International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue III, March 2018- Available at www.ijraset.com

Keyupdates in Cloud Storage Auditing With Outsourcing Verifiability

V.Kumararaja[1], M.Manjureka[2], A.Mahesh[3]
Assistant Professor[1], Scholar M.E[2], Assistant Professor[3]
[1, 2, 3]Er.PerumalManimekalai College of Engineering, Hosur, Tamilnadu-635117

Abstract: ***Key-exposure resistance has always been an important issue for in-depth cyber defense 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 project, how to make the key updates as transparent as possible for the client and propose a new paradigm called cloud storage auditing with verifiable outsourcing of key updates. In this paradigm, key updates can be safely outsourced to some authorized party, and thus the key-update burden on the client will be kept minimal. Specifically, we leverage the third party auditor in many existing public auditing designs, let it play the role of authorized party in our case, and make it in charge of both the storage auditing and the secure key updates for key-exposure resistance. Data access control is an effective way to ensure the data security in the cloud. Due to data outsourcing and untrusted cloud servers, the data access control becomes a challenging issue in cloud storage systems. There are multiple authorities co-exist and each authority is able to issue attributes independently in this design, TPA only needs to hold an encrypted version ofthe client's secret key, while doing all these burdensome tasks on behalf of the client.***

Keywords: AA Setup, SKeyGen, UKeyGen, SK Update& CA Setup

I. INTROUCTION

Cloud computing is computing in which large groups of remote servers are networked to allow centralized data storage and online access to computer services or resources. Clouds can be classified as public, private or hybrid. Cloud computing, or in simpler shorthand just "the cloud", also focuses on maximizing the effectiveness of the shared resources. This can work for allocating resources to users. This approach should maximize the use of computing power thus reducing environmental damage as well since less power, air conditioning, rack space, etc. are required for a variety of functions. With cloud computing, multiple users can access a single server to retrieve and update their data without purchasing licenses for different applications.

A. Characteristics of cloud computing

1) Cloud computing exhibit five essential characteristics as defined by NIST (National Institute of Standards and Technology)

a) On-demand self-service. A consumer can unilaterally provide computing capabilities.

b) Broad network access. Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms. Resource pooling. The provider's computing resources are pooled to serve multiple consumers, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand.

c) Rapid elasticity. Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out and rapidly released to quickly scale in.

d) Measured service. Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service.

B. Authorities in Cloud

1) Authentication Flows: This authentication starts; the authentication consumer lists the access re-quests that require authentication. For each request, the authentication consumer will register a policy with the authentication engine. The policy includes at least three parts: the access request, the information to be collected from client devices or data aggregator for this access request, and a rule to generate the authentication result. During normal operation, client devices periodically report to

the data aggregator. This data will be used to track user behavior and support authentication requests. The authentication flow starts when an access request is received by the authentication consumer. (This request may have been initiated by a client device that the system collects data from, or by another device, such as a credit card reader.) Upon receiving the request, the authentication consumer redirects the request to the authentication engine, along with request details. The authentication engine re-thieves the policy for the access request, extracts the information that needs to be collected, and sends an inquiry to the client device and/or data aggregator.

2) *Data Analysis and Processing:* Both pull and push methods are adopted by client devices to provide data. The push path is from client devices to data aggregators. The main purpose is to constantly report the context and behavior of client devices. The push operation allows the client device to clear storage space by clearing its local cache after reporting. The pull path is a request from the authentication engine to client devices and data aggregators to send data back to the authentication engine.

C. Security and Privacy

1) *Application security :* Cloud providers ensure that applications available as a service via the cloud (SaaS) are secure by specifying, designing, implementing, testing and maintaining appropriate application security measures in the production environment.
2) *Privacy:* Providers ensure that all critical data (credit card numbers, for example) are masked or encrypted (even better) and that only authorized users have access to data in its entirety. Moreover, digital identities and credentials must be protected as should any data that the provider collects or produces about customer activity in the cloud.
3) *Physical security:* Cloud service providers physically secure the IT hardware (servers, routers, cables etc.) against unauthorized access, interference, theft, fires, floods etc. and ensure that essential supplies (such as electricity) are sufficiently robust to minimize the possibility of disruption. This is normally achieved by serving cloud applications from 'world-class' data centers.
4) *Personnel security:* Various information security concerns relating to the IT and other professionals associated with cloud services are typically handled through pre, para and post-employment activities such as security screening potential recruits, security awareness and training programs, proactive security monitoring and supervision, disciplinary procedures and contractual obligations embedded in employment contracts, service level agreements, codes of conduct, policies.

