International Journal of Research
Available at https://edupediapublications.org/journals

p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 12
August 2016

Providing High Security Assurance To Anti Collusion Information Distribution Scheme for Self-Motivated Clusters in the Cloud

Dharavath Champla
M.Tech Computer Science and Engineering
Asst. Professor
Champla.805@gmail.com
Ashoka Institute of Engineering and Technology Under JNTU H.

Yasaram Ganesh
M.Tech Computer Science and Engineering
Asst. Professor
yasarapuganesh@gmail.com
Cristu Jyothi Institute of Technology Under JNTU H.

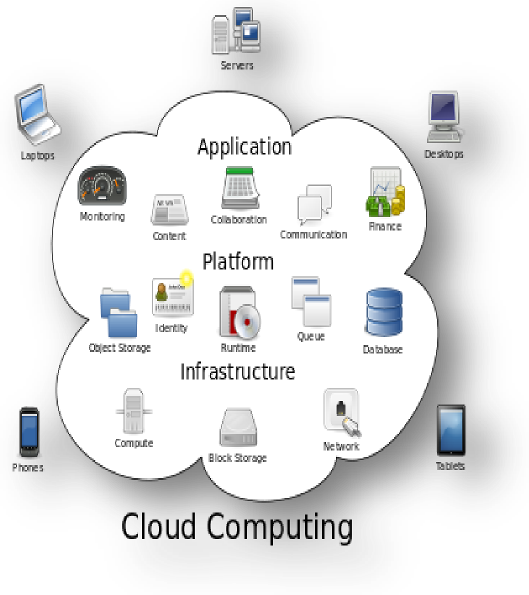
Abstract:

Benefited from cloud computing, users can get an effective and cost-effective way to swap data between cloud group members with low maintenance features and low running costs. Meanwhile, we must provide security assurance for data file exchange, since they are subcontracted. Unfortunately, due to frequent changes to the actual one, data sharing while retaining privacy remains a challenging issue, especially for a cloud that is unreliable due to collusive attack. In addition, for existing schemes, security of key distribution is based on the secure communication channel, however, having such a channel is a strong prerequisite and difficult to practice. In this document, we propose a secure data exchange schema for dynamic members. First of all, we propose a secure method to distribute keys without any secure communication channel and users can securely secure their private keys from the group administrator. Second, our schema can get detailed access control, any group user can use source in the cloud, and revoked users can not re-access the cloud after they've been revoked. Third, we can protect the scheme from collusion, which means that revoked users cannot get the original data file, even if they conspire with the unreliable cloud. In our approach, by leveraging the polynomial function, we can get a safe user revocation scheme. Finally, our schema can achieve good efficiency, which means that earlier users do not need to modernize their private keys for the circumstances, if a new user joins the cluster or a user is withdrawn from the group.

1. INTRODUCTION:

What is cloud computing?

Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet). The name comes from the common use of a cloud-shaped symbol as an abstraction for the complex infrastructure it contains in system diagrams. Cloud computing entrusts remote services with a user's data, software and computation. Cloud computing consists of hardware and software resources made available on the Internet as managed third-party services. These services typically provide access to advanced software applications and high-end networks of server computers.



Structure of cloud computing

How Cloud Computing Works?

The goal of cloud computing is to apply traditional supercomputing, or high-performance computing power, normally used by military and research facilities, to perform tens of trillions of computations per second, in consumer-oriented applications such as financial portfolios, to deliver personalized information, to provide data storage or to power large, immersive computer games.

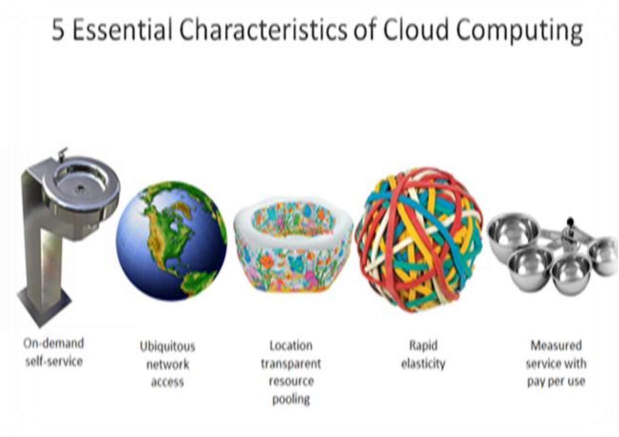
The cloud computing uses networks of large groups of servers typically running low-cost consumer PC technology with specialized connections to spread data-processing chores across them. This shared IT infrastructure contains large pools of systems that are linked together. Often, virtualization techniques are used to maximize the power of cloud computing.

