ISSN : 2231-0711
V. V. Jog et al | International Journal of Computer Science Engineering and Technology(IJCSET) | Dec 2014 | Vol 4, Issue 12,392-394

Security of outsourced data in cloud using Dynamic Auditing

V. V. Jog[1] , Deepali Pande[2]
[1] *Professor, Computer Engineering Department, SKNCOE, Pune, India*
[2]*M. E. Computer Engineering Department, SKNCOE, Pune, India*

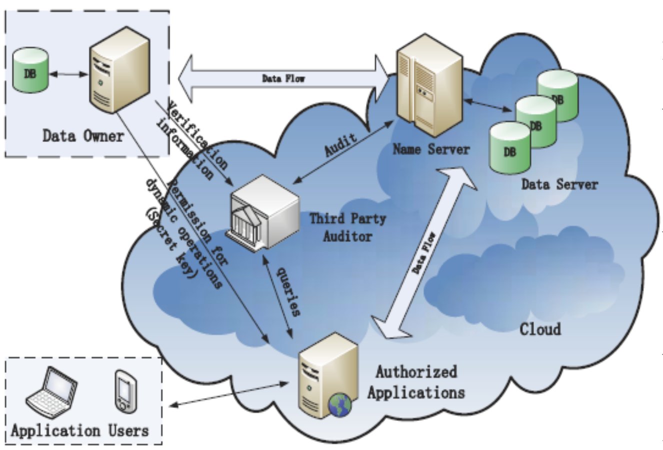
Abstract-Now a days Cloud is the term which is involved in every aspect of our life . It provides a environment called as scalable environment to store large amount of data and their related processes. It provides a low cost service called as outsource storage and is also independent of platform. Though it provides high data storage but there is always a problem of security of data stored in cloud. In this system we are proposing a system which is capable enough to solve cloud storage security problem. It verifies the integrity of cloud and the data which is outsourced. It also supports timely detection of anomaly and dynamic data operations.

Key terms: Retrivability, TPA, metadata

1. INTRODUCTION

In this era cloud computing is getting popular, as it provides large data storage and good access facilities but security issue is always a problem. In order to solve this problem a system is generated using dynamic auditing. Here we are trying to design a method to enhance the security of untrusted cloud , we are also designing a method which will maintain the integrity of file stored at public cloud.

2. PROGRAMMER'S DESIGN
3.



A. Mathematical Model Tag Generation

Let n=file size in bytes
b=size of block in bytes
Number of blocks(N_b)=n/b
m=Number of bytes in metadata per block where m<b
size of metadata=m* N_b

actual

$$\text{metadata}=\sum_{i=1}^{Nb}\ \sum_{j=i*m}^{j+m} filedata\,[i*j]$$

Sampling Audit

Block number B_n =random()%N_b

$$\text{Data}=\sum_{j=Bn*m}^{j+m} filedata\ [j]$$

$$\text{Metadata}=\sum_{i=n+Bn*m}^{i+m} metadat[i]$$

If data and metadata is equal then file is correct
Otherwise file is modified

Low order hybrid chaotic sequence tag generation:

Logistic Chaotic Map
$^{1}X_{n+1} = \lambda * X_{n} * (1-X_n)$
where X_n is between 0 and 1

Improved Logistic Map
$^{2}X_{n+1}=1-2*X_n^{2}$
where X_n is between -1 to 1

Chebyshev Chaotic Map
$^{3}X_{n+1} = \cos(5*\text{arc} \cos X_n)$
where X_n is between -1 and 1.

$X_{n+1} = ({}^{1}X_{n+1} + {}^{2}X_{n+1} + {}^{3}X_{n+1}) / 3;$
N_i=number of blocks in file F
where i=1 to N

ith key=> $K_i = N_i$ EXOR X_i
L_i = number of random bytes from i^{th} block
R_i = actual random byes selected from i^{th} block (size is L)
Metadata of $R_i = R_{ij}$ XOR K_i where j is between 0 to L-1

Adversary may try to break metadata in order to modify file and fool the TPA.
If adversary able to crack metadata then TPA will get false negative results.

