RESEARCH ARTICLE OPEN ACCESS

An Efficient Approach for Data Sharing in Cloud Computing Using Digital Signature

Elayaraja.D[1], J.Caroline EL Fiorenza[2] (Assistant Professor)
Department of Computer Science and Engineering,SRM University, Ramapuram Campus, Chennai.

----------**********----------

Abstract:

Cloud Computing is the delivery of Computing services over the Internet. The Cloud Data services stores Data in the cloud and shares across multiple users, who can easily modify the shared data as a group. To ensure the shared data integrity, users in the group need signatures on all data blocks .Due to Data modifications done by different users in the group, it is essential that the shared data blocks are to be signed by different users. Once a user is revoked from the group for security reasons, the existing user must be re-signed. This system proposes a public auditing procedure for the integrity of shared data which is performed by a third party auditor, with valuable user revocation. Instead of downloading and Re-Signing the shared blocks by the existing user, we allow the cloud to Re-sign blocks by digital signature during user revocation. Also, our process supports batch auditing and maintain the data in the form of versions. Hence it improves the efficiency of user revocation, maintain the Data modifications history and the compatibility to retrieve the earlier versions. Also Cloud computing is completely about productivity, economy, and corporate agility. But there raises a question how we can commercially attain those benefits if their cloud management solution becomes inefficient, incomplete, and inflexible. Even though there are many aspects in cloud environment.

Keywords: - **Cloud computing, Data security, Internet, Key, cloud server, digital signature and encryption.**

----------**********----------

INTRODUCTION

The Cloud Computing is the combination of different services and applications Online over the web. In Modern times, Cloud computing has moved to a different level with high importance. It is a fast growing technology and will be the future of IT sector & IT world. Its a process of moving database, applications and files to a huge datacentre. These data are not only stored in cloud, but it is being shared and used by multiple users across the globe. Real time applications available in the market are Google drive, Drop Box, I cloud etc.. by various companies. When a shared data is being created by a user, each and every user in the particular group can amend access and alter the data. The bigger advantage is that the latest version of the shared data can be provided to the group by any user of that group.

It is known that Cloud promises secure and safe environment to the users. Yet, one critical or major issue to be handled is the data integrity. In order to achieve this,

various features and ideas have been proposed. To maintain the shared data integrity, users of a particular group should have signatures on all data blocks being used by them. As the data modification is being done by different users of a particular group, it is necessary that the shared data blocks should be signed by various users of the group. Any user who violates or leave the group, that particular user must be removed from the group by the administrator or group owner. Signature created by the removed user is no longer valid to the group. The data blocks must be signed again by an existing/different user of that group though the shared data content is not changed when a user is removed from the group. By using the public keys of available users in the group, the Integrity of the entire data can be validated.

CLOUD COMPUTING FEATURES:

One of the salient features is to allow a TPA (Third Party Auditor) to audit the integrity of cloud data without the need of downloading the actual data from cloud.He is also referred to as Public verifier. He might be a person who likes to use the cloud data to search, compute and various other purposes. But these features do lag to consider the effectiveness of User removal when correctness of data is being audited. During removal, user is allowed to download the shared data & sign it again in the current method. This will become useless due to huge size of data in the cloud systems. Both owners and public verifiers (TPS) can audit cloud data integrity without downloading the complete data. To handle the efficiency of multiple auditing by various TPA, we ideate Public Auditing Procedure for maintaining the integrity of shared data along with user revocation. In this method, cloud will re-sign the data blocks instead of an existing user resigning, during the process of user revocation. This is possible with the proxy re-signatures by using Digital signature. This system facilitates the data to be signed out to a particular user who modifies it. Data will be locked to the user who does the modification preventing others from updating in parallel. An audit history of data modification comprising of modified data, time, user who has modified and justification are captured and maintained. It also provides an ease to restore the earlier versions in case of corruption.

