VOL. 10, NO. 11, JUNE 2015 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

SECURITY CONSERVATION BASED COMMON EVALUATION OF MUTUAL INFORMATION IN CLOUD COMPUTING

Lavanya M., Bhoomica C., Vishwapriya J. and Vaithiyanathan V.
School of Computing, Sastra University, Tamilnadu, India
E-Mail: m_lavanyass@ict.sastra.edu

ABSTRACT

Cloud technology is not only storage medium to store data but resources can also be shared across multiple users. But the integrity of information in cloud is subjected to doubtfulness due to the presence of hardware or software malfunctions and human faults. A number of mechanisms permit both data owners and public verifiers to effectively inspect cloud data correctness without downloading the whole information from the cloud server. The proposed paper introduces novel Token Based Ring System (TBRS) based Privacy-Preserving Technique which raises the security level of the information and supports hiding the identity privacy for group members and shared data stored in the cloud. We exploit enhanced ring signatures to preserve the identity of the signer. With this the identity of the signer on each block in shared data is kept private by utilizing tokens. We further extend the concept of ring signatures to support dynamic groups. Enhanced security and performance analysis prove that the proposed schemes are highly securable and efficient.

Keywords: cloud computing, security, ring signature, privacy preserve, dynamic group.

INTRODUCTION

Cloud computing is a new paradigm to share resources across multiple users. The process of dispensing is done by providing certain permission to the users. Cloud service providers offers a productive and cost-effective storage services compared to the traditional system. Several standard online storage services have been provided for enterprises which include Drop box, I Cloud and Google Drive. However the assurance and accuracy of data in cloud is subjected to doubtfulness because of the hardware/software malfunctions and human faults. The correctness of information stored in cloud should be verified before consuming it. This is done in traditional method by retrieving the whole information from the cloud and establishes data verification by examining the integrity of signatures of the complete information. However, this method is successful in verifying the integrity of data in cloud. But the effectiveness of performing this method on cloud is uncertain. The fact is that the size of information in cloud is huge. To overcome this challenge, the large file is divided into a number of blocks where each block is signed independently by different users of the group. A public verifier could render proficient integrity checking task. The user confidential information in the cloud is revealed to public verifier if conserving the identity privacy is failed. We utilize enhanced ring signatures to construct Token Based Ring System (TBRS) which improves the security of information stored in cloud. Compared to the existing ring signature mechanism, the proposed system referred as Ring Signature for Dynamic Groups (RSDG) which preserves the confidential data in cloud if an existing user leaves the ring.

RELATED WORKS

Number of related works is proposed for preserving identity and data privacy. Oruta, [1] is the initial privacy conserving mechanism that permits public evaluation on shared information. It helps in conserving the congruence of the signer on each block who is kept secret from a Third Party Auditor (TPA). This mechanism engages ring signature to compute authentication metadata required to audit the accuracy and assurance of data in cloud. Ring signature idea was initially initiated by Rivest, A. Shamir *et al.* [2]. With this mechanism, a verifier is satisfied that a signature is accessed by utilizing one of the group member's private key.

Provable Data Possession (PDP) is the first idea that permits a client to determine the integrity of data stored inside cloud which is put forward by Ateniese, R. Burns *et al.* [3]. With use of RSA dependent homomorphism authenticators, the auditor is capable of publicly verifying the integrity of information without retrieving the whole data. Auditing the accuracy of dynamic information is not satisfied.

Similarly another idea called as Proofs of Retrivalability (POR) was defined by Juels and Kaliski [4] which is designed to examine the rightness of shared data. It is proposed for large files using *sentinels* and can be done by using keyed hash function Hash (F). Single key is used regardless of the dimension of the file. Accurate verification of data is done by verifier who confronts the cloud by describing the spot of a group of sentinels and quering the cloud to give back the related sentinel values. But it requires higher resource costs for implementation.

Two improved POR schemes are designed by Shacham and Waters [5]. The foremost method is designed for BLS signatures and the subsequent method is based on pseudorandom function. In order to assist

dynamic operations on data Ateniese *et al.* [3] presented a coherent PDP mechanism build on symmetric keys. This mechanism supports delete and update operations but insert operation is not possible. It is because insert operation use symmetric keys to verify the integrity of data.

D. Boneh *et al.* [7] signature scheme uses bilinear pairing for verification and allows a user to verify that a signer is rightful. Signer rightfulness is verified by checking the signature of the signer which is collection of components in an elliptic curve. This signature scheme is provably secure and these signatures are referred to as short signatures.

In order to assist dynamic performance Wang *et al.* utilized Merkle Hash Tree and BLS signatures [6]. Dynamic Provable Data Possession (DPDP) is a scheme introduced by Erway *et al.* [8] by using authenticated dictionaries.

