Bost, P.-A. Fouque, and D. Pointcheval, ``Veri_able dynamic symmetric searchable encryption: optimality and forward security," Int. Assoc. Cryptol. Res., Las Vegas, NV, USA, Tech. Rep. 2016/062, 2016, vol. 62.

[4] R. Bost, B. Minaud, and O. Ohrimenko, ``Forward and backward private searchable encryption from constrained cryptographic primitives," in Proc. ACM CCS, 2017, pp. 1465_1482.

[5] D. Cash, P. Grubbs, J. Perry, and T. Ristenpart, ``Leakage-abuse attacks against searchable encryption," in Proc. CCS, 2015, pp. 668_679.

[6] D. Cash, S. Jarecki, C. S. Jutla, H. Krawczyk, M.-C. Ro³u, and M. Steiner, ``Highly-scalable searchable symmetric encryption with support for Boolean queries," in Proc. CRYPTO, 2013, pp. 353_373.

[7] D. Cash et al., ``Dynamic searchable encryption in very-large databases: Data structures and implementation," in Proc. NDSS, vol. 14. 2014, pp. 23_26.

[8] X. Chen, J. Li, J. Weng, J. Ma, and W. Lou, ``Veri_able computation over large database with incremental updates," IEEE Trans. Comput., vol. 65, no. 10, pp. 3184_3195, Oct. 2016.

[9] X. Chen, X. Huang, J. Li, J. Ma, W. Lou, and D. S. Wong, ``New algorithms for secure outsourcing of large-scale systems of linear equations," IEEE Trans. Inf. Forensics Security, vol. 10, no. 1, pp. 69_78, Jan. 2015.

[10] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, ``Searchable symmetric encryption: Improved de_nitions and ef_cient constructions," J. Comput. Secur., vol. 19, no. 5, pp. 895_934, Jan. 2011.