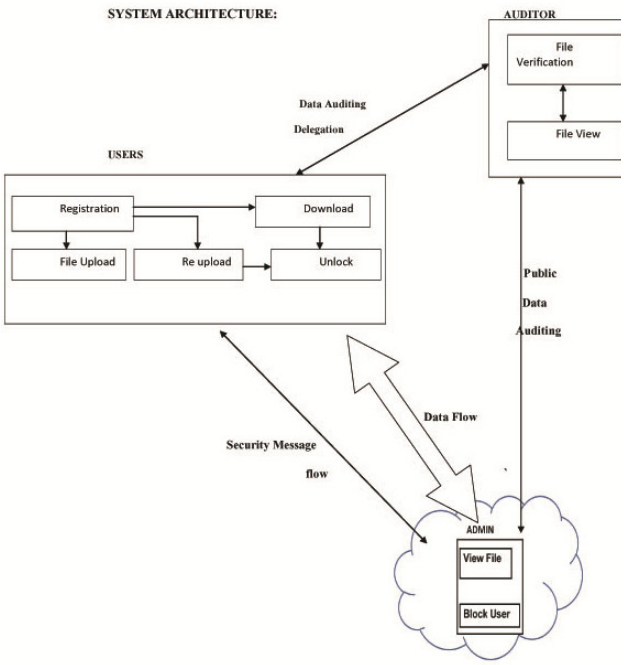
- **SCALABILITY**
- **ENVIRONMENT FRIENDLY**:.
- **COST EFFICIENT**
- **UP TO DATE**
- **IMPROVED PERFORMANCE**

How digital signatures work:

Digital signatures are often used to implement electronic signatures, a broader term that refers to any electronic data that carries the intent of a signature, but not all electronic signatures use digital signatures. Digital signatures based on public key cryptography. Using a public key algorithm such as RSA, one can generate two keys that are mathematically linked: one private and one public. Digital signature gives the receiver reason to believe the message was sent by the claimed sender. A digital

signature can be used with any kind of message whether it is encrypted or not simply so the receiver can be sure of the sender's identity and that the message arrived intact. Digital signatures make it difficult for the signer to deny having signed something (non-repudiation) assuming their private key has not been compromised as the digital signature is unique to both the document and the signer, and it binds them together. A digital certificate, an electronic document that contains the digital signature of the certificate-issuing authority, binds together a public key with an identity and can be used to verify a public key belongs to a particular person or entity.

System Architecture:



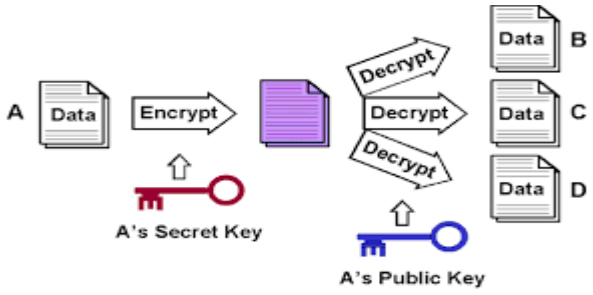
Asymmetric cryptography:

The process of cryptography in which one key is used for message encryption and another for message decryption for safe data transmission is called Asymmetric Cryptography. Two separate keys (one private and another public) are required whereas the two parts of key pair are linked mathematically. Any new user who likes to send an encrypted message has to get the proper recipient's public key. Any kind of message (text or file or document or an image) which is encrypted by a public key can be decrypted only by using the matching private key which uses the similar algorithm.

1. Choose two large prime numbers $p \neq q$ randomly and independently of each other. Compute $N = p\,q$.
2. Choose an integer $1 < e < N$ which is coprime to $(p\text{-}1)(q\text{-}1)$.
3. Compute d such that $d\ e \equiv 1 \pmod{(p\text{-}1)(q\text{-}1)}$.
4. Destroy all records of p and q.

- (Steps 2 and 3 can be performed with the extended Euclidean algorithm; see modular arithmetic. Additionally, solving for either e or d may be performed using the Diophantine equation $ed - k\phi(n) = 1$.)

Public keys are N and e; Private keys are N and d. It is clearly noted "d" is secret and "N" is public. Alice keeps the private key in secret and transfers the public key to Bob.



Authentication

It is known that Anonymous key exchanges are not secured as it does not provide valid authentication of the involved parties. It is greatly vulnerable to be attacked by a Middle man. Ex: Diffie-Hellman key exchange.

Various cryptographic authentication schemes have been developed to provide secure authentication via key agreement and to protect the data from middle man attacks. These methods generally bind the agreed key to other agreed-upon data mathematically, such as:

- Public/private key pairs
- *Diffie-Hellman*
- **RSA**

Public keys:

The Public Key Cryptography is mainly used to communicate messages in a way only the intended recipient can understand that even if there is a middle man attack. In this method, the intended recipient can verify the identity of the actual sender (from who the message was originated) using the sender's public key. This method of identification is called "Digital Signature". This helps in greater confidentially and secure authentication. Public-key encryption involves a set of keys, comprising a public and a private key associated with an entity that needs to verify its identity electronically or to sign the data digitally or to encrypt the data. All public keys are published and the respective private keys are kept secret.

