RESEARCH ARTICLE OPEN ACCESS

Provable data possession for securing the data from untrusted server

1st S.Karthikeyan , 2nd J.praveen And 3rd Author Mrs Sumathy
Department Of Information Technology From Jeppiaar Engineering College

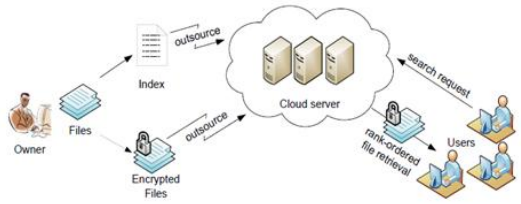
ABSTRACT:
The model described for the use of Provable data Possession which allow the client to access the stored data at an Untrusted server that the server possesses the original data without retrieving it. This model executes the probabilistic proof of possession by random set of blocks which is derived from the server that dramatically reduces the cost of I/O. Sometimes the Client maintenance the constant amount of data which is used to verify the proof. The response protocol can transmit a small amount of data, which can minimize network communication. The two provably –Securer PDP Schemes presents more efficient schemes than previous solution .Even when compared with schemes that achieve weaker guarantees. It is the widely distributed storage systems. Using the experiment we can implement and verify the practicality of PDP and we can revel that the performance of the PDP that is bounded by disk I/O and that cannot be determined by computation.

I. INTRODUCTION:

The authenticity of data can be emerged as a critical issue while storing data on the untrusted servers. The data can move from peer-to-peer storage systems, network file system, web-service object stores, and database systems. These kinds of systems prevents storage servers from mixed kind of representation and modifying data by analysing and providing authenticity to check when accessing the data.The archiveal storage requires many guarantees about the authenticity of data during the process of storage . During the process of accessing the data it is insufficient to detect and modify the data. Due to the storage ,the server retains tremendous amount of data, in which little can be accessed. Data can be held long period of time during which there may be exposure to data loss from administration errors as the physical implementation of storage evolves. Archival network storage presents unique performance demands. Futhermost I/O solution is used to establish the data possession interface with on-demand bandwidth to store and retrieve data. They conclude that the client need to be able to verify that a server access the entire file. These requirements is not present in the previous solutions. Few schemes provide a weaker guarantees by enforcing storage complexity. Than the client data the server has to store a large amount of data , but it is not necessary to have the same exact data . While handling the client with large number of data it is not required to have entire file, than the server.Define the model for provable data possession(PDP) that provides probabilistic proof that a third party can store a file. The model is unique in that it allow the server to acces small portions of the file int generating the proof; The challenge and the response are each slightly more than 1 Kilbit. Both schemes use homorophics verifiable tags. At a later time, the client can verify that server posseses the file by generating a random challenge against a randomly selected set of the blocks. The server can generate the proof of possession by using the queried blocks and their corresponding tags. Thus the client convinced of data possession without actually having to retrieve the blocks.

Efficient PDP schemes is used as the fundamental construct underlying an archival introspection system that we are developing for the long term preservation of data. In multiple sites the database can be replicated. The location and physical implementation can replices are managed indenpendlty by the use of each partner and will evolve over time. Efficient PDP schemes will make sure that the calculation of each reqirements of remote data checking that donot unduly burden the remote storing sites. Parters may even outsource storage to third-party storage server providers. Efficient PDP schemes will make sure the requirements of remote data checking do not undergo. The implementation that have more efficient schemes (E-PDP) and two other remote data checking protocols and evaluated their performance.

NOTE: A version of the preceedings of CCS 2007 that contained an error in the security proof: We made an assumption which does not hold when the parameter . This can allow anyone not just owner, to challenge the server for data possession.



PROCEDURE OR TECHNIQUES:

I Provable Data Possession (PDP):

We framework the provable data possession . The client C process the file that contains the collection of n blocks. These performance can make a goals, our PDP schemes sample the server's storage, accessing a random subset of blocks. The another way of application in PDP schemes is in the context of the resistance. There are many use of cause where duly authorized the third party that may need to say and modify a documents in some kind of controlled and limited way. The problem is to prevent the unauthorized modifications is by the technique or schemes known as homomorphic tags. Because of the homomorphic property, tags computed for multiple file blocks that can be combined into a single value. At larger time, the client can verify that the possess the file by generating a random challenge against a randomly selected set of the blocks. In some cases, there are few well-known solutions. A PDP can be able to act as a deterrent to cheat thus to increase the trust in the system and helping spread its popularity and usage. The require data replications on-demand computation of a function over the entire outsourced data. The efficient PDP is a fundamental schema which undergoes an archival introspection that develops a long-term preservation part of the astronomy data. The database is used to replicate at multiple sites. Those sites includes many resourse sharing partner that can exchange the storage capacity to achieve reliability and scale. The replicates physical and locational implementation can manage independently by each partner and that will be useful to evolve over time. The storage resourse can be moved to the third-party server provider by the partners. Efficient PDP schemes will make sure that the requirements of remote data checking do not unduly burder the remote storage sites. The performance of Efficient PDP and other two remote data checking protocols will be implemented. Experiments shows that probabilistic possession guarantees to verify possession of large data sets. Though the PDP is difficult to encrypt and decrypt. The updated version of PDP is derived as CDPD.