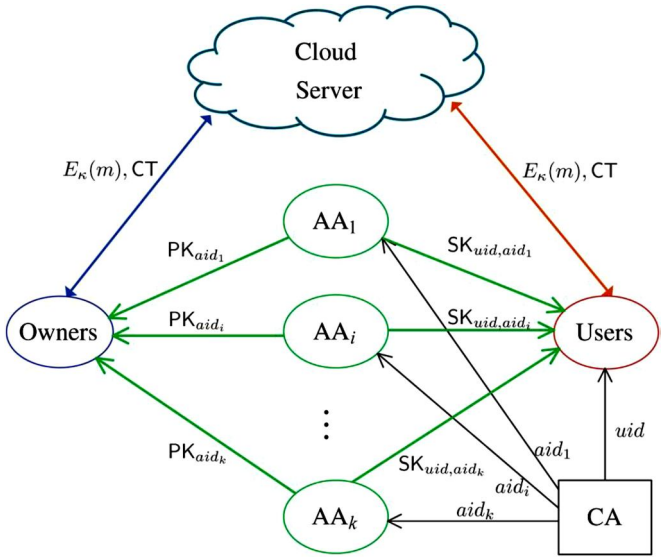
II. PREVIOUS WORKS

In this process, propose an effective and flexible distributed scheme with explicit dynamic data support to ensure the correctness of users‟ data in the cloud. We rely on erasure correcting code in the file distribution preparation to provide redundancies and guarantee the data dependability. This construction drastically reduces the communication and storage overhead as compared to the traditional replication-based file distribution techniques. By utilizing the holomorphic token with distributed verification of erasure-coded data, our scheme achieves the storage correctness insurance as well as data error localization: whenever data corruption has been detected during the storage correctness verification, our scheme can almost guarantee the simultaneous localization of data errors, i.e., the identification of the misbehaving server(s). Our work is among the first few ones in this field to consider distributed data storage in Cloud Computing. Our contribution can be summarized as the following three aspects: Compared to many of its predecessors, which only provide binary results about the storage state across the distributed servers, the challenge-response protocol in our work further provides the localization of data error. Unlike most prior works for ensuring remote data integrity, the new scheme supports secure and efficient dynamic operations on data blocks, including: update, delete and append. Extensive security and performance analysis shows that the proposed scheme is highly efficient and resilient against Byzantine failure, malicious data modification attack, and even server colluding attacks.

III. SYSTEM ORGANIZATION

Design is the first step in the development phase for any techniques and principles for the purpose of defining a device, a process or system in sufficient detail to permit its physical realization. Once the software requirements have been analyzed and specified the software design involves three technical activities – design, coding, implementation and testing that are required to build and verify the software. The design activities are of main importance in this phase, because in this activity, decisions ultimately affecting the success of the software implementation and its ease of maintenance are made. These decisions have the final bearing upon reliability and maintainability of the system. Design is the only way to accurately translate the customer’s requirements into finished software or a system. Design is the place where quality is fostered in development. Software design is a process through

which requirements are translated into a representation of software. Software design is conducted in two steps. Preliminary design is concerned with the transformation of requirements into data.



UML stands for Unified Modeling Language. UML is a language for specifying, visualizing and documenting the system. This is the step while developing any product after analysis. The goal from this is to produce a model of the entities involved in the project which later need to be built. The representation of the entities that are to be used in the product being developed need to be designed. The main purpose of a use case diagram is to show what system functions are performed for which actor. Roles of the actors in the system can be depicted It depicts the Objects and classes involved in the scenario and the sequence of messages exchanged between the objects needed to carry out the functionality of the scenario. Sequence diagrams typically are associated. These decisions have the final bearing upon reliability and maintainability of the system. Design is the place where quality is fostered in development. Software design is conducted in two steps.

IV. SYSTEM MODEL

A. Global Trust Authority Initialize Model

The CA is a global trusted certificate authority in the system. It sets up the system and accepts the registration of all the users and AAs in the system. For each legal user in the system, the CA assigns a global unique user identity to it and also generates a global public key for this user. However, the CA is not involved in any attribute management and the creation of secret keys that are associated with attributes.

