Secure Data in cloud computing using encryption algorithms

Laxmikant S. Bhattad , Prof.P. P. Deshmukh
PG Scholar Department of computer science and engineering Amravati, Maharashtra India
Professor Department of computer science and engineering Amravati, Maharashtra India

Abstract-

Cloud computing paradigm enables the users to access the outsourced data from the cloud server without the hardware and software management. With the character of low maintenance, cloud computing provides an economical and efficient solution for sharing group resource among cloud users. In order to address this problem, we proposed an efficient data security method using cryptographic techniques. Thus, the proposed method not only encrypts the sensitive data, but also detects the dishonest party to access the data using combined hash functions. Unfortunately, sharing data in a multi-owner manner while preserving data and identity privacy from an un-trusted cloud is still a challenging issue, due to the frequent change of the membership.

For the effective utilization of sensitive data from CSP, the data owner encrypts before outsourcing to the cloud server. To protect data in cloud, data privacy is the challenging task. We have analyzed the proposed method in terms of storage, communication and computational overheads. The result shows that the proposed security method is more efficient than the existing security system.

Keywords— Cloud Computing, Data Control, Data Sharing, Privacy Preserving, Verification, Access Control, Encryption, Decryption, Data Storage and Data Privacy,

1. INTRODUCTION

Cloud computing is a flexible, cost- effective and proven delivery platform for providing business or consumer IT services over the Internet. Cloud computing supports distributed service oriented architecture, multi-users and multi-domain administrative infrastructure, it is more prone to security threats and vulnerabilities. At present, a major concern in cloud adoption is its security and Privacy. Cloud computing is recognized as an alternative to traditional information technology due to its intrinsic resource-sharing and low-maintenance characteristics. In cloud computing, the cloud service providers (CSPs), such as online shopping sites, are able to deliver various services to cloud users with the help of powerful datacenters. Intrusion prospects within cloud environment are many and with high gains. Security and Privacy issues are of more concern to cloud service providers who are actually hosting the services. In most cases, the provider must guarantee that their infrastructure is secure and clients' data and applications are safe by implementing Security policies and mechanisms. By migrating the local data management systems into cloud servers, users can enjoy high-quality services and save significant investments on their local infrastructures.

We propose a secure multi-owner data sharing scheme. It implies that any user in the group can securely share data with others by the untrusted cloud. Our proposed scheme is able to support dynamic groups efficiently. Specifically, new granted users can directly decrypt data files uploaded before their participation without contacting with data owners. User revocation can be easily achieved through a novel revocation list without updating the secret keys of the remaining users. The size and computation overhead of encryption are constant and independent with the number of revoked users. We provide secure and privacy-preserving access control to users, which guarantees any member in a group to anonymously utilize the cloud resource. Moreover, the real identities of data owners can be revealed by the group manager when disputes occur. We provide rigorous security analysis, and perform extensive simulations to demonstrate the efficiency of our scheme in terms of storage and computation overhead. One of the most fundamental services offered by cloud providers is data storage. Let us consider a practical data application. A company allows its staffs in the same group or department to store and share files in the cloud. By utilizing the cloud, the staffs can be completely released from the troublesome local data storage and maintenance.

Cloud computing, data is stored in remote massively scalable data centers where compute resources can be dynamically shared to achieve significant economies of scale. The storage capacity needs to scale with compute resources to effectively manage and gain maximum cloud benefits. It has the following common characteristics; (i) Pay-per-use (ii) Elastic capacity (iii) Self-service interface and (iv) Resources that are abstracted or virtualized.

2. BACKGROUND

2.1 Cloud Deployment Models

There are three types cloud Deployment models that widely used are:

2.1.1Public:

It is referred as external cloud or multi-tenant cloud, this model represents an openly accessible cloud environment in this cloud can be accessed by general public. Customer can access resources and pay for the operating resources. Public

Cloud can host individual services as well as collection of services

2.1.2Private:

It is also known as internal cloud or on-premise cloud, a private cloud provides a limited access to its resources and services to consumers that belong to the same organization that owns the cloud. In other words, the infrastructure that is managed and operated for one organization only, so that a consistent level of control over security, privacy, and governance can be maintained.

