INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 4 ISSUE 2 (2018) PAGES 3226 - 3231
RECEIVED : 10.03.2018 PUBLISHED : 11.04.2018

April 11, 2018

AUDIT FREE CLOUD STORAGE VIA DENIABLE ATTRIBUTE BASED ENCRYPTION

K.Vignesh[1],D.Naveen Kumar[2],P.Latha[3]

Students[1, 2,] ,Assistant Professor[3]

Department of Computer Science and Engineering

Kingston Engineering College, Vellore, India.

I . ABSTRACT

With the fast improvement of distributed computing, distributed storage has been acknowledged by an expanding number of associations what's more, people, in that filling in as a helpful and on-request outsourcing application. Be that as it may, after losing neighborhood control of information, it turns into an earnest requirement for clients to confirm whether cloud specialist organizations have put away their information safely. Consequently, numerous analysts have committed themselves to the plan of inspecting conventions coordinated at outsourced information. In this paper, we propose a productive open inspecting convention with worldwide and examining block less confirmation and additionally clump reviewing, where information flow are significantly more productively bolstered than is the situation with the best in class

II. INTRODUCTION:

For data auditing in a cloud, many protocols have been proposed in the past few years and can be divided into private protocols and public protocols. In the model of private auditing protocols, the participating entities are the DO and the CSP. Only the DO possesses the private key, and the entire auditing process is executed by the owner. However, these solutions increase the burden on DOs, who are not equipped with sufficient computing resources. Moreover, the fatal flaw is that the auditing results are unconvincing because the DO and the CSP distrust each other, and the DO is the sole source of the verification results. To remove the above doubts, a trustworthy TPA is introduced into the system.

III. EXISTING SYSTEM:

SYSTEM DESCRIPTION:

The rapid development of such a cloud service has various causes such as its on demand outsourcing function, ubiquitous network access, and location-independent resources. For instance, data are no longer local with cloud storage, ensuring that data owners (DOs) do not have to worry about software or hardware failures. In addition, overhead resulting from maintenance, financial cost, time, and other resources would be greatly reduced, relieving the burden on DOs and local devices.

DISADVANTAGE:

This takes half of the total table length to locate a certain element on average.

The time stamp participating in is generated by the DO itself as well. That is where the problem lies.

On the other hand, the outsourced data might suffer from cloud service providers.

IV. PROPOSED SYSTEM

SYSTEM DESCRIPTION:

We design an efficient public auditing protocol with novel dynamic structure for outsourced data in the cloud, which preforms better than the state of the art. Note that global and sampling verification is presented to achieve mutual trust between DOs and CSPs. Meanwhile, data dynamics are efficiently provided by the new dynamic structure. In addition, various auditing properties, such as block less verification and batch auditing, are supported. The main contributions of this paper are summarized as follows. we support global and sampling verification to address this issue. Guarantee of sampling verification makes owners believe that the cloud has properly stored their data.

ADVANTAGES:

Global and sampling verification is proposed in the protocol.

Efficient data dynamics with a novel dynamic structure are provided in the protocol.

Various auditing properties are supported by the protocol.

We are the first to design a dynamic structure combining a doubly linked info table and a location array to efficiently support data dynamics.

Various important properties are established in the proposed auditing protocol to give it greater practical value.

V. LITERATURE SURVEY

[1] Public Integrity Auditing for Dynamic Data Sharing with Multi-User Modification

Jiawei Yuan, Shucheng Yu, Member,In past years, the rapid development of cloud storage services makes it easier than ever for cloud users to share data witheach other. To ensure users' confidence of the integrity of their shared data on cloud, a number of techniques have been proposedfor data integrity auditing with focuses on various practical features, e.g., the support of dynamic data, public integrity auditing, low communication/computational audit cost, low storage overhead. However, most of these techniques consider that only the original data owner can modify the shared data, which limits these techniques to client read-only applications. Recently, a few attempts started considering more realistic scenarios by allowing multiple cloud users to modify data with integrity assurance.