In order to minimize the repository of signatures in their public auditing mechanism, Zhu *et al.* [9] utilized the fragment structure. Index hash tables are added in addition to provide dynamic operations for users. To safeguard confidential user information from the TPA by deploying random masking a public mechanism was proposed by Wang *et al.* [10]. To assist diverse inspection of tasks from different users the mechanism is bestowed to enable batch auditing by leveraging aggregate signatures [11].

PROPOSED TECHNIQUE

Cloud computing provides many techniques to provide security to the information in cloud and hide the identity privacy of the user. To improve the existing environment we have introduced two schemes TBRS which raises the security level of the information and RSDG which supports hiding the identity privacy for group members The existing system utilizes ring signature concept where the user of the ring needs to sign in using his/her private key and group members public key in order to access a particular block of a file stored in cloud. This private and public key will be generated by the data owner of the ring and it is shared with the users of the ring and it is also stored in the cloud for verification. The private key is unique for every user in the ring and is said to be confidential. The users of the ring are predefined before storing the information in the cloud. The data owner of the particular ring is unknown to the public verifier. The authentication of the user is verified by the public verifier. When the user sign in using both the keys, the cloud service provider checks it with the keys stored in the cloud and then authenticates the user.

EXPLANATION OF THE ARCHITECTURE

Data owner predefines the number of users who can access the file before storing it in the cloud. Data owner splits a file into blocks and generates the private key for each user and block token id for each and every block and then stores it in the cloud with the help of cloud service provider. This private key, public key and block token id is distributed to the users in the ring. The users of the ring can access the file by giving their private key, public key and block token id as input

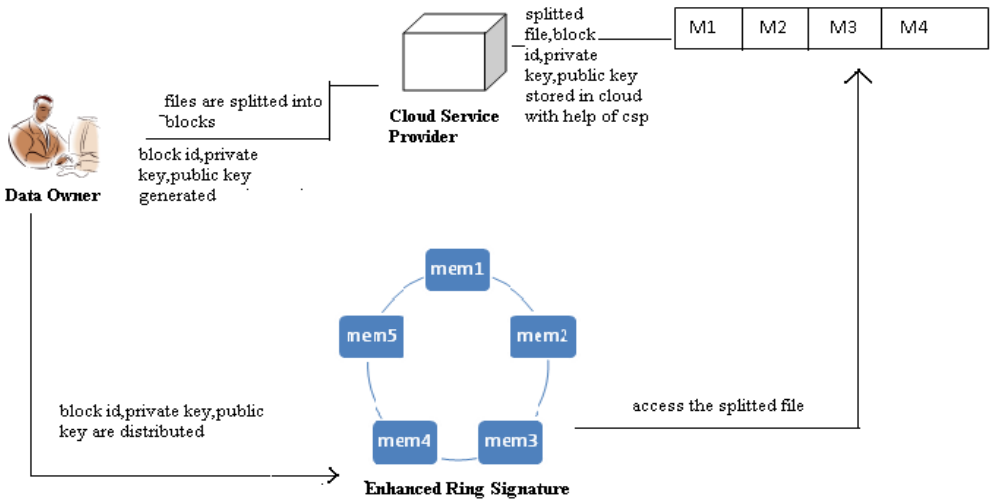

Figure-1. Ring based Architecture.

The proposed paper uses a technique referred as TBRS, increases the security level of information by introducing token id for each and every block of a file in cloud. When a user decides to access a particular block, the first step that need to be encountered is that he/she needs to sign in using his/her private key and group

members public key. Next token id for accessing the block needs to be given as input. After entering the block he/she can either perform read or modify operation. If the user performs a modification in the block then intimation is automatically send to the data owner indicating the modification. Then the data owner re-computes the token id for every block in the file and this new token is passed to every user of the group. Thus a new ring signature is recomputed. If a member of the group enters or exits the ring, he/she will multicast the message to the data owner and the members of the group indicating that he/she is either entering or leaving. The second technique RSDG supports this facility. When the data owner comes to know that the particular user is leaving the ring, he requests the cloud service provider to remove that user's private key from cloud storage and provide the necessary information (private key, public key, block token id) about the ring in case a member enters. This will help in preserving the information from the intruder.

Pseudocode: TRBS Algorithm

```
BEGIN
INPUT: ÞḰ = private key, ΔḰ= Public key ,Ţ= Token number
IF((ÞḰ  && ΔḰ ) == Valid)  THEN
  // Accept block token number from user
    IF (Ţ == Valid)   THEN
DO
   //Allow User to Read a block βi
   // Allow  User to commit
IFNew( βi)!= βi THEN
  //Intimate  Data owner
END IF
END IF
//Re-compute New ring
END IF
END
```

Table-1. Comparison table.