2.1.3Hybrid:

A hybrid cloud is a combination of public and private cloud. It provides benefit of multiple deployment models. It enables the enterprise to manage steady-state work load in the private cloud, and if the workload increases asking the public cloud for intensive computing resources, then return if no longer needed.

3. ISSUES IN CLOUD DATA STORAGE AND SECURITY

Cloud Computing moves the application software and databases to the large data centers, where the management of the data and services may not be fully trustworthy. This unique attribute, however, poses many new security challenges which have not been well understood. In this article, we focus on cloud data storage security, which has always been an important aspect of quality of service to ensure the correctness of user data in the cloud.

3.1 Trust: Trust is defined as reliance on the integrity, strength, ability and surety of a person or thing. Entrusting your data on to a third party who is providing cloud services is an issue. Recent incidents like In April of 2012 Amazon's Elastic Compute Cloud service crashed during a system upgrade, knocking customers' websites off-line for anywhere from several hours to several days. That same month, hackers broke into the Sony PlayStation Network, exposing the personal information of 77 million people around the world. And in June a software glitch at cloud-storage provider Drop box temporarily allowed visitors to log in to any of its 25 million customers' accounts using any password or none at all.

3.2 Privacy: Different from the traditional computing model, cloud computing utilizes the virtual computing technology, users' personal data may be scattered in various virtual data center rather than stay in the same physical location, even across the national borders, at this time, data privacy protection will face the controversy of different legal systems. On the other hand, users may leak hidden information when they accessing cloud computing services. Attackers can analyze the critical task depend on the computing task submitted by the user.

3.3 Security: Cloud service providers employ data storage and transmission encryption, user authentication, and authorization. Many clients worry about the vulnerability of remote data to criminals and hackers. Cloud providers are enormously sensitive to this issue and apply substantial resources to mitigate this problem.

3.4 Ownership: Once data has been relegated to the cloud, some worry about losing their rights or being unable to protect the rights of their customers. Many cloud providers address this issue with well-skilled user-sided agreements. According to the agreement, users would be wise to seek advice from their favorite's legal representation

3.5 Performance and Availability: Business organizations are worried about acceptable levels of performance and availability of applications hosted in the cloud.

3.6 Legal: There are certain apprehensions for a cloud service provider and a client receiving the service like location of the cloud provider, infrastructure and physical location of the data and outsourcing of the cloud provider's services etc.

3.7 Multiplatform Support: More an issue for IT departments using managed services is how the cloud based service integrates across different platforms and operating systems, e.g. OS X, Windows, Linux and thin clients. Usually, some customized adaption of the service takes care of any problem. Multiplatform support requirements will ease as more user interfaces become web-based.

3.8 Intellectual Property: A company invents something new and it uses cloud services as part of the invention. Is the invention still patentable? Or there can be issues like cloud service provider can make claim for that invention or leak the information to the competitor.

3.9 Data Backup: Cloud providers employ redundant servers and routine data backup processes, but some people worry about being able to control their own backups. Many providers are now offering data dumps onto media or allowing users to back up data through regular downloads.

3.10 Data Portability and Conversion: Some people have concerns like, switching service providers; there may be difficulty in transferring data. Porting and converting data is highly dependent on the nature of the cloud provider data retrieval format, particular in cases where the format cannot be easily revealed.

Worst case, a cloud subscriber will have to pay for some custom data conversion. These are certain areas in which cloud computing requires to excel and solve problem related to it. Out of all the problems Security, Privacy and Intellectual property put the major threats on growth of cloud computing that are needed to be worked upon.

