International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 5 | ISSN : 2456-3307

Providing security for the Encrypted shared data in the cloud Environment

O. Sahithya[1], A. Supriya[2]

[1]M.Tech Student, Department of Computer Science And Engineering, Sri Padmavati Mahila Visvavidyalayam University, Tirupathi, India

[2]Assistant Professor, Department of Computer Science And Engineering, Sri Padmavati Mahila Visvavidyalayam University, Tirupathi, India

ABSTRACT

In the gift system a secure multi-keyword class-conscious search theme over encrypted cloud data, that at a similar time supports dynamic update operations like deletion and insertion of documents. Specifically, the vector house model and conjointly the widely-used TF_IDF model unit combined among the index construction and question generation. we tend to tend to construct a special tree-based index structure and propose a "Greedy Depth-first Search" rule to provide economical multi-keyword class-conscious search. The secure kNN rule is employed to inscribe the index and question vectors, and within the meanwhile guarantee correct association score calculation between encrypted index and question vectors. Therefore on resist math attacks, phantom terms unit supplementary to the index vector for bright search results. Attributable to the utilization of our special tree-based index structure, the planned theme will do sub-linear search time and upset the deletion and insertion of documents flexibly. Intensive experiments unit conducted to demonstrate the efficiency of the planned theme. Among the planned system we tend to tend to propose the first privacy-preserving mechanism that allows public auditing on shared data keep among the cloud. Specially, we tend to tend to take advantage of ring signatures to calculate the verification knowledge needed to audit the integrity of shared data. With our mechanism, the identity of the signer on each block in shared data is unbroken personal from a third-party auditor (TPA), United Nations agency continues to be able to publically verify the integrity of shared data whereas not retrieving the full file. Our experimental results demonstrate the effectiveness and efficiency of our planned mechanism once auditing shared data.

Keywords : TF_IDF, kNN, Greedy Depth-first Search, TPA, PDP, HARS, FTP

I. INTRODUCTION

Cloud service suppliers manage an Enterprise-class infrastructure that gives a scalable, secure and reliable atmosphere for users, at a way lower marginal price because of the sharing nature of resources. It's routine for users to use cloud storage services to share information with others in an exceedingly team, as information sharing becomes a typical feature in most cloud storage offerings, as well as Drop box and Google Docs. The integrity of knowledge in cloud storage, however, is subject to skepticism and scrutiny, as information hold on in AN untrusted cloud will simply be lost or corrupted, because of hardware failures and human errors [1]. To safeguard the integrity of cloud information, it's best to perform public Auditing by introducing a 3rd party auditor (TPA), World Health Organization offers its auditing service with additional powerful computation and communication skills than regular users. The primary obvious information possession (PDP) mechanism [2] to perform public auditing is intended to visualize the correctness of knowledge hold on in AN untrusted server, while not retrieving the whole information. Moving a leap forward, Wang et al. [3] (referred to as WWRL during this paper) is intended to construct a public auditing mechanism for cloud information, in order that throughout public auditing, the content of personal information happiness to a private user isn't

disclosed to the third party auditor. We have a tendency to believe that sharing information among multiple users is maybe one in all the foremost participating options that motivates cloud storage. A novel drawback introduced throughout the method of public auditing for shared information within the cloud is how to preserve identity privacy from the TPA, as a result of the identities of signers on shared information might indicate that a selected user within the cluster or a special block in shared information may be a higher valuable target than others.

Problem Statement:

Here we have a tendency to solely take into account a way to audit the integrity of shared knowledge within the cloud with static teams. It suggests that the cluster is pre-defined before shared knowledge is made within the cloud and also the membership of users within the cluster isn't modified throughout knowledge sharing. The initial user is to blame for deciding World Health Organization is ready to share her knowledge before outsourcing knowledge to the cloud. Another fascinating drawback is a way to audit the integrity of shared knowledge within the cloud with dynamic teams a replacement user may be added into the cluster associated an existing cluster member maybe revoked Throughout knowledge sharing whereas Still conserving identity privacy. We'll leave this drawback to our future work. When a user (either the initial user or a bunch user) needs to ascertain the integrity of shared knowledge, she 1stsends associate auditing request to the TPA. Once receiving the auditing request, the TPA generates associate auditing message to the cloud server, associated retrieves an auditing proof of shared knowledge from the cloud server. Then the TPA verifies the correctness of the auditing proof. Finally, the TPA sends associate auditing report back to the user supported the results of the verification.

Ring Signatures

The idea of ring signatures is 1st planned by Rivest et al. [4] in 2001. With ring signatures, a voucher is convinced that a signature is computed victimization one in everyof cluster members' personal keys, however the voucher isn't ready to confirm that one. This property is wont to preserve the identity of the signer from a voucher. The ring signature theme introduced by Boneh et al. [5] (referred to as BGLS during this paper) is made on additive maps. We'll extend this ring signature theme to construct our public auditing mechanism.