[2] Identity-Based Data Outsourcing with Comprehensive Auditing in Clouds. Yujue Wang, Qianhong Wu, Member, IEEE, Bo Qin, Wenchang Shi Robert H. Deng, Fellow, IEEE, Jiankun Hu, Cloud storage system provides facilitative file storage and sharing services for distributed clients. To address integrity, controllable outsourcing and origin auditing concerns on outsourced files, we propose an identity-based data outsourcing (IBDO) scheme equipped with desirable features advantageous over existing proposals in securing outsourced data. First, our IBDO scheme allows a user to authorize dedicated proxies to upload data to the cloud storage server on her behalf, e.g., a company may authorize some employees to upload files to the company's cloud account in a strong security with desirable efficiency.

[3] Auditing Anti-Malware Tools by Evolving Android Malware and Dynamic Loading Technique. Yinxing Xue, Guozhu Meng, Yang Liu, Tian Huat Tan, Hongxu Chen, Jun Sun, and Jie Zhang.Although a previous paper shows that existing antimalware tools (AMTs) may have high detection rate, the report is based on existing malware and thus it does not imply that AMTs can effectively deal with future malware. It is desirable to have an alternative way of auditing AMTs. In our previous paper, we use malware samples from android malware collection GENOME to summarize a malware meta-model for modularizing the common attack behaviors and evasion techniques in reusable features

[4] Enabling Cloud Storage Auditing with Verifiable Outsourcing of Key Updates. Jia Yu, Kui Ren, Senior Member, IEEE, and Cong Wang, Member, IEEE. Key-exposure resistance has always been an important issue for in-depth cyber defence in many security applications. Recently, how to deal with the key exposure problem in the settings of cloud storage auditing has been proposed and studied. To address the challenge, existing solutions all require the client to update his secret keys in every time period, which may inevitably bring in new local burdens to the client, especially those with limited computation resources such as mobile phones. In this paper, we focus on how to make the key updates as transparent as possible for the client and propose a new paradigmcalled cloud storage auditing with verifiable outsourcing of key updates.

[5] Auditing a Cloud Provider's Compliance with Data BackuP. ad Ismail, Christophe Kiennert, Jean Leneutre, and Lin CheN. The new developments in cloud computing have introduced significant security challenges to guarantee the confidentiality, integrity, and availability of outsourced data. A Service Level Agreement (SLA) is usually signed between the cloud provider and the customer. For redundancy purposes, it is important to verify the cloud provider's compliance with data backup requirements in the SLA. There exists a number of security mechanisms to check the integrity and availability of outsourced data. This task can be performed by the customer or be delegated to an independent entity that we will refer to as the verifier. However, checking the availability of data introduces extra costs, which can discourage the customer of performing data verification too often.

VI. SYSTEM CONFIGURATION

The requirements specification is a technical specification of requirements for the software products. It is the first step in the requirements analysis process it lists the requirements of a particular software system including functional, performance and security requirements. The requirements also provide usage scenarios from a user, an operational and an administrative perspective. The purpose of software requirements specification is to provide a detailed overview of the software project, its parameters and goals. This describes the project target audience and its user interface, hardware and software requirements. It defines how the client, team and audience see the project and its functionality**.**

H/W SYSTEM CONFIGURATION:

• Processor	- Intel Pentium
• Speed	- 1.1 GHz
• RAM	- 2 GB (min)
• Hard Disk	- 20 GB

S/W SYSTEM CONFIGURATION:

• Operating System	-Windows 7/8/10
• Front End	- HTML, J2EE
• Database	- Mysql.
• Database Connectivity	- JDBC**.**

VII. MODULES USED IN THIS PROJECT

1.DATA OWNERS:

Data owner can upload data's, that data are split into part data then send to trusted data checker, job of the data checker is to generate signature key from MD5 and compare with previous keys, if mismatch then that data send to Key generator Server , Job of the key generator are generate encryption key as user specified algorithm ,finally encrypt then store in Database .

2.OWNER DATASET:

In this Module We create data owner dataset, this dataset only map owner with our upload data's , we maintain common database for effectively find duplications. The files will be uploading only once. If another data owner going to upload the same file in database means they will get the notification (the data is already uploaded in database).So data owner can save cost and time.