4. RELATED WORK

In data sharing system is defining of access policies and dynamic data updating. In Junbeom Hur, explains the cryptographic based solution for data sharing using cipher-text policy attribute-based encryption to improve the security of the data. In this method the data owners defines the access policies on the data to be distributed. The major drawback of this method is the unauthorized users can access the key to decrypt the encrypted data. The first and straight forward solution to ensure the data integrity is, the data owner pre-compute the MACs for the entire file with a set of secrete keys, before our sourcing data to cloud server. During auditing process, for each time the data owner reveals the secret key to the cloud server and ask for new MAC for verification. In this method the number of verification is restricted to the number of secrete keys. Once the keys are exhausted, the data owner has to retrieve the entire file from the cloud server to compute the new MACs for the remaining blocks. This method takes the huge number of communication overhead for verification of entire file, which effect the system efficiency.

Another solution to overcome the drawback of previous method is to generate the signatures for every block instead of MACs to obtain the public audit-ability. This solution can provide probabilistic assurance of data correctness and public audit-ability, which again results in large communication overhead and effect the system efficiency. The above solutions are supports only static data and none of them can deal with the dynamic data updates. In cloud computing, both data and applications are controlled by the data owner and cloud service provider. In this security model, it provides a single default gateway as a platform to secure user data across public cloud applications. The default gateway encrypts only sensitive data using encryption algorithm, before sending in to the cloud server. In this method the data is accessed by only authorized users but the cloud service provider can grant the access permission for unauthorized users while cheating to the data owner. Therefore, this method degrades the security as proper key management is not implemented in the system.

4.1 Software as a service.

Software-as-a-Service (SaaS): It is also referred as Software available on demand; it is based on multi-tenant Architecture. Software like word processor, CRM (Customer Relation Management), etc. or application Services like schedule, calendar, etc. are executed in the "Cloud" using the interconnectivity of the internet to do Manipulation on data. Custom services are combined with3rd party commercial services via Service oriented Architecture to create new applications. It is a software Delivery for business applications like accounting, content delivery, Human resource management (HRM), Enterprise Resource planning (ERP) etc. on demand on pay-as-you go, users exercise the service provider's already-deployed applications, which are hosted on a cloud infrastructure. The applications are accessible from client devices through a thin client interface, such as a Web browser (e.g., Web-based email).

4.2 Platform as a Service.

Platform-as-a-Service (PaaS): This layer of cloud provides computing platform and solution stack as service**.** Platform-as-a-Service provides the user with the freedom of application design, application development, testing, deployment and hosting as well as application services such as team collaboration, web service integration and database integration, security, scalability, storage, persistence, state management, application versioning, without thinking about the underlying hardware and software layers by providing facilities required for completion of project through web application and services via Internet users are enabled to deploy user-created or acquired applications created using programming languages and tools onto the cloud infrastructure supported by the cloud service provider

4.3 Infrastructure as a Service.

Infrastructure as a Service (IaaS): Infrastructure as a service delivers a platform virtualization environment as a service. Instead of purchasing servers, software, datacenter space or network equipment, clients can buy these resources as outsourced service. In other words the client uses the third party infrastructure services to support its operations including hardware, storage, and server's networking component users are allowed to provision processing, storage, networks, and other fundamental computing resources. Multiple VMs running guests and specific application software can be deployed.