Algorithm Used: CA Setup

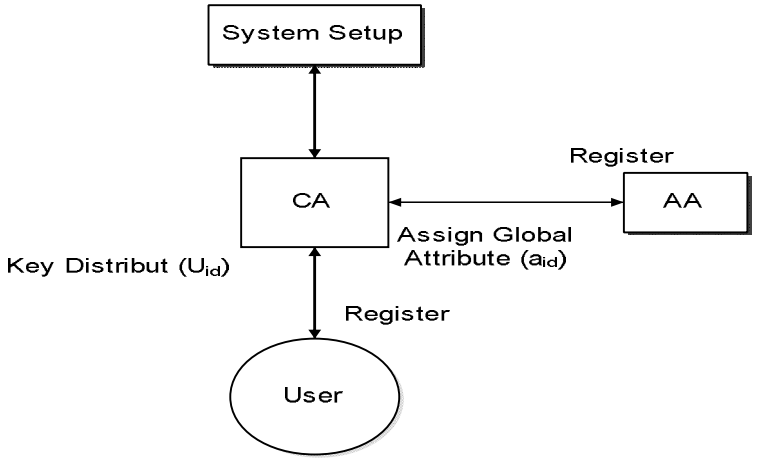


Figure: 2Global Trust Authority Initialize Module

B. Independent Attribute Authority Module

AA is an independent attribute authority that is responsible for entitling and revoking user's attributes according to their role or identity in its domain. In our scheme, every attribute is associated with a single AA, but each AA can manage an arbitrary number of attributes. Every AA has full control over the structure and semantics of its attributes. Every AA has full control over the structure and semantics of its attributes. Each AA is responsible for generating a public attribute key for each attribute it manages and a secret key for each user reflecting his/her attributes.

Algorithm Used

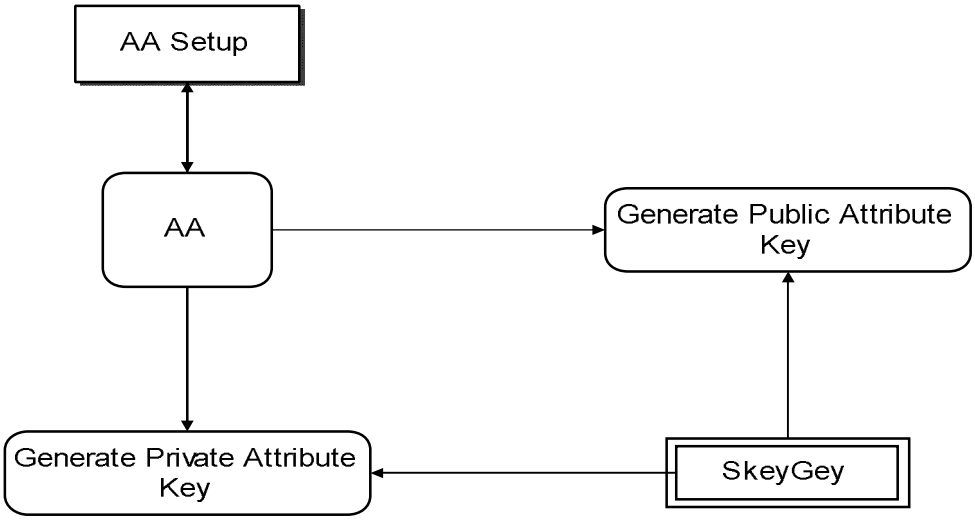


Figure: 3Independent Attribute Authority Module

C. Data Revocation Model

Discuss about how to handle user revocation and Data revocation problem. It should be ensured that users must not have the ability to access data, even if they possess matching set of attributes. For this reason, the owners should change the stored data and send updated information to other users. In revocation involved changing the public and secret keys of the minimal set of attributes which are required to decrypt the data.

