International Journal of Contemporary Research in Computer Science and Technology (IJCRCST) ISSN: 2395-5325
Volume 3, Special Issue 2 (March '2017)
Proceeding of - National Conference on Recent Trends in Information Technology and Communication,
Conference held at Velammal Engineering College,Chennai,India.

CLOUD STORAGE SERVICE USING OPTIMIZED KEY AUDITING

C.M.Nalayini,
Assistant Professor,
Department of Information Technology,
Velammal Engineering College,
Chennai,India.

Lavanya K,
UG Students,
Department of Information Technology,
Velammal Engineering College,
Chennai,India.

Saji Reshma,
UG Students,
Department of Information Technology,
Velammal Engineering College,
Chennai,India.

Abstract: In electronic life, many organizations suffering from the problem of processing huge amount of data within a elapsed time. Cloud computing is based on remote servers. It provides on the internet to store the data, manage and process the data rather than a PC. Although cloud storage provides great benefit to users, it brings new security challenging problems. Once the client's secret key for storage auditing is exposed to cloud, the cloud is able to easily hide the data loss incidents for maintaining its reputation, even discard the client's data rarely accessed for saving the storage space. In our design, TPA(Third Party Authority) only needs to hold an encrypted version of the client's secret key whenever the client upload the new file into the cloud. The client wants to send and retrieve the data from using the client's encrypted secret key. The goal of this paper is to design a cloud storage to evaluate protocol that can satisfy above essential to reach the outsourcing of key updates.

Keywords: Cloud storage, Outsourcing computing, Cloud storage auditing, Key updates, Verifiability.

I.INTRODUCTION

Cloud storage is a model of data storage on which the remote servers accessed from the cloud. It is maintained and managed the data by using cloud storage service provider. It has been considered in many applications including scientific computations, linear algebraic computation model, linear programming and modular exponentiation computations, etc.

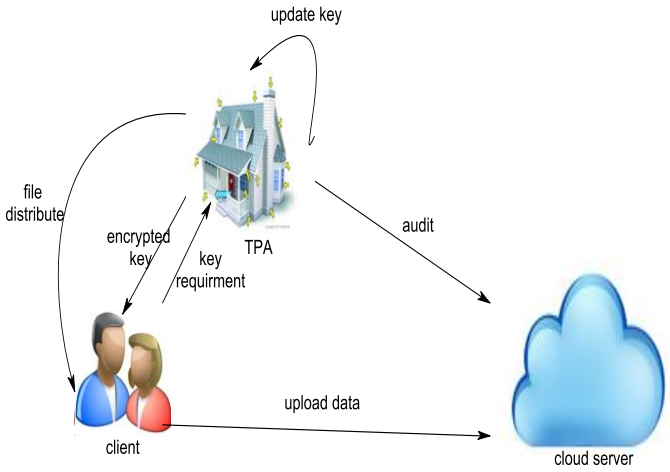
a) **Pay as you go:** An estimate model of cloud services is based on storage utilization model.

b) B.Private cloud:
This is a form of cloud computing platform that is implemented within the corporate firewall, under the control of the IT department.

c) Public cloud:
It is a form of cloud computing in which a company relies on at third-party cloud service provider for services such as servers, data storage and applications, which are delivered to the company through the internet.

d) Client Data Computing:
The client is the owner of the files that are uploaded to cloud. The total size of these files is not fixed, that is, the client can upload the growing files to cloud in different time points. The cloud stores the client's files and provides download service for the client.

e) Upload Data:
The client wants to upload new files to the cloud, it needs to verify the validity of the encrypted secret key from the TPA and recover the real secret key. These process happened in different time periods. In that time periods the client needs to upload new files to the cloud. Also, the work for verifying the correctness of the encrypted secret key can fully be done by the cloud.



f) Key Request:
The client sends the key requirement to the TPA only when he wants to upload new files to cloud. And then the TPA sends the encrypted secret key to the client. After that, the client decrypts it to get his real secret

key, generates authenticators for files, and uploads these files along with authenticators to cloud.

g) Auditing Proof:
TPA audits the secret key for the client's file when the client was upload the new file in the server. "Proof of retrievability" (PoR) was proposed to ensure both control and retrievability of data at untrusted servers. Also,TPA proposed a public privacy-preserving auditing protocol.