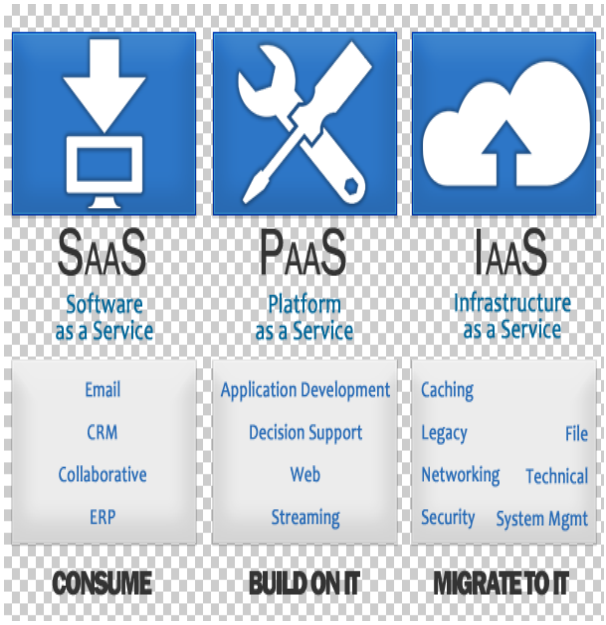

Fig1:1 Cloud Computing Framework

4.1 Algorithm for Revocation Verification:

Input: System parameter (H0,H1,H2), a group signature alpha, and a set of revocation keys A1,…..Ar
Output: Valid or Invalid.
Begin
set temp=e(T1,H1)e(T2,H2)
for i=1 to n
if e(T3 - Ai, H0) = temp
Return Valid
end if
end for
Return Invalid
end

5. CONCLUSIONS

To control the outsourced data and provide the quality of the cloud storage service for the users, we propose an efficient data encryption, data decryption, key rotation and cryptographic hash function techniques. To detect the dishonest party we implemented the verification techniques using hash function at TTP. We have investigated the computation overhead, communication overhead and storage overhead for the outsourced data. The simulation result for accessing the outsourced data from the CSP shows that the proposed cloud security system is highly secure than the existing security systems. To support, insertion, deletion and updation dynamic operations on encrypted data block, we can further extend this security system. More specially, efficient user revocation can be achieved through a public revocation list without updating the private keys of the remaining users, and new users can directly decrypt files stored in the cloud before their participation. Moreover, the storage overhead and the encryption computation cost are constant.

REFERENCES

[1] Xuefeng Liu, Yuqing Zhang, Member, IEEE, Boyang Wang, and Jingbo Yan Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 24, NO. 6, JUNE 2013.

[2] 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," Comm. ACM, vol. 53, no. 4, pp. 50-58, Apr. 2010.

[3] S. Kumaraand K.Later, "Cryptographic Cloud Storage," Proc. Int'l Conf. Financial Cryptography and Data Security (FC), pp. 136- 149, Jan. 2010.

[4] Prakash G L, Dr. Manish Prateek, and Dr. Inder Singh, "Data Security Algorithms for Cloud Storage System using Cryptographic Method", International Journal of Scientific & Engineering Research, Volume 5, Issue 3, March -2014.

[5] S. Yu, C. Wang, K.Ran, and W. Lou, "Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing, "Prow. IEEE INFOCOM, pp. 534-542, 2010.

[6] Rich Marginal, solaria communication. "Cloud computing is changing how we communicate".

[7] Randolph Barr, Quay's Inc., "How to gain comfort in losing control to the cloud".

[8] Greg Boss, Padma Malady, Dennis Quinn, Linda Ledgering, Harold Hall, HI PODS, developer works/web sphere/zones/hippos.

[9] Thrum Dillon, Chen Wu, Elizabeth Chang, 2010 24th IEEE International Conference on Advanced Information Networking and Applications,"Cloud computing: issues and challenges".

[10] Schadt, E. E., Linderman, M. D., Sorenson, J., Lee, L., and Nolan, G. P. Computational solutions to large-scale data management and analysis, Nature Reviews Genetics, Vol. 11, 647–657. doi:10.1038/nrg2857

[11] Schaffer, H. X as a service, cloud computing, and the need for good judgment. IT Professional, Vol. 11, 5 (2009).

[12] B. Liu, Y. Chen, A. Hades, Department of Electrical and Computer Engineering, Binghamton University, SUNY, Binghamton,

[13] Book written by William stalling, AES, Chapter 5, Chapter4, in cryptography and network security.