Available online at www.ijiere.com
International Journal of Innovative and Emerging Research in Engineering
e-ISSN: 2394 - 3343 p-ISSN: 2394 - 5494

Efficient key Generation Algorithm in PDP (PROVABLE DATA POSESION)

KINJAL PATNI
CHOKHANDI CHAMPAGALI ANSH COMPLEX, VADODARA AND 390017,INDIA

ABSTRACT:
Recently, data outsourcing is in trend because of high data generation growth. People are using Remote Data Storage System to use their data remotely anywhere any time via internet. While accessing data via internet and outsourcing data on online storage, client should think about various issues like network bandwidth, Data integrity, Availability of data. Out of this issue we are focusing on "Provable Data Possession". It is related to integrity of outsourced data of user. To check integrity of outsourced data, in many literatures different PDP schema are proposed. But they have some limitation regarding key generation and few others as mentioned in our work. So we have focused on improved and efficient key generation in PDP schema. We have developed such PDP scheme which reduce the overhead on user's side with limited computation resources and efficient generate secure key for our PDP schema.

Keywords: Provable Data Possession, Phase of PDP, RSA, version RSA,Dual-RSA

I. INTRODUCTION

We are living in the Informational world. We need to keep Information about every aspect of our lives. In other words, Information is an asset that has a value like any other asset. As assets, Information needs to be secured from attacks. So when talk about the term Information Security, we need to secure our data which are stored in local disk or on remote data storage server. No matter where we store our data, but main three goals of Information Security should be fulfilled. Three main goals are:

- Confidentiality
- Integrity
- Availability

As per above mentioned three goals, to be secured, information needs to be hidden from unauthorized access (CONFIDENTIALITY), protected from unauthorized change (INTEGRITY), and available to an authorize entity when it is needed (AVAILABILTY).

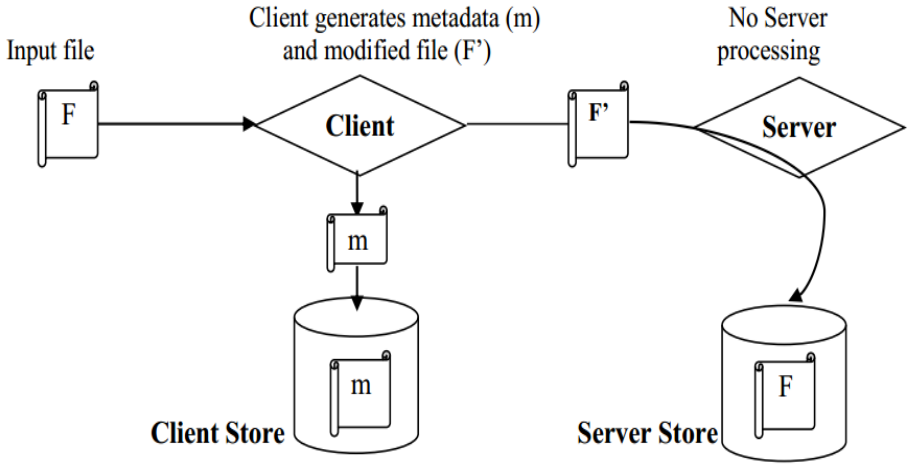
Before few years, local disk was in trend. The term local disk refers to physical disk in which user can store the data, and they know that his data is stored in that disk. But size of local disk is bounded with some limitations, like limited storage, no remote access of those data which are reside in those local disk which configured in different type of computer. There are many portable storage devices are also available to carry our data with us when and wherever we move all time to access our data at any time. Some devices do not allow accessing those portable devices.

II. PROVABLE DATA POSSESSION

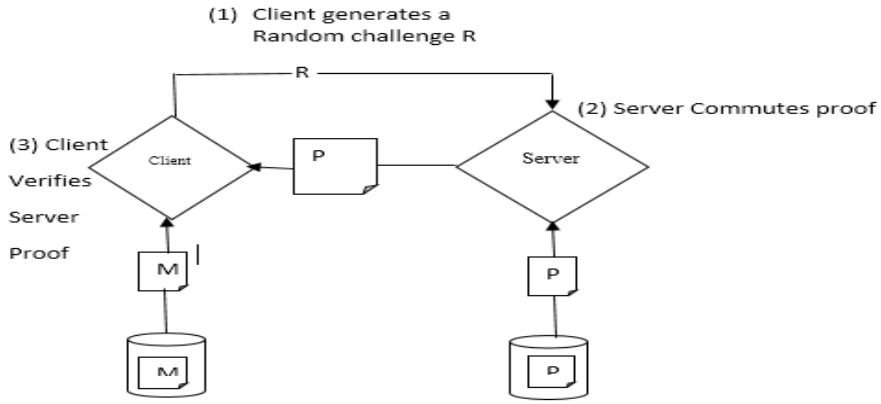
Remote data storage service has become a faster profit grow the point by providing a comparably low-cost, scalable, position-independent platform for client's data. But the main issue is how to frequently, efficiently and securely verify the storage server is faithfully storing its client's (potentially very large) outsourced data. The storage server is assumed to be unstructured in terms of both security and reliability. Provable Data Possession is a technique for ensuring the integrity of data in outsourcing storage device. It allows a client that has stored data at entrusted server to verify that the server possesses the original data without retrieving it. PDP 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 in widely-distributed storage system.