II.PROBLEM STATEMENT

The method for firm outsourcing of some scientific computations was proposed by Atallah. Chevallier-Mames designed the first effective algorithm for secure delegation of elliptic curve pairings based on an suspicious server. The first outsourcing algorithm for modular exponentiations, which was based on the methods of pre computation and server-aided computation. The first cloud storage auditing protocol based on in distinguish ability obscure, which is especially useful for low-power cloud users. Proposed a public auditing protocol for shared cloud data supporting both identity privacy and identity traceability. Any dishonest behaviors, such as deleting or modifying the client's data previously stored in cloud, can all be detected, even if the cloud gets the client's current secret key for cloud storage auditing. However, the client needs to update his secret key in each time period. One important security problem is how to efficiently check the integrity of the data stored in cloud. Auditing protocols focused on different aspects of cloud storage auditing such as high efficiency, protection of data, protection of identities and sharing of data, etc. Key Exposure is the second problem in cloud storage auditing. Cloud storage auditing protocol with key showing flexibility by updating the user's secret key periodically. It can be reduced by key exposure problem in cloud service auditing.

III.RELATED WORK

[1]. In this paper, the author suggests that the outsourcing secure framework for computations, costs, numerical properties and levels of security. These techniques can be embedded in a very high level, easy-to-use system that hides their complexity. But, the network cost increases at the various level.

[2]. In this paper, author uses proof-of-retrievability schemes with full proofs of privacy and protected in the strongest model. The implementation of BLS signatures and secure in the random oracle model, has the shortest question and response of any proof-of-retrievability with public verifiability. The pseudo-random function is firm in the standard model, has the shortest response of any proof-of-retrievability scheme with private verifiability.But it is a longer query.

[3]. Here the author uses a highly efficient and provable secure PDP(Provable Data Possession) technique based on symmetric key cryptography, while not requiring any bulk encryption. Also, in contrast with its predecessors, our PDP technique allows outsourcing of vigorous data, i.e., it efficiently supports operations, such as block modification, deletion and append.

[4]. In this paper, MR-PDP(Multiple Replica-Provable Data Possession) used to stored duplicate is computationally much more efficient than using a single-replica PDP scheme to store t separate, unrelated files (e.g., by encrypting each file separately advance to storing it). Another advantage of MR-PDP is that it can generate further replicas on demand, at little expense, when some of the existing duplicate fail.

[5]. Here, the author suggests a secure cloud storage system supporting privacy-preserving public auditing. Further extend our result to enable the TPA to perform audits for multiple users simultaneously and efficiently. Extensive security and performance study show the schemes are provable secure and highly efficient.

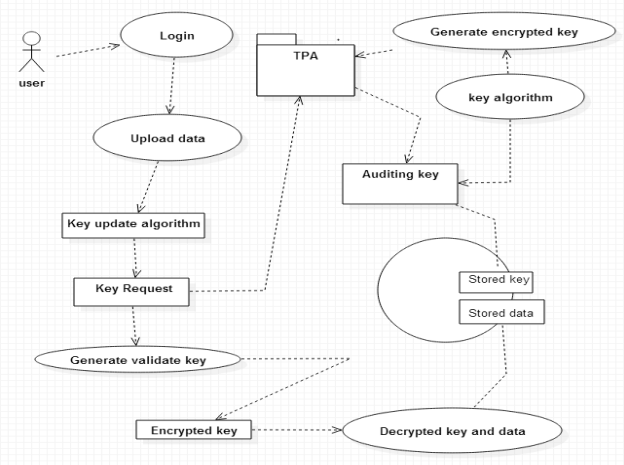
[6]. In this paper, the author presents a new remote data possession checking protocol It allows an unlimited number of file integrity verifications. The maximum running time can be chosen at set-up time and traded off against storage at the verifier.

[7]. In this paper, the author suggested a new implementation algorithm for secure outsourcing data in modular exponentiations. In the proposed algorithm, the modular exponentiations need to be computed are hidden to the malicious server. In the computation procedure, the server cannot obtain any information with respect to the input and output while the client can verify the returned result efficiently. In addition, the proposed algorithm can promote the efficiency of all security protocols based on discrete logarithm.

IV.PROPOSED WORK

We proposed a new model called cloud storage auditing with verifiable outsourcing of key updates. In this new model, key-update operations are not performed by the client, but by a third party. The third party holds an encrypted secret key of the client for cloud storage auditing and updates it under the encrypted state in each time period. The client accepted the encrypted secret key from the third party and decrypts it whenever the client was upload new files to cloud. In addition, the client can verify the validity of the encrypted secret key. In our design, the third party auditor (TPA) plays the role of the authorized party who is in charge of key updates. We formalize the definition and the security model of the cloud storage auditing protocol with verifiable outsourcing of key updates.