Characteristics and Services Models:

The salient characteristics of cloud computing based on the definitions provided by the National Institute of Standards and Terminology (NIST) are outlined below:

- **On-demand self-service**: A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service's provider.
- **Broad network access**: Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, laptops, and PDAs).
- **Resource pooling**: The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location-independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or data center). Examples of resources include storage, processing, memory, network bandwidth, and virtual machines.
- **Rapid elasticity**: Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out and rapidly released to quickly scale in. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.
- **Measured service**: Cloud systems automatically control and optimize

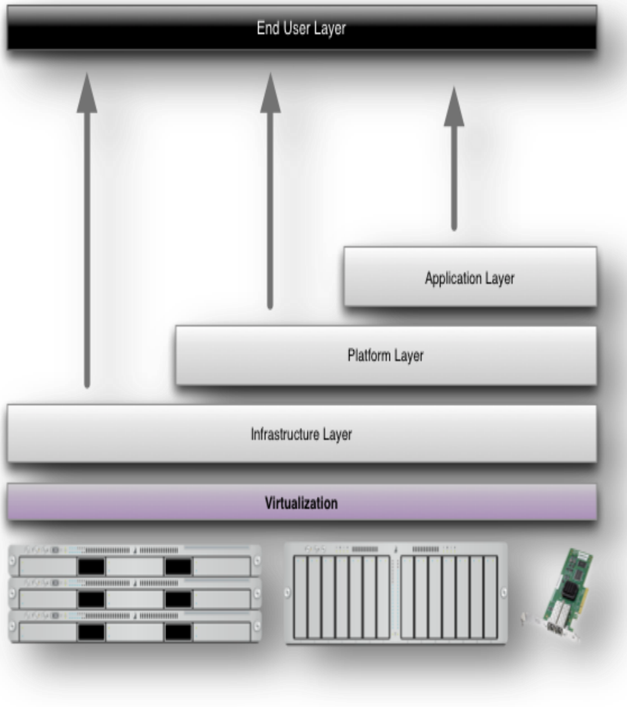
resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be managed, controlled, and reported providing transparency for both the provider and consumer of the utilized service.


5 Essential Characteristics of Cloud Computing
On-demand self-service
Ubiquitous network access
Location transparent resource pooling
Rapid elasticity
Measured service with pay per use

Characteristics of cloud computing

Services Models:

Cloud Computing comprises three different service models, namely Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS). The three service models or layer are completed by an end user layer that encapsulates the end user perspective on cloud services. The model is shown in figure below. If a cloud user accesses services on the infrastructure layer, for instance, she can run her own applications on the resources of a cloud infrastructure and remain responsible for the support, maintenance, and security of these applications herself. If she accesses a service on the application layer, these tasks are normally taken care of by the cloud service provider.



Structure of service models

Benefits of cloud computing:

1. **Achieve economies of scale** – increase volume output or productivity with fewer people. Your cost per unit, project or product plummets.
2. **Reduce spending on technology infrastructure.** Maintain easy access to your information with minimal upfront spending. Pay as you go (weekly, quarterly or yearly), based on demand.
3. **Globalize your workforce on the cheap.** People worldwide can access the cloud, provided they have an Internet connection.
4. **Streamline processes.** Get more work done in less time with less people.
5. **Reduce capital costs.** There's no need to spend big money on hardware, software or licensing fees.

6. **Improve accessibility.** You have access anytime, anywhere, making your life so much easier!
7. **Monitor projects more effectively.** Stay within budget and ahead of completion cycle times.
8. **Less personnel training is needed.** It takes fewer people to do more work on a cloud, with a minimal learning curve on hardware and software issues.
9. **Minimize licensing new software.** Stretch and grow without the need to buy expensive software licenses or programs.
10. **Improve flexibility.** You can change direction without serious "people" or "financial" issues at stake.

