

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Special Issue 6, May 2015

Dynamic Auditing for Data Verification and Cloud Storages

N. Hariharan Kumar

P.G Student, Department of CSE, P. A. College of Engineering and Technology, Pollachi, India

ABSTRACT: Cloud computing is an ondemand service where customer can access various computer resources with internet. Unlucky reliability of cloud data is subject to uncertainty due to infrastructure breakup problem and possible of human errors. Various systems has been designed to protect the cloud data to ensure data security. Cloud service provider may hide the data leakages due to customer Satisfaction. Third Party Auditor validates the cloud customer information and ensures data integrity. Traceability is the major problem occurs over the cloud audit mechanism. We propose the cloud audit methodology for cloud data security with encrypted data with efficient cloud security.

KEYWORDS: Cloud computing; encryption and decryption data protection and integrity.

I. INTRODUCTION

Cloud computing is computing used in large groups of remote servers is networked to allow centralized data storage and online access to computer services or resources. Clouds can be classified as public, private or hybrid. The criticisms about it are mainly focused on its social implications and happens to the owner of remote servers is a person or organization user as their interests may point in different directions, the user may wish the shared information is kept private as the owner of the remote servers may take advantage of it for own business. The characteristics of cloud computing include on-demand self service, broad network access, resource pooling, rapid elasticity and measured service. On-demand self service means customers will request and manage their computing resources. Broad network access allows services to be offered over the Internet and private networks. Customers draw from a pool of computing resources, usually in remote data centers. Services will be scaled larger and smaller, and use of a service is measured and customers are billed accordingly.

Cloud computing contains the following key characteristics

1. Agility improves with user's ability to provision technological infrastructure resources.
2. Application Programming Interface (API) accessibility to software to enables machines to interact with cloud software in the same way on traditional user interface facilitates interaction between computers and humans[1]. Cloud computing service normally use REpresentational State Transfer (REST) based APIs.
3. Cost reductions claimed by cloud providers. A public cloud deployment model changes the capital expenditure to operational expenditure. Pricing on the cloud computing is usage based on hourly and also resource utilized. Less computer maintenance knowledge needed for cloud deployments. The cloud repository contains various articles depends on detailed cost aspects. Resource based and module based service also available in cloud service model. It concludes the costs savings depend on the type of activities supported and the model of infrastructure availability.
4. Device and location independence enable users to access systems using a web browser regardless of their location and device use. Infrastructure is provided by a third-party and accessed with the internet, users can connect from anywhere in the world.
5. Maintenance of cloud computing applications is flexible, no need installed on each cloud user's computer and accessed from different places using the internet.
6. Peak-load capacity increase users and the cloud engineers not needed for highest possible load-levels.
7. Utilization and efficiency improvements for systems are often utilized 10 to 20% only.
8. Performance is monitored and consistent and loosely coupled architectures are constructed using web services as the system interface.

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Special Issue 6, May 2015

9. Reliability improves with the use of multiple redundant sites, which makes well designed cloud computing suitable for business continuity and disaster recovery.

10. Scalability and elasticity performed with dynamic provisioning of resources on a fine-grained.

11. Security can improve due to centralization of data, increased security-focused resources. The concerns persist about loss of control over certain sensitive data and the lack of security for stored kernels. Security is often as good as better than other traditional systems in part because providers are able to devote resources to solving security issues. Complexity is greatly increased once data is distributed over a wider area and over a greater systems shared by unrelated users, access to security audit logs is impossible. Private cloud installations are in part motivated by user's desire to retain control over the infrastructure and avoid losing control of information security.

The National Institute of Standards and Technology's definition of cloud computing identifies five essential characteristics:

1. On-demand self-service consumer will unilaterally provision computing capabilities, such as server time and network storage as needed automatically interaction with each service provider.
2. Broad network access capabilities are available over the network and accessed through standard mechanisms to promote use by heterogeneous thin and thick client platforms.
3. Resource pooling the resources is pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand.
4. Rapid elasticity capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. the consumer and capabilities available for provisioning often appear unlimited and will be appropriated in any quantity at any time.
5. 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 storage. Resource usage are monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service. Backup should be taken regularly.

The cloud computing service models are:

1. Software as a Service (SaaS)
2. Platform as a Service (PaaS)
3. Infrastructure as a Service (IaaS)

In Software as a Service (SaaS) model, a pre-made application, along with any required software, operating system, hardware and network are provided. In Platform as a Service (PaaS) an operating system, hardware, and network are provided, and the customer installs and develops its own software and applications.

The Infrastructure as a Service (IaaS) model provides just the hardware and network the customer installs and develops its own operating systems, software and applications.