PROPOSED PDP SCHEME:

We can describe and explain the proposed scheme.

II Threat model:

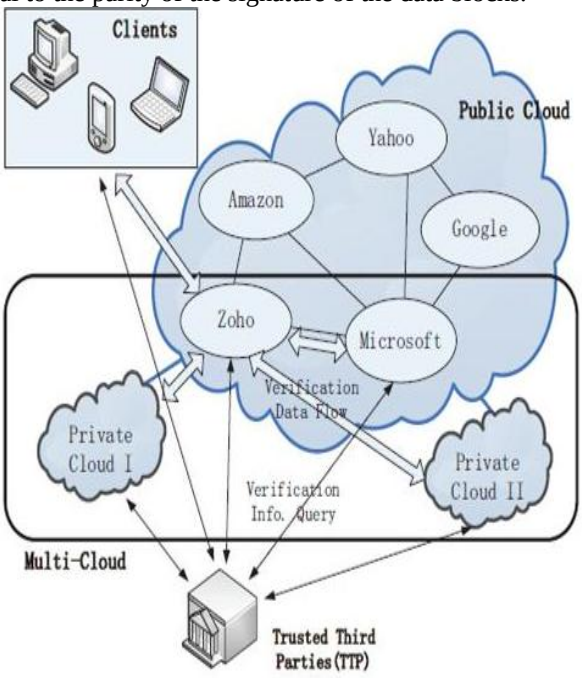
The failure to do so represents a data loss. The sever is not trusted. The misbehaviour of the storage can be discardiged the data which cannot been or rarely accessed and hided a data loss incident.

III Requirements and parameter:

The features of the parameters of a scheme may have

- Computation complexity
- Block access complexity
- Communication complexity

The amount of computation and block access at the server is to be maintained. The bandwidth efficiency should be minimized. The complexity at the client is of less importance. The goals of pdp schemes sample the storage accessing the subset of the blocks. In fact as a special case of our pdp scheme the client will update the proof of the file. The client may detect server misbehaviour with high probability by asking proof for a certain amount of blocks.Based on the property that the signature of the parity block that is equal to the parity of the signature of the data blocks.



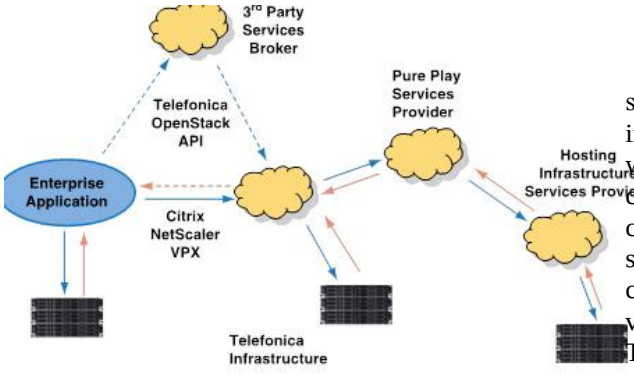
to print the TIFF files to make sure nothing was lost in the conversion.

IV Security Analysis:

We follow the security definitions in the form of a security game. It is our duty to prove that our prototype is a type of proof of knowledge of he quired blocks, i.e. , if the adversary passes the verification phase then we can extract the queried blocks. The Homomorphic hash function have been used in source which is used for authentication. The Homomorphic

can be used to compose a multiple blocks into a single value. This protocol is used only to compose the subset of the blocks that is based on the erasing coding. The provable data possession is not capable for the source authentication technique. The PDP can be enforcement is complexity for the storage , which shows that a server retains an enlarge amount of information as the file received from the client. The server is not necessary to retain the original file. Based on the new assumption the storage purpose is much complex. The schemes involves many consideration which access the parties and provide two additional features that can be used for the commitiment for the schemes.The main use of the PDP and the function of the PDP is implemented by the use of the hash function.The scheme does not required additional storage in the server and if the data in the client has very low entorphy then the client need to keep the low amount of state being used. This means that the server file access is very linear and is the complex storage during the prosess of the data. PDP is restricted form of the memory checking in that memory checking verifies every read and write process at every program . which can be utilized. Due to many restriction the checking of memory is more difficult and it cannot be determined significantly. Although the process is comparable in the scope the PDP, and their POR schemes can only be applied to encrypt files and that can handle only a limited number of queries which has to fixed a prior. The another way to check the remote storage is to make data resistant undetectable deletion through the use of enlargement Which is used to encode data and to create dependencies among the storage system. Thus deleting any data can able to delete the other unrelated data throughtout the system.