Advantages:

- **Price:** Pay for only the resources used.
- **Security**: Cloud instances are isolated in the network from other instances for improved security.
- **Performance:** Instances can be added instantly for improved performance. Clients have access to the total resources of the Cloud's core hardware.
- **Scalability:** Auto-deploy cloud instances when needed.
- **Uptime:** Uses multiple servers for maximum redundancies. In case of server failure, instances can be automatically created on another server.
- **Control:** Able to login from any location. Server snapshot and a software library lets you deploy custom instances.
- **Traffic:** Deals with spike in traffic with quick deployment of additional instances to handle the load.

2. Research Work

2.1 ORUTA:PRIVACY PRESERVIG PUBLIC AUDITING FOR SHARED DATA IN THE CLOUD

With cloud data services, it is commonplace for data to be not only stored in the cloud, but also shared across multiple users. Unfortunately, the integrity of cloud data is subject to skepticism due to the existence of hardware/software failures and human errors. Several mechanisms have been designed to allow both data owners and public verifiers to efficiently audit cloud data integrity without retrieving the entire data from the cloud server. However, public auditing on the integrity of shared data with these existing mechanisms will inevitably reveal confidential information-identity privacy-to public verifiers. In this paper, we propose a novel privacy-preserving mechanism that supports public auditing on shared data stored in the cloud. In particular, we exploit ring signatures to compute verification metadata needed to audit the correctness of shared data. With our mechanism, the identity of the signer on each block in shared data is kept private from public verifiers, who are able to efficiently verify shared data integrity without retrieving the entire file. In addition, our mechanism is able to perform multiple auditing tasks simultaneously instead of verifying them one by one. Our experimental results demonstrate the effectiveness and efficiency of our mechanism when auditing shared data integrity.

2.2. SECURITY CHALLENGES FOR THE PUBLIC CLOUD

In this talk, I will first discuss a number of pressing security challenges in Cloud Computing, including data service outsourcing security and secure computation outsourcing. Then, I will focus on data storage security in Cloud Computing. As one of the primitive services, cloud storage allows data owners to outsource their data to cloud for its appealing benefits. However, the fact that owners no longer have physical possession of the outsourced data raises big security concerns on the storage correctness. Hence, enabling secure storage auditing in the cloud environment with new approaches becomes imperative and challenging. In this talk, I will present our recent research efforts towards storage outsourcing security in cloud computing and describe both our technical approaches and security & performance evaluations.

2.3. PRIVACY-PRESERVING PUBLIC AUDITING FOR DATA STORAGE SECURITY IN CLOUD COMPUTING

Cloud computing is the long dreamed vision of computing as a utility, where users can remotely store their data into the cloud so as to enjoy the on-demand high quality applications and services from a shared pool of configurable computing resources. By data outsourcing, users can be relieved from the burden of local data storage and maintenance. However, the fact that users no longer have physical possession of the possibly large size of outsourced data makes the data integrity protection in Cloud Computing a very challenging and potentially formidable task, especially for users with constrained computing resources and capabilities. Thus, enabling public audit ability for cloud data storage security is of critical importance so that users can resort to an external audit party to check the integrity of outsourced data when needed. To securely introduce an effective third party auditor (TPA), the following two fundamental requirements have to be met: 1) TPA should be able to efficiently audit the cloud data storage without demanding the local copy of data, and introduce no additional on-line burden to the cloud user; 2) The third party auditing process should bring in no new vulnerabilities towards user data privacy. In this paper, we utilize and uniquely combine the public key based homomorphic authenticator with random masking to achieve the privacy-preserving public cloud data auditing system, which meets all above requirements. To support efficient handling of multiple auditing tasks, we further explore the technique of bilinear aggregate signature to extend our main result into a multi-user setting, where TPA can perform multiple auditing tasks simultaneously. Extensive security and performance analysis shows the proposed schemes are provably secure and highly efficient.

2.4. COMPUTING ENCRYPTED CLOUD DATA EFFICIENTLY UNDER MULTIPLE KEYS

The emergence of cloud computing brings users abundant opportunities to utilize the power of cloud to perform computation on data contributed by multiple users. These cloud data should be encrypted under multiple keys due to privacy concerns. However, existing secure computation techniques are either limited to single key or still far from practical. In this paper, we design two efficient schemes for secure outsourced computation over cloud data encrypted under multiple keys. Our schemes employ two non-colluding cloud servers to jointly compute polynomial functions over multiple users' encrypted cloud data without learning the inputs, intermediate or final results, and require only minimal interactions between the two cloud servers but not the users. We demonstrate our schemes' efficiency experimentally via applications in machine learning. Our schemes are also applicable to privacy-preserving data aggregation such as in smart metering.