Various cloud deployment services are typically made available in a different types of cloud services. In public cloud services provided by a public cloud are offered over the Internet and are owned and operated by a cloud provider. Some examples include services aimed at the general public, such as online photo storage services, e-mail services and social networking sites. Services for enterprises are also being offered in a public cloud.

Private cloud infrastructure is operated solely for a specific organization, and is managed by the organization and a third party. In a community cloud, the service is shared by several organizations and made available only to those groups.

Hybrid cloud contains a combination of different methods of resource pooling. It is a combination of both public and private cloud. Cloud services are popular because cloud can reduce the cost and complexity of owning and operating computers and networks. Since cloud users no need to invest in information technology infrastructure, purchase hardware, and buy software licenses, the benefits are low up-front costs, rapid return on investment, rapid deployment, customization, flexible use, and solutions can make use of new innovations.

II. SURVEY ON CLOUD

Powerful auditing mechanisms must always supplement the cloud application. Various approaches to preserve privacy at the time of public auditing methods analyzed in the chapter[2],[6]. All these approaches would preserve the

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Special Issue 6, May 2015

privacy of user and data and while performing public auditing on the cloud. Analyzing of various security audit mechanism would serve as a helping note in the progress of strengthening the dynamic audit for shared data verification and data storages in cloud. Q.Wang [3]. Describes the enabling public verifiability and data dynamics for storage security in cloud computing. The technique ensures the integrity of data storage in Cloud Computing and considers the task of allowing a Third Party Auditor (TPA), on behalf of the cloud client to verify the integrity of the dynamic data stored in the cloud. The introduction of TPA eliminates the involvement of client through the auditing of whether his data stored in the cloud is indeed intact can be important in achieving economies of scale for Cloud Computing. The support for data dynamics via the most general forms of data operation, such as block modification, insertion and deletion, is also a significant step toward practicality, since services in Cloud Computing are not limited to archive or backup data only. K.Ren [8]. Defines the public auditability for cloud storage is of critical importance so users can resort to a Third Party Auditor (TPA) to check the integrity of outsourced data and be worry-free. Securely introduce an effective TPA, the auditing process should bring in no new vulnerabilities towards user data privacy, and introduce no additional online burden to user. Secure cloud storage system supporting privacy-preserving public auditing and extend the result to enable TPA to perform audits for multiple users simultaneously and efficiently. Extensive security and performance analysis show the schemes are provably secure and highly efficient.Y.Zhu [7].Derived a dynamic audit service for verifying the integrity of untrusted and outsourced storage. Audit service constructed based on the techniques, fragment structure, random sampling and index-hash table [9].

III. DYNAMIC AUDITING FOR SHARED DATA VERIFICATION AND STORAGES IN CLOUD

In dynamic auditing for shared data, privacy is accomplished by allowing the parties to upload their data in multi clouds and data is split into multiple parts so it gives more protection. Two kinds of threats related to the integrity of shared data are possible. First, an adversary may try to corrupt the integrity of shared data. Second, the cloud service provider may inadvertently corrupt or even remove data in its storage due to hardware failures and human errors. The public verifier may reveal the identity of the signer on each block.Integrity of data cannot be proved during the process of auditing, a public verifier allowed to verify the correctness of shared data integrity, may try to reveal the identity of the signer on each block in shared data based on verification metadata. Data correctness is the main objective of the cloud auditing mechanism Authenticated file system. Third Party Audit (TPA) is able to verify the integrity of shared data for users without retrieving the entire data. Meanwhile, the identity of the signer on each block in shared data kept private from the TPA. Multiple auditing tasks simultaneously performed by TPA instead of verifying one by one.Dynamic auditing for shared data verification is simple and efficient approach. To ensure cloud data integrity without sacrificing the anonymity of data owners requires significant verification metadata. SEcurity Mediator (SEM). It decouples the anonymity protection mechanism from the Provable Data Possession (PDP). Organization can employ its own anonymous authentication mechanism, and the cloud is oblivious to that since it only deals with typical PDP metadata and no extra storage overhead.

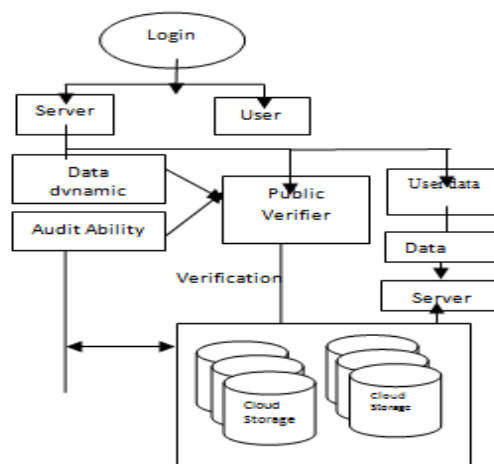


Figure 1 Dataflow Diagram

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Special Issue 6, May 2015

Figure 1 explains about the data flow diagram of our auditing mechanisms. Cloud server stores the data. User has to login as individual user or group user for storing and auditing data. Public verifier is the responsible for manage and monitor the data changes in the Cloud Storage. User data modification is stored in the log file of the cloud server with date and time.