System model:



Secret Key Algorithm:

Cipher text generate:

```
C(bytein[4*b],byteout[4*b],word
w[b*(r+1)])
begin
byte state[4,b]
state = in
AddRoundKey(state, w[0, b-1])
for round = 1 step 1 to r–1
 SubBytes(state)
 ShiftRows(state)
 MixColumns(state)
 AddRoundKey(state, w[rd*b, (rd+1)*b-1])
 end for
 SubBytes(state)
 ShiftRows(state)
 AddRoundKey(state, w[r*b, (r+1)*b-1])
 out = state
 end
```

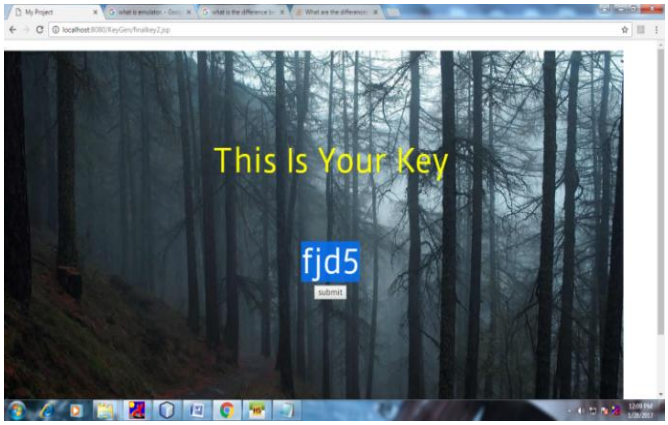
Key generate:

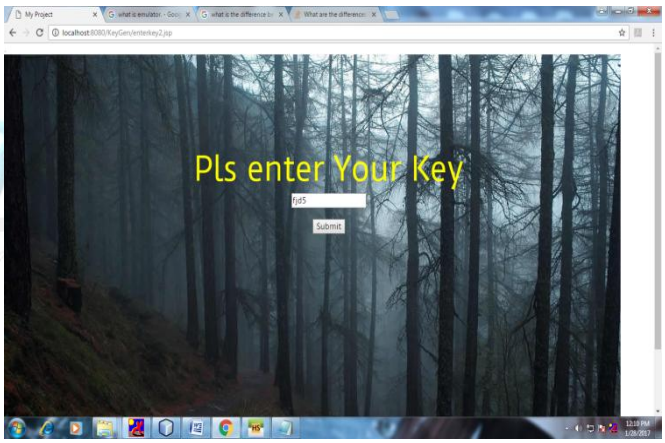
```
Key(byte key[4*k], word w[b*(r+1)], k)
Begin
word tem
l= 0
while (l < K)
w[l] = word(key[4*l], key[4*l+1], key[4*l+2], key[4*l+3])
l = l+1
end while
l=k;
while (l < b * (r+1)]
tem= w[l-1]
if (l mod K= 0)
tem=SubWord(RotWord(tem))xor Rcon[l/k]
else if (k > 6 and lmod k = 4)
tem = SubWord(tem)
end if w[l] = w[l-k] xor tem l = l+ 1
endwhile
end
```

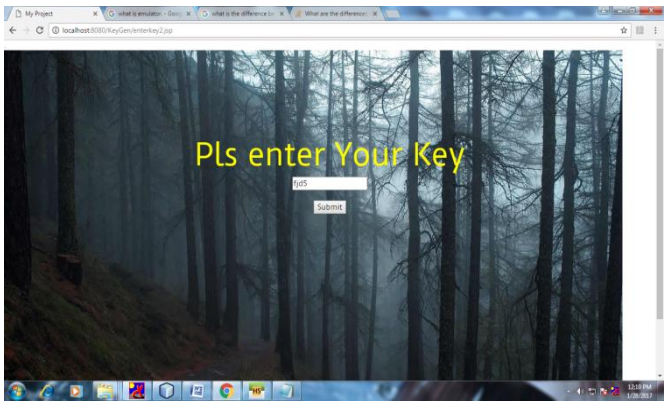
Cipher text inverse:

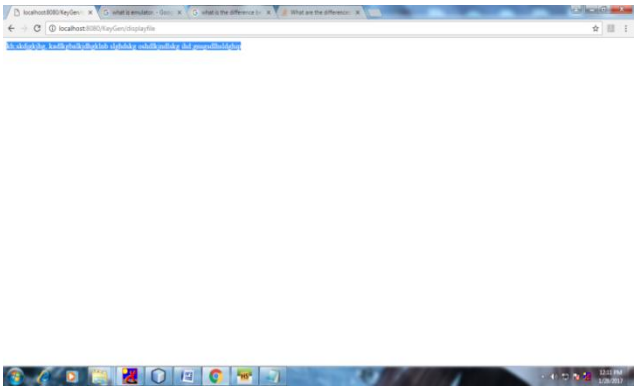
```
Eqciph(byte in[4*b], byte out[4*b], word w[b*(r+1)])
begin
byte state[4, b]
state = in
AddRoundKey(state, w[r*b, (r+1)* b-1])
for round = r-1 step -1 downto 1
InvSubBytes(state)
InvShiftRows(state)
InvMixColumns(state)
AddRoundKey(state,w[round*b, (round+1)*b-1])
end for
 InvSubBytes(state)
 InvShiftRows(state)
 AddRoundKey(state, w[0, b-1])
 out = state
  for l = 0 step 1 to (r+1)*b-1
 w[l] = w[l]
end for
for round = 1 step 1 to r-1
InvMixColumns(w[round*b, (round+1)*b-
1])
end for
```

V.Experimental Set up:









Advantages:

- Easy to updates key.
- When uploading the new files,the client's can easily verification for validity encrypted secret keys by using TPA.
- The key verification process with different number of checked data.

VI. CONCLUSION

In this paper, we study on how to outsource key updates for cloud storage examine with key-exposure resilience. We propose the first cloud storage examine protocol with verifiable outsourcing of key updates. In this protocol, key updates are outsourced to the TPA and are see through for the client. In addition, the TPA only sees the encrypted version of the client's secret key, while the user can further verify the validity of the encrypted secret keys when downloading them from the TPA. In future work,to update the current status of the auditing verification to the Client. Where the TPA can perform multiple auditing tasks in a batch manner for better efficiency. Extensive analysis shows that our schemes are provably secure and highly efficient.

VIII. REFERENCES

[1]. M. J. Atallah, K. N. Pantazopoulos, J. R. Rice, and E. E. Spafford, "Secure outsourcing of scientific computations," Adv. Comput., vol. 54, pp. 215–272, 2002.

[2]. H. Shacham and B. Waters, "Compact proofs of retrievability," in Advances in Cryptology. Berlin, Germany: Springer-Verlag, 2008, pp. 90–107.

[3]. G. Ateniese, R. Di Pietro, L. V. Mancini, and G. Tsudik, "Scalable and efficient provable data possession," in Proc. 4th Int. Conf. Secur. Privacy Commun. Netw., 2008, Art. ID 9.

[4]. R. Curtmola, O. Khan, R. Burns, and G. Ateniese, "MR-PDP: Multiplereplica provable data possession," in Proc. 28th IEEE Int. Conf. Distrib. Comput. Syst., Jun. 2008, pp. 411–420.

[5]. D. Benjamin and M. J. Atallah, "Private and cheating-free outsourcing of algebraic computations," in Proc. 6th Annu. Conf. Privacy, Secur. Trust, 2008, pp. 240–245.

[6]. F. Sebe, J. Domingo-Ferrer, A. Martinez-balleste, Y. Deswarte, and J. Quisquater, "Efficient remote data possession checking in critical information infrastructures," IEEE Trans. Knowl. Data Eng., vol. 20, no. 8, pp. 1034–1038, Aug. 2008.

[7]. X. Chen, J. Li, J. Ma, Q. Tang, and W. Lou, "New algorithms for secure outsourcing of modular exponentiations," in Proc. 17th Eur. Symp. Res. Comput. Secur., 2012, pp. 541–556.

[8]. G. Ateniese et al., "Provable data possession at untrusted stores," in Proc. 14th ACM Conf. Comput. Commun. Secur., 2007, pp. 598–609.

[9]. A. Juels and B. S. Kaliski, Jr., "PORs: Proofs of retrievability for large files," in Proc. 14th ACM Conf. Comput. Commun. Secur., 2007, pp. 584–597.

[10]. C. Wang, K. Ren, and J. Wang, "Secure and practical outsourcing of linear programming in cloud computing," in Proc. IEEE INFOCOM, Apr. 2011, pp. 820–828.