2.5. ACHIEVING SECURE, SCALABLE, AND FINE-GRAINED DATA ACCESS CONTROL IN CLOUD COMPUTING

Cloud computing is an emerging computing paradigm in which resources of the computing infrastructure are provided as services over the Internet. As promising as it is, this paradigm also brings forth many new challenges for

data security and access control when users outsource sensitive data for sharing on cloud servers, which are not within the same trusted domain as data owners. To keep sensitive user data confidential against untrusted servers, existing solutions usually apply cryptographic methods by disclosing data decryption keys only to authorized users. However, in doing so, these solutions inevitably introduce a heavy computation overhead on the data owner for key distribution and data management when fine-grained data access control is desired, and thus do not scale well. The problem of simultaneously achieving fine-grainedness, scalability, and data confidentiality of access control actually still remains unresolved. This paper addresses this challenging open issue by, on one hand, defining and enforcing access policies based on data attributes, and, on the other hand, allowing the data owner to delegate most of the computation tasks involved in fine-grained data access control to untrusted cloud servers without disclosing the underlying data contents. We achieve this goal by exploiting and uniquely combining techniques of attribute-based encryption (ABE), proxy re-encryption, and lazy re-encryption. Our proposed scheme also has salient properties of user access privilege confidentiality and user secret key accountability. Extensive analysis shows that our proposed scheme is highly efficient and provably secures under existing security models.

EXISTING SYSTEM:

Kallahalla et al presented a cryptographic storage system that enables secure data sharing on untrustworthy servers based on the techniques that dividing files into file groups and encrypting each file group with a file-block key.

Yu et al exploited and combined techniques of key policy attribute-based encryption, proxy re-encryption and lazy re-encryption to achieve fine-grained data access control without disclosing data contents.

DISADVANTAGES OF EXISTING SYSTEM

- The file-block keys need to be updated and distributed for a user revocation; therefore, the system had a heavy key distribution overhead.
- The complexities of user participation and revocation in these schemes are linearly increasing with the number of data owners and the revoked users.
- The single-owner manner may hinder the implementation of applications, where any member in the group can use the cloud service to store and share data files with others.

PROPOSED SYSTEM

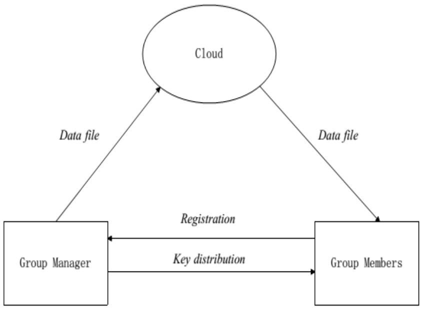
- In this paper, we propose a secure data sharing scheme, which can achieve secure key distribution and data sharing for dynamic group.
- We provide a secure way for key distribution without any secure communication channels. The users can securely obtain their private keys from group manager without any Certificate Authorities due to the verification for the public key of the user.
- Our scheme can achieve fine-grained access control, with the help of the group user list, any user in the group can use the source in the cloud and revoked users cannot access the cloud again after they are revoked.
- We propose a secure data sharing scheme which can be protected from collusion attack. The revoked users can not be able to get the original data files once they are revoked even if they conspire with the untrusted cloud. Our scheme can achieve secure user revocation with the help of polynomial function.
- Our scheme is able to support dynamic groups efficiently, when a new user joins in the group or a user is revoked from the group, the private keys of the other users do not need to be recomputed and updated.
- We provide security analysis to prove the security of our scheme.

ADVANTAGES OF PROPOSED SYSTEM

- The computation cost is irrelevant to the number of revoked users in RBAC scheme. The reason is that no matter how many users are revoked, the operations for members to decrypt the data files almost remain the same.

- The cost is irrelevant to the number of the revoked users. The reason is that the computation cost of the cloud for file upload in our scheme consists of two verifications for signature, which is irrelevant to the number of the revoked users. The reason for the small computation cost of the cloud in the phase of file upload in RBAC scheme is that the verifications between communication entities are not concerned in this scheme.
- In our scheme, the users can securely obtain their private keys from group manager Certificate Authorities and secure communication channels. Also, our scheme is able to support dynamic groups efficiently, when a new user joins in the group or a user is revoked from the group, the private keys of the other users do not need to be recomputed and updated.