II. HOMOMORPHIC AUTHENTICABLE RING SIGNATURES

Overview

In this section, we tend to introduce a replacement ring signature theme that is appropriate for public auditing. Then, we'll show a way to build the privacy-preserving public auditing mechanism for shared knowledge within the cloud supported this new ring signature theme within the next section. As we tend to introduced in previous sections, we tend to shall utilize ring signatures to cover the identity of the signer on every block, in order that personal and sensitive info of the cluster isn't disclosed to the TPA. However, ancient ring signatures [4], [5] cannot be directly used into public auditing mechanisms, as a result of these ring signature schemes don't support block less verification. While not block less verification, the TPA should transfer the entire record to verify the correctness of shared knowledge that consumes excessive information measure and takes long verification times. Therefore, we tend to initial construct a replacement homomorphic authenticable ring signature (HARS) theme, that is extended from a classic ring signature theme [5], denoted as BGLS. The ring signatures generated by HARS is ready not solely to preserve identity privacy however conjointly to support block less verification.

Construction of HARS

HARS contains 3 algorithms: KeyGen, RingSign and Ring Verify. In KeyGen, every user within the cluster generates her public key and personal key. In Ring Sign, a user within the cluster is ready to sign a block along with her personal key and every one the cluster members' public keys. A champion is allowed to ascertain whether or not a given block is signed by a bunch member in Ring Verify. Theme Details. Let G1, G2 and GT be increasing cyclic teams of order p, g1 and g2 be generators of G1 and G2 severally. Let e: G1 × G2 → GT bean additive map, and ψ: G2 → G1 be a calculable isomorphy with ψ (g2) = g1. There's a public map-to-point hash perform H1: *→G1. The world parameters square measure (e, ψ, p, G1, G2, GT, g1, g2, H1). The full variety of users within the cluster

is d. Let U denote the cluster that features all the the users.

KeyGen. For a user u_i in the group U, she randomly picks $x_i \in Z_p$ and computes $w_i = g_2^{x_i} \in G_2$. Then, user u_i's public key is $\mathbf{pk}_i = w_i$ and her private key is $\mathbf{sk}_i = x_i$.

RingSign. Given all the d users' public keys $(\mathbf{pk}_1, ..., \mathbf{pk}_d) = (w_1, ..., w_d)$, a block $m \in Z_p$, the identifier of this block id and the private key $\mathbf{sk}_s$ for some s, user u_s randomly chooses $a_i \in Z_p$ for all $i \neq s$, where $i \in [1, d]$, and let $\sigma_i = g_1^{a_i}$. Then, she computes

$$\beta = H_1(id) g_1^m \in G_1, \quad (1)$$

and sets

$$\sigma_s = \left(\frac{\beta}{\psi(\prod_{i \neq s} w_i^{a_i})} \right)^{1/x_s} \in G_1. \quad (2)$$

And the ring signature of block m is $\boldsymbol{\sigma} = (\sigma_1, ..., \sigma_d) \in G_1^d$.

RingVerify. Given all the d users' public keys $(\mathbf{pk}_1, ..., \mathbf{pk}_d) = (w_1, ..., w_d)$, a block m, an identifier id and a ring signature $\boldsymbol{\sigma} = (\sigma_1, ..., \sigma_d)$, a verifier first computes $\beta = H_1(id) g_1^m \in G_1$, and then checks

If the above equation holds, then the given block m is signed by one of these d users in the group. Otherwise, it is not.

Push and Pull Mode

To allow users to be timely and accurately informed about their data usage, our distributed logging mechanism is complemented by an innovative auditing mechanism. We support two complementary auditing modes: 1) push mode; 2) pull mode.

Push Mode:

In this mode, the logs are periodically pushed to the data owner (or auditor) by the harmonizer. The push action will be triggered by either type of the following two events: one is that the time elapses for a certain period according to the temporal timer inserted as part of the JAR file; the other is that the JAR file exceeds the size stipulated by the content owner at the time of creation. After the logs are sent to the data owner, the log files will be dumped, so as to free the space for future access logs. Along with the log files, the error correcting information for those logs is also dumped.

This push mode is the basic mode which can be adopted by both the PureLog and the AccessLog, regardless of whether there is a request from the data owner for the log files. This mode serves two essential functions in thelogging architecture: 1) it ensures that the size of the log files does not explode and 2) it enables timely detection and correction of any loss or damage to the log files. Concerning the latter function, we notice that the auditor, upon receiving the log file, will verify its cryptographic guarantees, by checking the records' integrity and authenticity. By construction of the records, the auditor, will be able to quickly detect forgery of entries, using the checksum added to each and every record.

Pull Mode

This mode allows auditors to retrieve the logs anytime when they want to check the recent access to their own data. The pull message consists simply of an FTP pull command, which can be issues from the command line. For naive users, a wizard comprising a batch file can be easily built. The request will be sent to the harmonizer, and the user will be informed of the data's locations and obtain an integrated copy of the authentic and sealed log file.

III. CONCLUSION

In this paper, we tend to propose Oruta, the primary privacy preserving public auditing mechanism for shared information within the cloud. we tend to utilize ring signatures to construct homomorphism authenticators, therefore the TPA is in a position to audit the integrity of shared information, nevertheless cannot distinguish United Nations agency is that the signer on every block, which may reach identity privacy. To boost the potency of verification for multiple auditing tasks, we tend to additional extend our mechanism to support batch auditing. A motivating drawback in our future work is the way to expeditiously audit the integrity of shared information with dynamic teams whereas still protective the identity of the signer on every block from the third party auditor.