Algorithm Used:

1) UKeyGen

2) SKUpdate

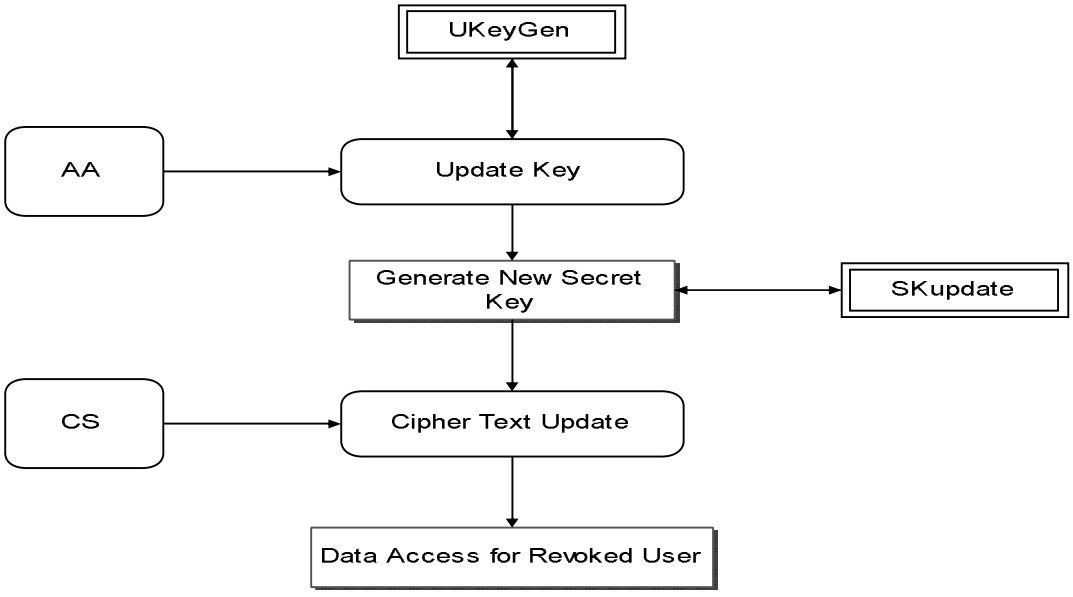


Figure:4Independent Attribute Authority Module

D. Data Storage Module (Server Module)

Cloud is operated by CSPs and provides priced abundant storage services. However, the cloud is not fully trusted by users since the CSPs are very likely to be outside ofthecloudusers"trusteddomain.Thecloudserverishonestbutcurious.Cloudserverto verify the signature the cloud server responds the corresponding data file and the revocation list to the user and response the particular file to authenticated users.

Algorithm Used

1) Verify Signature

V. CONCLUSIONS

In this paper proposed a revocable multi-authority CP-ABE scheme that can support efficient attribute revocation. Then, constructed an effective data access control scheme for multi-authority cloud storage systems. Also proved that scheme was provable secure in the random oracle model. The revocable multi-authority CP-ABE is a promising technique, which can be applied in any remote storage systems and online social networks etc.

A. Future Enhancements

It will be interesting to enhance the HSN with a third party auditor to verify the cloud server that stores and process the PHRs homomorphic Split key Encryption can become additional enhancement to verify the trustworthiness of the TPA.

REFERENCES

[1] Juels A and Kaliski,B. S ACM conference on Computer and communications security. New York, NY, USA: ACM,2007, pp. 584–597.
[2] Agrawal A et al. Ws-bpel extension for people (bpel4people), version 1.0., 2007
[3] Wang C,WangQ ,Ren K and Lou W "Ensuring data storage security in cloud computing," in Proc. of IWQoS'09, July 2009, pp. 1–9.
[4] Boneh D and M.K. Franklin M.K "Identity-Based Encryption from the Weil Pairing" in Proc. 21st Ann. Int"l Cryptology Conf.: Advances in Cryptology - CRYPTO"01, 2001, pp. 213-229.
[5] Bethencourt J, Sahai A and Waters B"Cipher text-Policy Attribute-Based Encryption" in Proc. IEEE Symp. Security and privacy (S&P"07), 2007, pp. 321-334.
[6] Chase M "Multi-Authority Attribute Based Encryption" in Proc. 4th Theory of Cryptography Conf. Theory of Cryptography (TCC"07), 2007, pp. 515-534
[7] Chase M andChowS.S.M "Improving Privacy and Security in Multi-Authority Attribute-Based Encryption" in Proc. 16th ACM Conf. Computer and Comm. Security (CCS"09), 2009, pp. 121-130
[8] Mell P and Grance T "The NIST Definition of Cloud Computing" National Institute of Standardsand Technology, Gaithersburg, MD, USA, Tech. Rep., 2009
[9] Jahid S, Mittal P and Borisov N "Easier: Encryption-Based Access Control in Social Networks with Efficient Revocation" in Proc. 6th ACM Symp. Information, Computer and Comm. Security(ASIACCS"11), 2011, pp. 411-415.