3. SYSTEM ARCHITECTURE



4. IMPLEMENTATION:

Implementation is a phase where the design of the project is turned into the running system. Here we are developing the working system to the user. It is very important phase in the software development. In this phase only we are implementing the software or system and give it to the user. So the new system should work effectively. The design and implementation of our proposed system is developed as follows.

CLOUD MODULE:

In this module, we create a local Cloud and provide priced abundant storage services. The users can upload their data in the cloud. We develop this module, where the cloud storage can be made secure. However, the cloud is not fully trusted by users since the CSPs are very likely to be outside of the cloud users' trusted domain. Similar to we assume that the cloud server is honest but curious. That is, the cloud server will not maliciously delete or modify user data due to the protection of data auditing schemes, but will try to learn the content of the stored data and the identities of cloud users.

GROUP MANAGER MODULE:

Group manager takes charge of followings:

- System parameters generation,
- User registration,
- User revocation, and

- Revealing the real identity of a dispute data owner.

Therefore, we assume that the group manager is fully trusted by the other parties. The Group manager is the admin. The group manager has the logs of each and every process in the cloud. The group manager is responsible for user registration and also user revocation too.

GROUP MEMBER MODULE:

Group members are a set of registered users that will

- Store their private data into the cloud server and
- Share them with others in the group.

Note that, the group membership is dynamically changed, due to the staff resignation and new employee participation in the company. The group member has the ownership of changing the files in the group. Whoever in the group can view the files which are uploaded in their group and also modify it.

FILE SECURITY MODULE:

- Encrypting the data file.
- File stored in the cloud can be deleted by either the group manager or the data owner. (i.e., the member who uploaded the file into the server).

GROUP SIGNATURE MODULE:

A group signature scheme allows any member of the group to sign messages while keeping the identity secret from verifiers. Besides, the designated group manager can reveal the identity of the signature's originator when a dispute occurs, which is denoted as traceability.

USER REVOCATION MODULE:

User revocation is performed by the group manager via a public available revocation list (RL), based on which group members can encrypt their data files and ensure the confidentiality against the revoked users.

5. CONCLUSION:

In this document, we have designed a secure data exchange scheme for collusion for dynamic groups in the cloud. In our schema, users can safely secure their private keys from the Certified Authority Administrator group and secure communication channels. In addition, our schema can efficiently support dynamic groups when a new user joins the group or a user is revoked by the group, the private keys of other users should not be recalculated and updated. Additionally, our schema may get the user's safe revocation, revoked users can not get the original data files when they are revoked, even if they conspire with the untrusted cloud.

6. REFERENCES

1. M.Armbrust, A.Fox, R.Griffith, A.D.Joseph, R.Katz,A.Konwinski, G. Lee, D.Patterson, A.Rabkin, I.Stoica, andM.Zaharia. "A View of

Cloud Computing,"Comm. ACM, vol. 53,no.4, pp.50-58, Apr.2010.

2. S.Kamara and K.Lauter,"Cryptographic Cloud Storage," Proc.Int'l Conf. Financial Cryptography and Data Security (FC), pp.136-149, Jan. 2010.
3. M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K.Fu,"Plutus: Scalable Secure File Sharing on Untrusted Storage," Proc.USENIX Conf. File and Storage Technologies, pp. 29-42, 2003.
4. E.Goh, H. Shacham, N. Modadugu, and D. Boneh, "Sirius: Securing Remote Untrusted Storage," Proc. Network and DistributedSystems Security Symp. (NDSS), pp. 131-145, 2003.
5. G. Ateniese, K. Fu, M. Green, and S. Hohenberger,"Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage," Proc. Network and Distributed Systems SecuritySymp. (NDSS), pp. 29-43, 2005.
6. Shucheng Yu, Cong Wang, Kui Ren, and Weijing Lou, "Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing," Proc. ACM Symp. Information, Computer and Comm. Security, pp. 282-292, 2010.
7. V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data," Proc. ACM Conf. Computer and Comm. Security (CCS), pp. 89-98, 2006
8. R. Lu, X. Lin, X. Liang, and X. Shen, "Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing,"