	PDP [3]	**WWRL** [10]	**ORUTA** [1]	**TBRS** (Proposed Method)
Public Auditing	✓	✓	✓	✓
Data Privacy	×	✓	✓	✓
Identity Privacy (static)	×	×	✓	✓
Identity Privacy (dynamic)	×	×	×	✓
Integrity of Data	×	×	×	✓

The analysis of PDP [3], WWRL [10], ORUTA [1] and TBRS are abstracted in Figure-2 and it is clear that TBRS algorithm helps in preserving the privacy of data and identity of the user in static as well as dynamic groups. The information stored in cloud will not be revealed easily to the intruder and thus the security of data stored in cloud is improved.

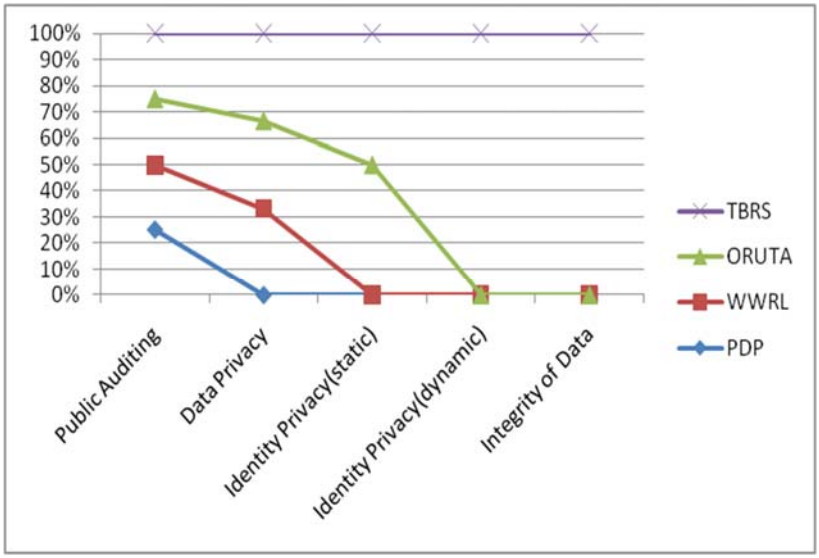

Figure-2. Comparison chart of proposed method.

CONCLUSIONS

Cloud computing is an environment that offers on-demand services to the clients from a shared pool of configurable resources. Cloud is not only a platform to store the user data but it can also be accessed by multiple users. The scheme TBRS utilizes enhanced ring signatures to improve the security of the information present in cloud with the help of tokens. The next system RSDG helps in conserving the confidential information stored in cloud in case an existing user exits the group and requests the cloud service provider to remove the information about that user. Enhanced security and performance analysis prove that the proposed schemes are highly securable and efficient the concept of multiple auditing tasks is left for future work.

REFERENCES

[1] B. Wang, B. Li, and H. Li. 2014. Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud. IEEE Transactions on Cloud Computing. 2(1): 43-56.

[2] R. L. Rivest, A. Shamir and Y. Tauman. 2001. How to Leak a Secret. In: Proc. International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT). Springer-Verlag. pp. 552-565.

[3] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson and D. Song. 2007. Provable Data Possession at Untrusted Stores. In: Proc. ACM Conference on Computer and Communications Security (CCS). pp. 598-610.

[4] A. Juels and B. S. Kaliski. 2007. PORs: Proofs pf Retrievability for Large Files. In: Proc. ACM Conference on Computer and Communications Security (CCS). pp. 584-597.

[5] H. Shacham and B. Waters. 2008. Compact Proofs of Retrievability. In: Proc. International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT). Springer-Verlag. pp. 90-107.

[6] D. Boneh, C. Gentry, B. Lynn and H. Shacham. 2003. Aggregate and Verifiably Encrypted Signatures from Bilinear Maps. In: Proc. International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT). Springer-Verlag. pp. 416-432.

[7] D. Boneh, B. Lynn, and H. Shacham. 2001. Short Signature from the Weil Pairing. In: Proc. International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT). Springer-Verlag. pp. 514-532.

[8] C. Erway, A. Kupcu, C. Papamanthou and R. Tamassia. 2009. Dynamic Provable Data Possession. In: Proc. ACM Conference on Computer and Communications Security (CCS). pp. 213-222.

[9] Y. Zhu, H. Wang, Z. Hu, G.-J. Ahn, H. Hu and S. S. Yau. 2001. Dynamic Audit Services for Integrity Verification of Outsourced Storage in Clouds. In:

Proc. ACM Symposium on Applied Computing (SAC). pp. 1550-1557.

[10] C. Wang, Q. Wang, K. Ren and W. Lou. 2010. Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing. In: Proc. IEEE International Conference on Computer Communications (INFOCOM). pp. 525-533.

[11] D. Boneh, C. Gentry, B. Lynn, and H. Shacham. 2003. Aggregate and Verifiably Encrypted Signatures from Bilinear Maps. In: Proc. International Conference on the Theory and Applications of Cryptographicn Techniques (EUROCRYPT). Springer-Verlag. pp. 416-432.