I. HELPFUL



V Proof sketch:

We are assuming that technical method is an ideal authenticated encryption. This implies that the given method is adversary and cannot be seen or alter, thus we can assume that it is stored directly by the challenger i.e., there is no need for the adversary to send it to the challenger and we can remove use of this method

More formally, our game is equivalent to the following:

- A simulator S sets up a PDP system and chooses its security parameters.
- The adversary selects values and sends them to the simulator
- The adversary can query the random oracle at any point in time. For each input to the random oracle the simulator replies with a random value and stores the input and corresponding output in the table.
- At the challenge phase the simulator challenges A on the value and sends a random value .A replies with a string .

II. THE IMPLEMENTATION AND PERFORMANCE FRAMEWORK:

We measure the performance of E-PDP is used to benefit the sampling based on our implementation of E-PDP in linux. All implementation were conducted on intel. Many algorithm uses the cpryto library openSSL.

- The PDP schemes allow the server to prove the possession block. This can be done by sampling , the ability is greatly reduces the server workload . The server misbehaviour can be still achieved by the detection method. The probabilistic guarantees which offer by a scheme that supports block sampling can be analyzed .The discrete random variable that is defined to be the probability of the server misbehaviour detection.

III. CONCLUSION:

The problem of verifying the untrusted server stores a client's data. In order to tackle this we introduced a model for provable data possession, which is used to minimize the file block accesses, the computation on the server, and the client's server communication. They incur a low overhead at the server and require a small,constant amount of communication per challenge. The Homomorphic veriflable tags are the key components of our schemes. They allow to verify possession of data in large data sets. In previous scheme when is PDP is used to prove possession in large amount of data, the sampling is not practical.

CONCLUSION:

The problem of verifying the untrusted server stores a client's data. In order to tackle this we introduced a model for provable data possession,

which is used to minimize the file block accesses, the computation on the server, and the client's server communication. They incur a low overhead at the server and require a small,constant amount of communication per challenge. The Homomorphic veriflable tags are the key components of our schemes. They allow to verify possession of data in large data sets. In previous scheme when is PDP is used to prove possession in large amount of data,the sampling method is not allowed and it is not practical . Our experiment shows that such schemes also impose a significant I/O and computational burder on the server.

References

[1] M. Abe and S. Fehr. Perfect NIZK with adaptive soundness. In Proc. of Theory of Cryptography Conference (TCC '07), 2007. Full version available on Cryptology ePrint Archive, Report 2006/423.

[2] J. Aspnes, J. Feigenbaum, A. Yampolskiy, and S. Zhong. Towards a theory of data entanglement. In Proc. of Euro. Symp. on Research in Computer Security, 2004.

[3] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song. Provable data possession at untrusted stores. In Proc. of the 14th ACM Conference on Computer and Communications Security (CCS '07). ACM Press, October 2007.

[4] M. Bellare, J. Garay, and T. Rabin. Fast batch verification for modular exponentiation and digital signatures. In Proc. of EUROCRYPT '98, LNCS, pages 236–250, 1998.

[5] M. Bellare and O. Goldreich. On defining proofs of knowledge. In Proc. of CRYPTO '92, volume 740 of LNCS, pages 390–420, 1992.

[6] M. Bellare and A. Palacio. The knowledge-of-exponent assumptions and 3-round zero-knowledge protocols. In Proc. of CRYPTO '04, Lecture Notes in Computer Science, pages 273–289. Springer, 2004.

[7] M. Bellare and A. Palacio. Towards plaintext-aware public-key encryption without random oracles. In Proc. of ASIACRYPT '04, volume 3329 of LNCS, pages 48–62. Springer, 2004.

[8] M. Bellare and P. Rogaway. Random oracles are practical: A paradigm for designing efficient protocols. In First Conference on Computer and Communications Security, pages 62–73. ACM, 1993.

[9] M. Bellare and P. Rogaway. The exact security of digital techniques for searches

[10] I. Clarke, O. Sandberg, B. Wiley, and T. W. Hong. Freenet: a distributed anonymous information storage and retrieval system. In International workshop on Designing privacy enhancing technologies, pages 46–66, New York, NY, USA, 2001. Springer-Verlag New York, Inc.

[11] B. Cooper and H. Garcia-Molina. Peer-to-peer data trading to preserve informatilon. ACM ToIS, 20(2):133–170, 2002.