ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING

National Conference on Advanced Innovation in Engineering and Technology (NCAIET-2015)

Alva's Institute of Engineering and Technology, Moodbidri

Vol. 3, Special Issue 1, April 2015

Oruta: Ensuring Data Integrity and Public Assessment for Shared Data in the Cloud

Mr. Joshil[1], Mrs. Rasheeda Z Khan[2]

M-Tech Student, Dept. of Computer Science and Engineering, Shree Devi Institute of Technology, Mangalore, Karnataka, India[1]

HOD and Assistant Professor, Department of Information Science and Engineering, Shree Devi Institute of Technology, Mangalore, Karnataka, India[2]

Abstract: The data is not only stored in the cloud but also can be shared across multiple users with the help of cloud storage services. Wherein, Public data is shared among multiple users but to preserve the Data Integrity is a challenge. In this paper, we propose shared public auditing and preserve the Data Integrity stored in the cloud. On our mechanism, We are going to securely increase the privacy level of the confidential data in a way so that the data is cannot be easily extracted from the Hacker or any unknown user and also we get the help from the TPA (Third Party Auditor), wherein it stores the unique key and using this it is encrypted and stored but the cloud user will be unaware of it. Only the public data is shared among various users in the cloud.

Keywords: Data Integrity, Shared Public Auditing, Hacker.

I. INTRODUCTION

Cloud provides a large storage space where a wide variety of information can be stored in it. The user need not worry of the path or the place where the data stored. But the problem arises when the data is stored in an untrusted cloud, the data can get corrupted or lost due to hardware breakdown and human mistakes [1].

For integrity protection, we perform public auditing by making use of the TPA (Third Party Auditor) wherein the computation is improved and faster access of communication. Wang et al [3] introduced a public auditing wherein TPA cannot access the confidential information. We give high priority to the private key in the TPA stored so that confidential data is made secure where we generate random keys.

We present in this Paper, in an untrusted cloud: Oruta, Ensuring data integrity and public auditing mechanism where we use signatures [4] to construct homomorphic unique tags [2], so that the privacy of the confidential information is kept secure from the unknown users or hackers.

Later, we support our mechanism for batch auditing wherein, simultaneously multiple data users can access shared data in a single auditing task. Moving on, we make the use of random masking [3] to keep the privacy of files and also protection of confidential data and we use dynamic operations with index hash tables [5]. Dynamic operations we implemented are insert, upload or download of files, delete or modify and view.

II. PROBLEM STATEMENT

As shown in fig.1, we have 3 parties: The TPA (Third Party Auditor), The cloud Server and the users wherein a user consists of two types, original user and group users. Original user creates the shared data and Group members can access the data stored and do changes if any. In the cloud server, shared data and the signatures are stored. On behalf of group members, the TPA checks the privacy of the shared data in the cloud server.

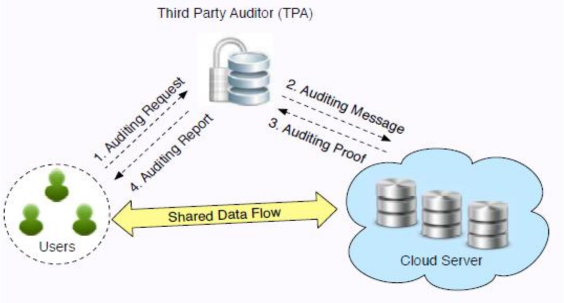

fig.1

In this paper, we consider in the shared data how to audit the privacy on static and dynamic groups. In static groups, before the shared data is created the group is defined in advance. In Dynamic groups, a new user can be added to the group and an existing group member can be removed from the group.

A user for the shared data wants to check the integrity firstly to the TPA he sends an auditing request. When the TPA gets the request, makes an auditing message and sends to the cloud server. The cloud servers reply with the auditing proof to the TPA. Later, the user gets the auditing

DOI 10.17148/IJIREEICE

report from the TPA where the auditing proof has been checked and verified.

A. Threat model

1. Integrity threats

There are two kinds of threats based on the shared data. Firstly, an unknown user may try to corrupt the privacy of the shared data and restrict the users of using the correct data. Secondly, due to hardware breakdown and human mistakes corrupts the data stored in it by the cloud service provider.

2. Private threats

The confidential data is kept as a secret and it is made inaccessible from any unknown users unless he is the owner to it. The privacy of the data is kept secret but the unknown users tries to fake and gain access to the TPA, once the signature is been revealed then he can access the confidential data.

III. SIGNATURES

With the help of Signatures, privacy is protected where we create random keys so that each time a new unique key is generated. With this help of this, unknown user will be unaware of the unique keys generated so because of this it is made more secure than normal.

IV. HOMOMORPHIC AUTHENTICATORS

The basic tool to construct data auditing mechanisms [2], [3] is homomorphic unique tags and it is based on signatures. It should hold the two properties: Blockless Verification and Non-Malleability. Blockless verification makes a user to satisfy single block with the help keys for encryption. If the key is correct then he can download all details to it. Non-malleability represent that with the fake keys he cannot download the details.

V. HOMOMORPHIC UNIQUE AUTHENTICABLE TAGS (HUAT)

A. Overview

We bring into use new unique signatures which is used for security for files or data that is stored in the cloud. As mentioned in the above sections, to preserve the confidential information we use in keys for protection. Since the key is fixed the hacker might get the key by faking or any such method. So to preserve the identity, we generate random Unique keys for each block of data named it as Homomorphic Unique Authenticable Tags (HUAT). All the keys will be generated and stored in the TPA. This uniqueness of keys preserves the data and supports blockless verification.

