International Journal of Web Technology
Volume: 03 Issue: 01 June 2014 Page No.19-21
ISSN: 2278-2389

Data Grid Privacy and Secure Storage Service in Cloud Computing

L.Revathi[1], S.Karthikeyan[2]
[1]Research Scholar, Department of Computer Applications, Dr. M.G.R. Educational and Research Institute University, Chennai
[2]Assistant Professor, Department of Computer Applications, Dr. M.G.R. Educational and Research Institute University, Chennai
Email: reddy.revathi24@gmail.com

Abstract-In cloud storage, users needs the data integrity protection in cloud computing task, especially for users with constrained computing resources. Thus, enabling public audit ability for cloud storage is of critical importance so that users can report to a third-party auditor (TPA) to check the integrity of outsourced data and be worry free .The data owner can share the space where his data are stored with other trusted people. Thus, users set the access rights with whom he/she wants to share the cloud space and that information will be forwarded to the TPA.[1] So, TPA on authentication or receiving the file access request, checks the user whether he is the real data owner or the user who has the rights to access the data. TPA lets these users to directly view the file and denies other users who try to access the file and pass the log report to the data owner. We use cryptographic techniques to securely store the data. We further have integrated RSA and TRIPLE DES algorithms for providing more security to the data. Thus the main objective we focused in this paper is providing privacy to the users and security to the data uploaded and stored by users in the cloud.

I. INTRODUCTION

In computernetworking,cloudcomputing is computing that involves a large number of computers connected through a communication network such as the Internet, similar to utility computing. In science, cloud computing is a synonym for distributed computing over a network, and means the ability to run a program or application on many connected computers at the same time. Network-based services, which appear to be provided by real server hardware and are in fact served up by virtual hardware simulated by software running on one or more real machines, are often called cloud computing. Such virtual servers do not physically exist and can therefore be moved around and scaled up or down on the fly without affecting the end user, somewhat like a cloud becoming larger or smaller without being a physical object. In common usage, the term "the cloud" is essentially a meaph or for the Internet. Marketers have further popularized the phrase "in the cloud" to refer to software, platforms and infrastructure that are sold "as a service. Typically, the seller has actual energy-consuming servers which host products and services from a remote location. Besides, it is often insufficient to detect the data corruption only when accessing the data, as it does not give users correctness assurance for those accessed data and might be too late to recovery.

II. RELATED WORK

Cloud computing is the long dreamed vision of computing as a utility, where data owners can remotely store their data in the cloud to enjoy on-demand high-quality applications and services from a shared pool of configurable computing resources.[2] While data outsourcing relieves the owners of the burden of local data storage and maintenance, it also eliminates their physical control of storage dependability and security, which traditionally has been expected by both enterprises and individuals with high service-level requirements. In order to facilitate rapid deployment of cloud data storage service and regain security assurances with outsourced data dependability, efficient methods that enable on-demand data correctness verification on behalf of cloud data owners have to be designed. In this article we propose that publicly auditable cloud data storage is able to help this nascent cloud economy become fully established. With public auditability, a trusted entity with expertise and capabilities data owners do not possess can be delegated as an external audit party to assess the risk of outsourced data when needed. Such an auditing service not only helps save data owners¿ computation resources but also provides a transparent yet cost-effective method for data owners to gain trust in the cloud. We describe approaches and system requirements that should be brought into consideration, and outline challenges that need to be resolved for such a publicly auditable secure cloud storage service to become a reality. Data vaulting systems are increasingly being used to store off-site copies or backups of critical data (for example, financial, government, or sensor data). If backup data stored in the data vault become corrupted without knowledge of the data owner (the data vault customer), no backup recovery is possible in case of loss of the primary critical data.[3] Using a remote data possession checking protocol, the data vault customer might be able to periodically verify that the data vault provider is storing a current and complete copy or backup of the critical files. Any corruption will be noticed by the data owner who will be able to take immediate action (such as making another backup or using another data vault provider). Remote data possession checking is an important component of intrusion detection systems (IDS) used to detect server corruption. However, if the application is a different service than the backup itself and the server can be corrupted/malicious, a remote data possession checking protocol alone is not enough: the server could back up original files and access them to properly run the protocol while using the corrupted versions to provide the service. In the Dependable Intrusion Tolerance architecture (DIT), integrity check is just one among the various building blocks used to detect corruption of remote data.