B. BLIND RSA ALGORITHM

RSA is one of the public-key cryptosystems and is widely used for secure data transmission. In such a cryptosystem, the encryption key is public and differs from the decryption key that will be kept secret. In RSA, this asymmetry is based on the factoring the product of two large prime numbers. RSA stands for Ron Rivest, Adi Shamir and Leonard Adleman, first publicly described the algorithm in 1977. The BLIND RSA algorithm involves three steps: key generation, encryption and decryption.

C. KEY GENERATION

RSA involves a public key and a private key. The public key can be known by everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted in a reasonable amount of time using the private key. The keys for the RSA algorithm are generated the following way:

1. Generate two large random and distinct primes and each roughly the same size.
2. For security purposes, the integers p and q should be chosen at random, and should be of similar bit-length.
3. Compute $n = pq$.
 n is used as the modulus for both the public and private keys. Its length, usually expressed in bits, is the key length.
4. Compute $\phi(n) = \phi(p)\phi(q) = (p - 1)(q - 1) = n - (p + q - 1)$, where ϕ is Euler's totient function.
5. Choose an integer e such that $1 < e < \phi(n)$ and $\gcd(e, \phi(n)) = 1$. The e and $\phi(n)$ are co prime.
 e is released as the public key exponent.
6. Determine d as $d \equiv e^{-1} \pmod{\phi(n)}$.
 d is kept as the private key exponent.

The public key consists of the modulus n and the exponent e . The private key consists of the modulus n and the exponent d that must be kept secret. p , q , and $\phi(n)$ must also be kept secret and used to calculate d .

The user computes the cipher text c for message using encryption key e corresponding to $c = m^e \pmod{n}$. The m is the original message and e is used as encryption key and n is the prime integer. The c is the cipher text obtained. This cipher text is sent to others in encrypted manner.

The user who has the decryption key can decrypt the cipher text corresponding to formula $m = c^d \pmod{n}$. The d is decryption key, c is the cipher text and n is the prime integer chosen at random. The original message m has been recovered.

IV. DYNAMIC AUDITING FOR CLOUD DATA

A. ADVANCED ENCRYPTION STANDARD

Advanced Encryption Standard (AES) algorithm is not only for security but also for fast in action. Both hardware and software implementation are faster by performance. New encryption standard recommended by NIST to replace DES. Encrypts data blocks of 128 bits in 10, 12 and 14 round depending on key size. It can be implemented on various platforms especially in small devices. It is carefully validated for many security applications.

B. METHODOLOGY

Step 1: Define the set of round keys from the cipher key.

Step 2: Initialize the first state array with the plaintext block data.

Step 3: Add the initial round key to the starting state array.

Step 4: Perform the nine rounds of state manipulation.

Step 5: Perform the tenth and final round of state manipulation.

Step 6: Finally copy the end state array out as the encrypted data (cipher text).

Each round of the encryption process requires a series of

steps to alter the state of array. These steps involve four types of operations. They are

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Special Issue 6, May 2015

Sub Bytes : This operation is a simple substitution that converts every bite into a different value.

ShiftRows : Each row is rotated to the right by a certain number of bytes.

MixColumns : Each column of the state array is processed separately to produce a new column. The new column replaces the old one.

XorRoundKey : This operation simply takes the existing state array, **Decryption**: Decryption involves reversing the steps for the encryption using inverse functions like *InvSubBytes* , *InvShiftRows* , *InvMixColumns*.

V. RESULTS AND DISCUSSION

In our model, privacy is accomplished by allowing the parties to upload their data in multiple clouds and data is split into multiple parts so it gives more protection. Two kinds of threats are possible in the integrity of shared data. An adversary has chance to corrupt the integrity of shared data. The cloud service provider inadvertently corrupts the data on the storage due to hardware failures and human mistakes. The public verifier may reveal the identity of the signer on each block.

Integrity of data should not be proved during the process of auditing, a public verifier is only person allowed to verify the correctness of shared data integrity, may try to show the identity of the signer on each block in shared data based on verified data.

To prove data freshness and the cloud possesses the latest version of shared data while still preserving identity privacy. Dynamic changes over the data in cloud server will be sent the public verifier when changes occur.