B. Construction OF HUAT

It can be done as follows: UniquekeyGen ,RingSign and RingCheck. In UniquekeyGen, a unique random key is generated for private key and a fixed key is kept for public data. In RingSign , the data that is kept private is encrypted with the signed unique random key that is generated whereas in public a fixed key is signed. In RingCheck , we decide which is private and which is public ,confidential data is kept safe and the public data is viewed to all users.

C. Security Properties of HUAT

Let us examine some of the important properties related to HUAT; some are correctness, Non-malleability, Identity privacy security, unique key encryption, Data Recovery through breakdown.

The data block is made secure by keeping some of the blocks as confidential or private and some information as public so that the confidential information is made more secure than the public data. These data is stored in the database in a secure way through encryption. The TPA should be correctly verify which is private and which is public and use the necessary keys for decryption of data and also check whether there is any corrupted data in the block. This is correctness. Next, goes to the non-malleability, where the hacker cannot change the privacy of the block or leak the information using his fake keys created. For each of the data stored privacy is kept for it i.e. public or private. If it is private or confidential, it is encrypted using random keys generated and stored in the database so that it is kept confidential to the unknown user whereas in the public it is shown to everyone to the registered user .Comparing to the private data storing of public data is similar but a small change of using the keys, rather using random keys public data uses fixed keys. Next, if we consider the encryption of data, every time a new unique key is generated with this it is encrypted using these keys so as to preserve the privacy of the confidential information so that it is not easily hacked. This type of preserving is known as unique key encryption. Even if we done all these methods ,there might be a chance that the database might breakdown because of this all the stored data might be get lost or corrupt, to protect from this a data recovery or a backup is done so even if the database breakdown, with this help all the contents will be recovered. This property is known as data recovery through breakdown.

VI. PRIVACY PRESERVING PUBLIC AUDITING FOR SHARED DATA IN THE CLOUD

A. Overview

With the properties of HUART, we made a little changes related to the previous ones. TPA holds the keys that is been randomly generated. The keys that is been generated are unique ones. With this unique keys generated we can store the data uniquely. As for the public ones, fixed keys is generated and stored so as the distinguish between both the data.

B. Dynamic operations

The different dynamic operations performed are insert, delete and modify data to the single block of data with the index hash tables [5] a unique recognition is given to distinguish each one of them. With this help the data

DOI 10.17148/IJIREEICE

belonging to that user will be stored in that block. . For a different group of data, a particular unique key is generated and protected with this key. This unique is kept secure with the help of TPA so that the user cannot fake the key and do the changes. Insertion is a method where we can insert a user to the database and update his/her details to it. A separate block is created for each user belonging to that group. With deletion, data can be deleted or destroyed if he/she is not interested in. Modification is one such way wherein he/she can change the contents if a new update required for it because of it the users belonging to that will be refreshed with latest details.

C. Construction

Public assessment is done as follows: actually it consists of UniquekeyGen, ValidKeyCheck, KeyEncrypt, Split, Combine, KeyVerify , KeyDecrypt . Firstly, when the TPA gets the request from the user to generate the keys, a unique key is generated and stored in the TPA. This is called UniquekeyGen. In ValidKeyCheck, only a valid key can be used that has been got from the TPA and checked, invalid key is discarded. Next, the valid key generated is used for encryption. This method is called KeyEncrypt. In Split , the encrypted data got is divided into three parts and kept into separate files.

If the user wants to see the data he has to go the reverse way as shown above, the split data is made into one piece by combining them. This is called Combine. In KeyVerify, it verifies whether the key is a valid one and whether it exists in the TPA or not. For the user to read the message the data should be in readable format so it has to be decrypted and shown to the user.

This one is called KeyDecrypt. Here we generate random keys [3] so that it is unique for each form of data. The unique key is kept in TPA so that he is a trusted one.

D. Security Analysis

Some of the security properties are as follows: Key Uniqueness, Data privacy and file split. We generate unique keys wherein for each group of data different keys are used for encryption. These keys will be stored in the TPA, who is a trusted one. This is Key Uniqueness.

The TPA cannot reveal any confidential content since it uses keys for encryption. It's not just normal keys; these keys are generated randomly for each data. Even if they Fake these keys, checking is performed to check whether the key is got from the TPA or not.

This is called Data privacy. Encryption of files by the key got from the TPA that has been randomly generated is been used. The encryption done is split into three parts and it is stored separated in different files. This is called as file split, because of this data cannot be easily got.

VII. RELATED WORK

Wang et al. [6] made fully dynamic operation possible in his approach. Wang et al. [3] introduced a public mechanism wherein with the help of TPA private data of the users can be made secure by random masking and also support batch auditing. Wang et al. [7] made possible for data not only for the dynamic operations but also for recognising the server which does not act accordingly. Halevi et al. introduced proof of ownership (POWs) to prevent from deduplication in remote data storage. He also showed to the server that the client holds some data file rather than hash value. Recently, Franz et al. from an untrusted cloud introduced Oblivious RAM technology where the access pattern can be hidden on outsourced data. Vimercati et al made the users access pattern secure by using shuffle index structure.

CONCLUSION

We introduce oruta, Ensuring data integrity and public assessment for shared data in the cloud. We make use homomorphic unique tags where a unique key is randomly created and stored in the TPA, with this help he will distinguish between a confidential information and public data. We also did public assessment where unique keys can be used for encryption . Next, it is split and kept separate so that it is not easily extracted or decrypted.

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 View 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 Data Possession at Untrusted Stores,"in Proc. ACM Conference on Computer and Communications Security (CCS), 2007, pp. 598–610.

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

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

[5]. 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 Symposium on Applied Computing (SAC), 2011, pp. 1550–1557.

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

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