- To break this matadata attacker has to find X_0 and λ.
- X_0 is between 0 and 1 and gap is 0.000001;

- λ is between -4 and 4 and gap is 0.000001
- Number of possiblilites=$10^6 * 8 * 10^6 = 8 * 10^{12}$
- Probability of finding $X_0 = P_x = 1/10^6$
- Probability of finding $\lambda = P_\lambda = 1/(8 * 10^6)$
- Probability of detecting matadata=$P_{detect} = P_x * P_\lambda = 1/10^6 * 1/(8 * 10^6) = 1.25 * 10^{-13}$

B. Metadata/Tag Generation Algorithm

1) User uploads the file to CSS. In background file will be transferred to TPA.
2) TPA encrypt the file by using AES algorithm. Stores secret key into it's database.
3) TPA generates metadata of the file in order to achieve data integrity. To generate metadata following steps are carried out:
    1) Split encrypted file into N blocks each of size M.
    2) Select random L bytes as metadata from each block.
    3) Apply encoding on each L bytes by using proposed chaotic based low overhead encoding.
    4) Generate metadata of size N*L bytes and append to file.
    5) TPA stores start and end position of L bytes of each block.
6) TPA also stores encoding key.
7) TPA transfers encrypted file along with encoded metadata to CSS.
8) TPA deletes encrypted file and metadata.

C. Data Verification Algorithm

TPA does periodic sampling audit of CSS.

1) TPA queries random block's random L bytes(start and end position is stored at TPA database) and corresponding metadata to CSS.
2) CSS will give corresponding response to TPA.
3) TPA decodes metadata by using decoding key and compares random L bytes with corresponding metadata.
4) If math found data is not tampered by adversary.
5) If match is not found it means that data is modified by adversary and TPA will inform corrosponding user by sending mail.

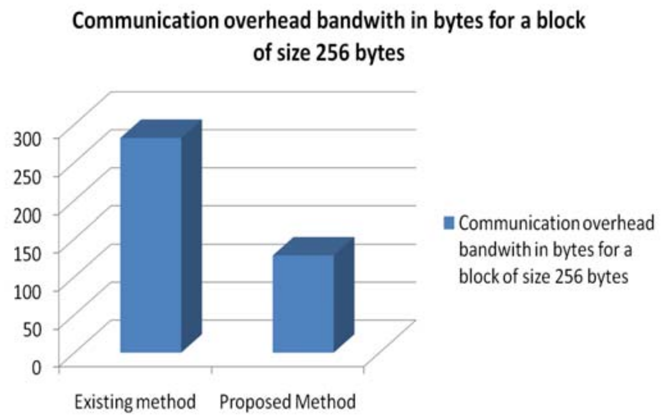
4. Expected Results of proposed System

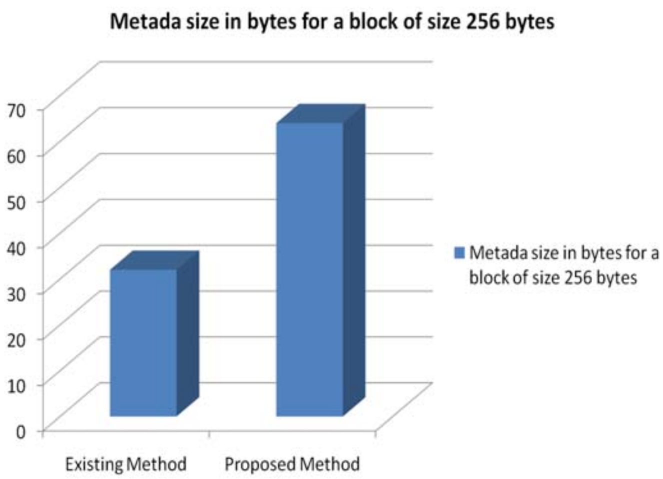
- Existing system is having lower metadata size as compared to proposed system.
  L=number of random bytes selected from a block for metadata
  Therefore, size of metadata=N*L where N is number of blocks
  N=number of blocks