III. METHODOLOGY

[1] RSA- algorithm:

RSA is a cryptosystem, which is known as one of the first practicable public-key cryptosystems and is widely used for

International Journal of Web Technology
Volume: 03 Issue: 01 June 2014 Page No.19-21
ISSN: 2278-2389

secure data transmission. In such a cryptosystem, the encryption key is public and differs from the decryption key which is kept secret. In RSA, this asymmetry is based on the practical difficulty of factoring the product of two large prime numbers, the factoring problem. RSA stands for Ron Rivest, Adi Shamir and Leonard AdlemanA user of RSA creates and then publishes the product of two large prime numbers, along with an auxiliary value, as their public key. The prime factors must be kept secret. Anyone can use the public key to encrypt a message, but with currently published methods, if the public key is large enough, only someone with knowledge of the prime factors can feasibly decode the message. Breaking RSA encryption is known as the RSA problem. It is an open question whether it is as hard as the factoring problem Cryptographic methods cannot be proven secure.[4] Instead, the only test is to see if someone can figure out how to decipher a message without having direct knowledge of the decryption key. The RSA method's security rests on the fact that it is extremely difficult to factor very large numbers. If 100 digit numbers are used for p and q, the resulting n will be approximately 200 digits. The fastest known factoring algorithm would take far too long for an attacker to ever break the code. Other methods for determining d without factoring n are equally as difficult. Any cryptographic technique which can resist a concerted attack is regarded as secure. At this point in time, the RSA algorithm is considered secure.

[2] 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) Choose two distinct prime numbers p and q.

- For security purposes, the integers p and q should be chosen at random, and should be of similar bit-length. Prime integers can be efficiently found using a primarily test.

2) 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.

3) Compute $\varphi(n) = \varphi(p)\varphi(q) = (p-1)(q-1)$, where φ is Euler's totient function.

4)Choose an integer e such that $1 < e < \varphi(n)$ and gcd$(e, \varphi(n)) = 1$; i.e., e and $\varphi(n)$ are co prime.

- e is released as the public key exponent.
- e having a short bit-length and small Hamming weight results in more efficient encryption – most commonly $2^{16} + 1 = 65{,}537$. However, much smaller values of e (such as 3) have been shown to be less secure in some settings.[5]

5)Determine d as $d \equiv e^{-1} \pmod{\varphi(n)}$; i.e., d is the multiplicative inverse of e (modulo $\varphi(n)$).

- This is more clearly stated as: solve for d given $d \cdot e \equiv 1 \pmod{\varphi(n)}$
- This is often computed using the extended Euclidean algorithm. Using the pseudocode in the *Modular integers* section, inputs a and n correspond to e and $\varphi(n)$, respectively.
- d is kept as the private key exponent.

The public key consists of the modulus n and the public (or encryption) exponent e. The *private key* consists of the modulus n and the private (or decryption) exponent d, which must be kept secret. p, q, and $\varphi(n)$ must also be kept secret because they can be used to calculate d. The standards define three keying options: Keying option

1: All three keys are independent.

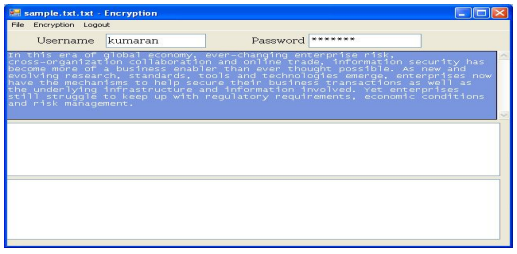
- Keying option 2: K_1 and K_2 are independent, and $K_3 = K_1$.
- Keying option 3: All three keys are identical, i.e. $K_1 = K_2 = K_3$

[3] Triple DES

In cryptography**,** Triple DES is the common name for the Triple Data Encryption Algorithm (TDEA or Triple DEA) symmetric-key block cipher, which applies the Data Encryption Standard (DES) cipher algorithm three times to each data block.The original DES cipher's key size of 56 bits was generally sufficient when that algorithm was designed, but the availability of increasing computational power made brute-force attacks feasible. Triple DES provides a relatively simple method of increasing the key size of DES to protect against such attacks, without the need to design a completely new block cipher algorithm. DES (the Data Encryption Standard) is a symmetric block cipher developed by IBM. The algorithm uses a 56-bit key to encipher/decipher a 64-bit block of data. The key is always presented as a 64-bit block, every 8th bit of which is ignored. However, it is usual to set each 8th bit so that each group of 8 bits has an odd number of bits set to 1.