3. SHARED DATASET:

Share Dataset is an light weight dataset that only contain mapping file metadata information, in our project we maintain one common big data database instead of unique because efficiently find duplication and memory management, if data owner share our data to client that data not replicate instead map client name. Data duplication enables data storage systems to find and remove duplication within data without compromising its availability.

4. SECURITY:

We are implementing “Dynamic Encryption key Generation”. It means all shared data only view with data owner permission, so we can avoid from unknown access. Social users are group members they can only view and share the data. If want show the data mean they need to get permission to data owner then data owner will send Encryption key after they can view the data. If data owner does not provide the KEY mean user cannot view the file. data encryption provides an important guarantee for the security and privacy of clients’ data, it limits the manners of the accessibility and availability of the encrypted data.

5. DOWNLOAD THE DUMMY FILE:

The data owner stores the original file and also the dummy file and also use the secret key for the original file. The user will retrieve the file using secret key given by the data owner. The hacker will side by side trace the file. As the hacker don’t have the secret key, they will try by giving the guessed random key. On that time the dummy file which is set by the data owner will downloaded by the user.

VIII. CONCLUSION:

In this paper, we propose a public auditing protocol with a novel dynamic structure composed of a doubly linked info table and a location array. Compared with the state of the art, an appropriate relationship between the DLIT and the LA makes our protocol perform better both in terms of efficient dynamic support and reduced overhead. Moreover, some basic challenges in cloud auditing, such as batch auditing, block less verification and lazy update, have been overcome by our protocol. Sufficient theoretical proof indicates the security of our protocol. Extensive numerical analysis and experimental comparison results could be used to validate the performance of our protocol, making it substantially more convincing

IX REFERENCES:

1] P. Mell and T. Grance, “The nist definition of cloud computing,” Communications of the Acm, vol. 53, no. 6, pp. 50–50, 2011.

[2] R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, and I. Brandic, “Cloud computing and emerging it platforms: Vision, hype, and reality for delivering computing as the 5th utility,” Future Generation Computer Systems, vol. 25, no. 6, pp. 599–616, 2009. IEEE TRANSACTION ON CLOUD COMPUTING, VOL. 13, NO. 9, MAY 2017 12

[3] K. Yang and X. Jia, “Data storage auditing service in cloud computing: challenges, methods and opportunities,” World Wide Web, vol. 15, no. 4, pp. 409–428, 2012.

[4] Z. Xia, X. Wang, X. Sun, and Q. Wang, “A secure and dynamic multi-keyword ranked search scheme over encrypted cloud data,” IEEE Transactions on Parallel and Distributed Systems, vol. 27, no. 2, pp. 1–1, 2015.

[5] Z. Fu, X. Sun, Q. Liu, L. Zhou, and J. Shu, "Achieving efficient cloud search services: Multi-keyword ranked search over encrypted cloud data supporting parallel computing," Ieice Transactions on Communications, vol. 98, no. 1, pp. 190–200, 2015.

[6] J. Shen, H. Tan, S. Moh, and I. Chung, "Enhanced secure sensor association and key management in wireless body area networks," Journal of Communications and Networks, vol. 17, no. 5, pp. 453–462, 2015.

[7] M. Green, "The threat in the cloud," IEEE Security and Privacy, vol. 11, no. 1, pp. 86–89, 2013.

[8] Q. Jiang, J. Ma, and F. Wei, "On the security of a privacy-aware authentication scheme for distributed mobile cloud computing services," IEEE Systems Journal.

[9] D. A. B. Fernandes, L. F. B. Soares, J. V. Gomes, M. M. Freire, and P. R. M. Incio, "Security issues in cloud environments: a survey," International Journal of Information Security, vol. 13, no. 2, pp. 113–170, 2014.

[10] L. F. B. Soares, D. A. B. Fernandes, J. V. Gomes, M. M. Freire, and P. R. M. Incio, Cloud Security: State of the Art. Springer Berlin Heidelberg, 2014.

.