- Computation overhead of proposed system is less as compare to existing system.
  N_i=number of blocks in file F
  where i=1 to N
  ith key=> $K_i = N_i$ EXOR X_i
  L_i = number of random bytes from i^{th} block
  R_i = actual random byes selected from i^{th} block (size is L)
  Metadata of $R_i = R_{ij}$ XOR K_i where j is between 0 to L-1

- Communication bandwidth required for CSS audit by TPA is less as compare to existing system.
  Communication Bandwidth of proposed system $= 2 * R_i$
  Communication Bandwidth of existing system = M =size of entire block

5. Graphs





6. Conclusion and Future Work

- Computation complexity of proposed algorithm is less than existing hash based algorithms.
- Communication bandwidth required for auditing by TPA is less as compare to existing method.
- Metadata size of the proposed method is larger. But it is more secure. Because proposed Low order hybrid chaotic sequence tag generation method is applied. Mathematical analysis proves that proposed method is very difficult to crack.
- Proposed tag generation algorith is having low overhead than existing hash based algorithms.

ACKNOWLEDGMENT

The authors would like to express heartfelt gratitude towards the people whose help was very useful to complete this dissertation work on the topic of "**Security of outsourced data in cloud using Dynamic Auditing**" It is great privilege to express sincerest regards to P.G. Guide Prof V. V. Jog and, for her valuable inputs, able guidance, encouragement, whole-hearted cooperation and constructive criticism throughout the duration of this work. Also thanks to H.O.D. P. N. Mahalle for his valuable inputs and whole-hearted. Author is also thankful to Principal A. V. Deshpande and the management. She would also like to thank all the faculties who have cleared all the major concepts that were involved in the un

REFERENCES

[1] A. Juels and B.S. Kaliski Jr., "PORs: Proofs of Retrievability for Large Files," Proc. ACM Conf. Computer and Communications Security (CCS '07), pp. 584-597, 2007.

[2] M. Mowbray, "The Fog over the Grimpen Mire: Cloud Computing and the Law," Technical Report HPL-2009-99, HP Lab., 2009.

[3] A.A. Yavuz and P. Ning, "BAF: An Efficient Publicly Verifiable Secure Audit Logging Scheme for Distributed Systems," Proc. Ann. Computer Security Applications Conf. (ACSAC), pp. 219-228, 2009.

[4] G. Ateniese, R.C. Burns, R. Curtmola, J. Herring, L. Kissner, Z.N.J. Peterson,and D.X. Song, "Provable Data Possession at Untrusted Stores," Proc. 14th ACM Conf. Computer and Comm. Security, pp. 598-609, 2007.

[5] C.C. Erway, A. Kupcu C. Papamanthou, and R. Tamassia, "Dynamic Provable Data Possession," Proc. 16th ACM Conf. Computer and Comm. Security, pp. 213-222, 2009.

[6] H. Shacham and B. Waters, "Compact Proofs of Retrievability,"Proc. 14th Int'l Conf. Theory and Application of Cryptology and Information Security: Advances in Cryptology *Advances in Cryptology (ASIACRYPT '08), J. Pieprzyk, ed., pp. 90-107, 2008.*

[7] H.-C. Hsiao, Y.-H. Lin, A. Studer, C. Studer, K.-H. Wang, H.Kikuchi, A. Perrig, H.-M. Sun, and B.-Y. Yang, "A Study of User-Friendly Hash Comparison Schemes," Proc. Ann. Computer Security Applications Conf. (ACSAC), pp. 105-114, 2009.

[8] A.R. Yumerefendi and J.S. Chase, "Strong Accountability for Network Storage," Proc. Sixth USENIX Conf. File and Storage Technologies (FAST), pp. 77-92, 2007.

[9] M. Xie, H. Wang, J. Yin, and X. Meng, "Integrity Auditing of Outsourced Data," Proc. 33rd Int'l Conf. Very Large Databases (VLDB), pp. 782-793, 2007.

[10] Guangxian Xu, Xiao Fu and Wei Wu ," Low-overhead Secure Network Coding based on Chaotic Sequence " Appl. Math. Inf. Sci. 7, No. 2L, 605-610 *(2013)*