IV. REFERENCES

[1]. M. Armbrust, A. Fox, R. Griffith, A. D.Joseph, R. H.Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A read of Cloud Computing," Communications of the ACM, vol. 53, no. 4, pp. 50-58, April 2010.

[2]. G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable information Possession at Untrusted Stores," in Proc. ACM Conference on laptop and Communications Security (CCS), 2007, pp. 598-610.

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

[4]. R. L. Rivest, A. Shamir, and Y. Tauman, "How to Leak a Secret," in Proc. International Conference on the speculation and Application of science and data Security (ASIACRYPT). Springer- Verlag, 2001, pp. 552-565.

[5]. D. Boneh, C. Gentry, B. Lynn, and H. Shacham, "Aggregate and Verifiably Encrypted Signatures from additive Maps," in Proc. International Conference on the speculation and Applications of cryptological Techniques (EUROCRYPT). Springer-Verlag, 2003, pp. 416-432.

[6]. H. Shacham and B. Waters, "Compact Proofs of Retrievability," in Proc. International Conference on the speculation and Application of science and data Security (ASIACRYPT). Springer- Verlag, 2008, pp. 90-107.

[7]. Y. Zhu, H.Wang, Z. Hu, G.-J. Ahn, H. Hu, and S. S.Yau, "Dynamic Audit Services for Integrity Verification of Outsourced Storage in Clouds," in Proc. ACM conference on Applied Computing (SAC), 2011, pp. 1550-1557.

[8]. S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving Secure, Scalable, and Fine-grained information Access management in Cloud Computing," in Proc. IEEE International Conference on laptop Communications (INFOCOM), 2010, pp. 534-542.

[9]. D. Boneh, B. Lynn, and H. Shacham, "Short Signature from the Weil Pairing," in Proc. International Conference on the speculation and Application of science and data Security (ASIACRYPT). Springer-Verlag, 2001, pp. 514-532.

[10]. D. Boneh and D. M. Freeman, "Homomorphic Signatures for Polynomial Functions," in Proc. International Conference on the speculation and Applications of cryptological Techniques (EUROCRYPT). Springer-Verlag, 2011, pp. 149-168.

[11]. A. L. Ferrara, M. Green, S. Hohenberger, and M. Ø. Pedersen, "Practical Short Signature Batch Verification," in Proc. RSA Con- ference, the Cryptographers' Track (CT-RSA). Springer-Verlag, 2009, pp. 309-324.

[12]. V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based secret writing for Fine-Grained Access management of Encrypted information," in Proc. ACM Conference on laptop and Communications Security (CCS), 2006, pp. 89-98.

[13]. A. Juels and B. S. Kaliski, "PORs: Proofs pf Retrievability for giant Files," in Proc. ACM Conference on laptop and Communications Security (CCS), 2007, pp. 584-597.

[14]. G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik, "Scalable and economical obvious information Possession," in Proc. International Conference on Security and Privacy in Communication Networks (SecureComm), 2008.

[15]. C. Erway, A. Kupcu, C. Papamanthou, and R. Tamassia, "Dynamic obvious information Possession," in Proc. ACM Conference on laptop and Communications Security (CCS), 2009, pp. 213-222.

[16]. C. Wang, Q. Wang, K. Ren, and W. Lou, "Ensuring information Storage Security in Cloud Computing," in Proc. IEEE/ACM International Workshop on Quality of Service (IWQoS), 2009, pp. 1-9.

[17]. B. Chen, R. Curtmola, G. Ateniese, and R. Burns, "Remote information Checking for Network Coding-based Distributed Stroage Systems," in Proc. ACM Cloud Computing Security Workshop (CCSW), 2010, pp. 31-42.

[18]. N. Cao, S. Yu, Z. Yang, W. Lou, and Y. T. Hou, "LT CodesbasedSecure and Reliable Cloud Storage Service," in Proc. IEEE International Conference on laptop Communications (INFOCOM), 2012.

[19]. S. Halevi, D. Harnik, B. Pinkas, and A. Shulman-Peleg, "Proofs of possession in Remote Storage Systems," in Proc. ACM Conference on laptop and Communications Security (CCS), 2011, pp. 491-500.

[20]. Q. Zheng and S. Xu, "Secure and economical Proof of Storage with Deduplication," in Proc. ACM Conference on information and

Application Security and Privacy (CODASPY), 2012.

[21]. M. Franz, P. Williams, B. Carbunar, S. Katzenbeisser, and R. Sion, "Oblivious Outsourced Storage with Delegation," in Proc. Finan- cial Cryptography and information Security Conference (FC), 2011, pp. 127- 140.

[22]. S. D. C. di Vimercati, S. Foresti, S. Paraboschi, G. Pelosi, and P. Samarati, "Efficient and personal Access to Outsourced information," in Proc. IEEE