IV. DISCUSSION OF RESULT

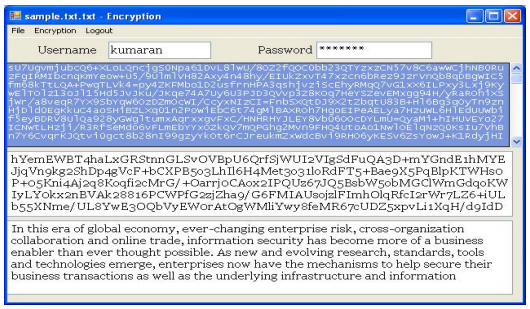
[A]ORIGINAL DATA



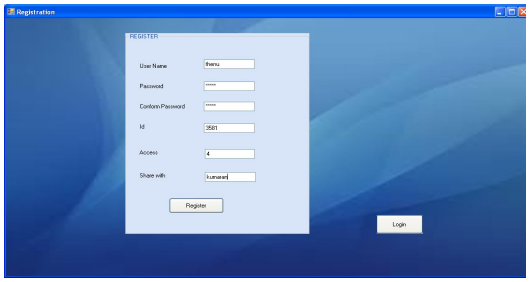
[B]SINGLE ENCRYPTED AND DECRYPTED DATA

International Journal of Web Technology
Volume: 03 Issue: 01 June 2014 Page No.19-21
ISSN: 2278-2389

[C]DOUBLE ENCRYPTED AND DECRYPTED DATA



CLOUD SPACE SHARING:



In this module, we let the users to share their data with other trusted users. Users can give the access rights to other users so that the users who are not the real data owners can also view the file with the authorization rights provided by real data owners. Users also let the TPA to know about this authorization. Thus the data space is being shared with other users such that the cloud space is used effectively. One or more users can view the data with the full authentication.

V. CONCLUSION AND FUTURE ENHANCEMENT

In this paper, we propose a privacy-preserving public auditing system for data storage security in cloud computing. We utilize the homomorphic linear authenticator and random masking to guarantee that the TPA would not learn any knowledge about the data content stored on the cloud server during the efficient auditing process, which not only eliminates the burden of cloud user from the tedious and possibly expensive auditing task, but also alleviates the users' fear of their outsourced data leakage. Considering TPA may concurrently handle multiple audit sessions from different users for their outsourced data files, we further extend our privacy-preserving public auditing protocol into a multiuser setting, where the TPA can perform multiple auditing tasks in a batch manner for better efficiency. Extensive analysis shows that our schemes are provably secure and highly efficient. Our preliminary experiment conducted on Amazon EC2 instance further demonstrates the fast performance of our design on both the cloud and the auditor side. We leave the full-fledged implementation of the mechanism on commercial public cloud as an important future extension, which is expected to robustly cope with very large scale data and thus encourage users to adopt cloud storage services more confidently. Considering TPA may concurrently handle multiple audit sessions from different users for their outsourced data files, we further extend our privacy-preserving public auditing protocol into a multiuser setting, where the TPA can perform multiple auditing tasks in a batch manner for better efficiency. Extensive analysis shows that our schemes are provably secure and highly efficient. Our preliminary experiment conducted on Amazon EC2 instance further demonstrates the fast performance of our design on both the cloud and the auditor side. We leave the full-fledged implementation of the mechanism on commercial public cloud as an important future extension, which is expected to robustly cope with very large scale data and thus encourage users to adopt cloud storage services more confidently.

REFERANCES

[1] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Storage Security in Cloud Computing," Proc. IEEE INFOCOM '10, Mar. 2010.

[2] C. Wang, K. Ren, W. Lou, and J. Li, "Towards Publicly Auditable Secure Cloud Data Storage Services," IEEE Network Magazine, vol. 24, no. 4, pp. 19-24, july/Aug. 2010.

[3] F. Sebe, J. Domingo-Ferrer, A. Martı´nez-Balleste, Y. Deswarte, and J.-J. Quisquater, "Efficient Remote Data Possession Checking in Critical Information Infrastructures," IEEE Trans. Knowledge and Data Eng., vol. 20, no. 8, pp. 1034-1038, Aug. 2008.

[4] A. Juels and B. S. K. Jr., "Pors: proofs of irretrievability for large files," in ACMConference on Computer and Communications Security, P. Ning, S. D. C. di Vimercati, and P. F. Syverson, Eds. ACM, 2007,

[5] J. Kincaid, "MediaMax/TheLinkup Closes Its Doors./, July 2008.

[6] Amazon.com, "Amazon s3 Availability Event: July 20, 2008," http://status.aws.amazon.com/s320080720.html, July 2008.

[7] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing," IEEE Trans. Parallel and Distributed Systems, vol. 22, no. 5, pp. 847-859, May 2011.

[8] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable Data Possession at Untrusted Stores," Proc. 14th ACM Conf. Computer and Comm. Security (CCS '07), pp. 598-609, 2007.