In PDP Model Generally two entities are involved: Client and Server. Sometimes Trusted third party and it or is also involved in PDP model. While only Client and Server are involved then generalized main two tasks are described below;

1. Pre-Processing at client side and upload the data on storage server.
2. Verify server possession.



(a) Pre-Process and Store [1]



(b)Verify Server Possession [1]

III. PHASES OF PDP

Generally, PDP Model is made up with basic five steps, which are as follow:

1. Setup
2. TagGen
3. Challenge
4. GenProof
5. CheckProof

1) Setup ⟶ (pk, sk) This function generates the public key pk and the secret key pk is public sk. to everyone, while sk is kept secret by the client.

Input: (e; ne; n) such that ne < n/2

- Randomly select an ne-bit integer x1 and an (n/2 – ne)- bit integer x2 such that p1=x1x2+1 is prime.
- Randomly select an (n/2-ne)-bit integer y2 such that p2=x1y2+1 is prime.
- Randomly select an ne-bit integer y1 such that q1= y1y2 + 1 is prime.
- Randomly select an n-bit integer e such that gcd (x1, x2, y1, y2, e) =1. Compute d and k1 satisfying ed = 1+k1(p1 – 1) (q1–1).
- If q2=k1x2 + 1 is not prime, then go back to step 4.
- Let N1 = p1q1; N2 = p2q2, and k2= y1.

Output: (e; N1; N2) and (d; p1; q1; p2; q2)

2**) TagGen (pk,sk,m) ⟶ Dm**

For each file block mi,i ε [1,n], the client computes the block tag as

$$D_i = (g^{m_i})^d \bmod N_1 \bmod N_2$$

3) **Challenge(pk,Dm) ⟶ Chal**

In order to verify the integrity of the file m, the verifier generates a random key r and a random group elements s ε ZN_1\ {0}. The verifier then computers $gs=_g{}^s$ mod N and sends chal= <r , gs> to the server.

4) **GenProof(pk,Dm,m,chal)** ⟶ **R**

When the server receives chal = <r,gs>, it generates a sequence of block indexes a1,a2,…., an by calling f(i) for i ε [1,n] iteratively. Then the server computes and sends R to the verifier.

$$R= g_s \ \sum_{i=0}^{n} ai\ mi \ \text{mod N1 mod N2}$$

5) **CheckProof(pk,Dm,chal,R)** ⟶ {"success", "failure"}

When the verifier receives R from the server, she computes $\{a_i\}$ i=1,…,n as the server does in the GenProof step. Then the verifier computes P ans R' as follows :

$$P= ((\pi^{n}{}_{I=1} D_I{}^{ai} \text{ mod N1})) \text{ mod N2}) \text{ mod N1 mod N2}$$

$$R'= P^s \text{ mod N1 mod N2}$$

After that the verifier checks whater R' = R. output "success". Otherwise the verification fails and the verifiers output " Failure".

IV. CONCLUSIONS

There are different types of PDP with its parameters like: data dynamics, key generation, sampling, tpa, public verifiability etc. in key generation, PDP is using RSA algorithm. There found some limitations in RSA named as factoring a large number and strength of keys. Variant of RSA algorithm like RSA small-d, RSA small-e, dual RSA from this algorithm dual RSA can take less response time and more security compare to RSA. So, I would like to improve setup phase of PDP in terms of strength of public and secret key and time required to generate these keys.

ACKNOWLEDGMENT

This work was partly supported by: The IEEE through National Science Council, Taiwan, under contract NSC 95-2221-E-007-030, CCS'07, *IEEE Transactions* on 53.8 (2007): 2922-2933. We thank Zhuo Hao, Sheng Zhong, Nenghai Yu, Ateniese, Giuseppe.

REFERENCES

[1] Ateniese, Giuseppe, et al. "Provable data possession at untrusted stores." Proceedings of the 14th ACM conference on Computer and communications security. Acm, 2007.
[2] Ateniese, Giuseppe, et al. "Scalable and efficient provable data possession." Proceedings of the 4th international conference on Security and privacy in communication networks. ACM, 2008.
[3] Cryptography and Network Security Williyam Stalling
[4] Hao, Zhuo, Sheng Zhong, and Nenghai Yu. "A privacy-preserving remote data integrity checking protocol with data dynamics and public verifiability." Knowledge and Data Engineering, IEEE transactions on 23.9 (2011): 1432-1437.
[5] Sebé, Francesc, et al. "Efficient remote data possession checking in critical information infrastructures." Knowledge and Data Engineering, IEEE Transactions on 20.8 (2008): 1034-1038.
[6] Sun, Hung-Min, et al. "Efficient provable data possession with the public verifiability and data privacy" Center of computer and information security research, Springer on ACISP 2015.
[7] X. Yu and Q. Wen, "A Multi-Function Provable Data Possession Scheme in Cloud Computing," no. 2012, pp. 1–19.
[8] Zhu, Yan, et al. "Efficient provable data possession for hybrid clouds." Proceedings of the 17th ACM conference on Computer and communications security. ACM, 2010.
[9] Cryptography and Network Security Forouzan.
[10] Sun, Hung-Min, et al. "Dual RSA and its security analysis." *Information Theory, IEEE Transactions* on 53.8 (2007): 2922-2933.