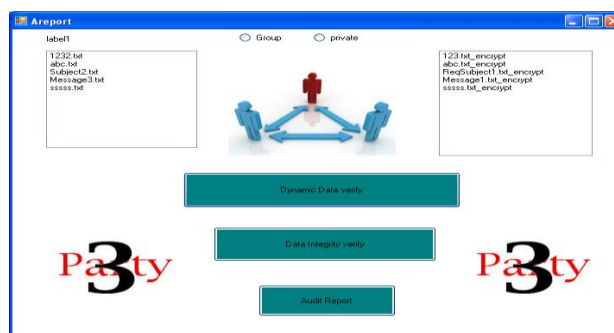


Figure 2 Shows the dynamic data verification form.

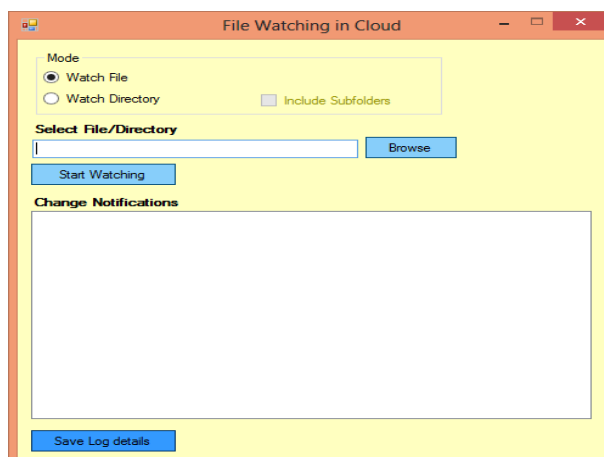


Figure 3 shows the traceability form for cloud users .

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Special Issue 6, May 2015

VI. CONCLUSION

We propose privacy preserving dynamic public auditing system for data storage in cloud computing. The AES algorithm provides the high security in the cloud storage data. Third Party Auditor performs dynamic auditing tasks automatically with modified date time and the system. Our proposed method shows that the cloud storage system is high secure and efficient.

REFERENCES

- [1]. Armburst.M et al (2013), 'A view of cloud computing', Comm. ACM, vol. 53, no. 4, pp. 50-58.
- [2]. Ateniese.G, Burns.R ,Curtmola.R, Herring.J, Kissner,L et al.(2007), 'Provable data possession at untrusted stores', Proc 14th ACM conf Computer and Comm.Security (CCS'09), pp 598-610.
- [3]. Cao.N,Yu.S,Yang et al. (2012), 'LT Codes-Based Secure and Reliable Cloud Storage services', Proc IEEE INFO-COM , pp 60-67
- [4]. Chen.B,Curtmola.R,Atiiese.G and Burns.R (2010), 'Remote Data Checking for Network Coding Based Distributed Storage Systems', Proc ACM Workshop Cloud Computing Security Workshop (CCW'10),pp 31-42.
- [5]. Li.M,Chow S.S et al (2013), 'Computing Encrypted Cloud data efficiently under multiple keys', Proc IEEE congComm and Network security(CNS 13) pp 90-99.
- [6]. Ren.K ,Wang.C and Wang.Q (2012), 'Security challenges for the Public Cloud', IEEE internet computing vol. 16, pp. 69-73.
- [7]. Rivest.R, Shamir.A et al. (1978), 'A Method for obtaining Digital Signatures and Public key Cryptosystems', Comm.ACM, vol 21,no 2, pp 120-126.
- [8]. Song.D, Shi.E, Fischer.I, and Shankar.U (2012), 'Cloud Data Protection for the Masses Hierarchy', Computer vol. 45,no.1,pp. 39-45.
- [9]. Shacham.H and Waters.B(2008), 'Compact proofs of Retrievability', Proc 14thInt'l Conf.Theory and Application of Cryptography (ASIACRYPT 08) pp 90-107.
- [10]. Wang.B, H.Erway (2009), 'Privacy-Preserving Public Auditing for shared Cloud Data Kupcu.A, papamanthou.C, and Tamassia.R(2009)', Dynamic Provable Data Possession, Proc. 16th ACM Conf Computer Security (CCS'09), pp 213-222.
- [11]. Wang.B, Li.B, and Li.H (2013), 'Panda Public auditing for Shared Data with Efficient User Revocation in the Cloud', IEEE Trans Services Computing .
- [12]. Wang.B et al. (2012), 'Privacy-Preserving Public auditing for shared data in cloud', Proc. IEEE fifth international conference cloud computing, pp. 295-302.
- [13]. Wang.B,Li.B, and Li.H (2013), 'Certificateless Public Auditing for data integrity in the cloud', Proc IEEE ConfComm and Network Security(CNS'13) pp.276-284.
- [14]. Wang.C,Chow.S,Wang.Q,Ren.K (2013), 'Privacy-Preserving Public Auditing for secure Cloud Storage', IEEE Trans Computers, vol 62, no 2,pp 362-375.