RSA DIGITAL SIGNATURE Algorithm :

Take two large primes, p and q, and compute their product $n = pq$; n is called the modulus. Choose a number, e, less than n and relatively prime to $(p-1)(q-1)$, which means e and $(p-1)(q-1)$ have no common factors except 1. Find another number d such that $(ed - 1)$ is divisible by $(p-1)(q-1)$. The values e and d are called the public and private exponents, respectively. The public key is the pair (n, e); the private key is (n,d). The factors p and q may be destroyed or kept with the private key.

Currently, it is difficult to retrieve the private key "d" from public key (n,e). If we can factorise n into p and q, then we can easily obtain the private key "d".

Hence the security of RSA system is by assuming the factoring is very difficult.

p = 61 — first prime number (to be kept secret or deleted securely)

q = 53 — second prime number (to be kept secret or deleted securely)

n = pq = 3233 — modulus (to be made public)

e = 17 — public exponent (to be made public)

d = — private exponent (to be kept

2753 secret)

The public key is (e, n). The private key is d. The encryption function is:

encrypt(m) = m^e mod n = m^{17} mod 3233 where m is the plaintext. The decryption function is: decrypt(c) = c^d mod n = c^{2753} mod 3233 where c is the ciphertext.

To encrypt the plaintext value 123, we calculate encrypt(123) = 123^{17} mod 3233 = 855

To decrypt the ciphertext value 855, we calculate decrypt(855) = 855^{2753} mod 3233 = 123

When RSA keys are used to sign a message digitally, a hash will be created by Alice for her message to bob. Hash value will be encrypted with her RSA private key and added to the message. Bob will verify that the sender of the message is Alice by decrypting the hash value with public key. In case of a match, it can be confirmed that the sender of the message is Alice and the message content is as exactly as she wrote it.

Diffie-Hellman

Diffie-Hellman key exchange is a cryptographic protocal which allows two unknown parties to each other to establish a secret key which is shared over an insecure channel. Using a symmetric key cipher the key can be used to encrypt further communications.

Synonyms of Diffie-Hellman key exchange include:

- **Diffie-Hellman key agreement**
- **Diffie-Hellman key establishment**
- **Diffie-Hellman key negotiation**
- **exponential key exchange**
- **Diffie-Hellman Algorithm**
- **Diffie-Hellman Algorithm**
- **Diffie-Hellman Algorithm**

Diffie-Hellman Algorithmwith example of the protocol :

- Alice and Bob agree to use a prime number p=23 and base g=5.
- Alice chooses a secret integer a=6, then sends Bob (g^a mod p)
  - 5^6 mod 23 = 8.
- Bob chooses a secret integer b=15, then sends Alice (g^b mod p)
  - 5^{15} mod 23 = 19.
- Alice computes (g^b mod p)^a mod p
  - 19^6 mod 23 = 2.
- Bob computes (g^a mod p)^b mod p
  - 8^{15} mod 23 = 2.

Both Alice and Bob have arrived at the same value, because g^{ab} and g^{ba} are equal. Note that only a, b, g^{ab} and g^{ba} are kept secret. All the other values are sent in the clear. Once Alice and Bob compute the shared secret they can use it as an encryption key, known only to them, for sending messages across the same open communications channel. Of course, much larger values of a,b, and p would be needed to make this example secure, since it is easy to try all the possible values of g^{ab} mod 23 (there will be, at most, 22 such values, even if a and b are large). If p was a prime of more than 300 digits, and a and b were at least 100 digits long, then even the best known algorithms for finding a given only g, p, and g^a mod p (known as the discrete logarithm problem) would take

longer than the lifetime of the universe to run. *g* need not be large at all, and in practice is usually either 2 or 5.

CONCLUSIONS AND FUTURE DIRECTIONS:

There are many benefits of using cloud computing such as cost efficiency, quick Deployment, improved accessibility etc. However, there are yet many practical problems which have to be solved. The data confidentiality is one of them. Many researchers contributed their efforts to minimize the data security issue in this domain with different solutionsthat described in this work It is the apt technology for allowing the user to save their data in cloud storage. Nowadays cloud computing has a various security issues such as authentication, privacy and integrity. In this paper we are authenticating the data by using the digital signature. RSA and Diffie-Hellman encryption algorithms are providing the data security on cloud computing. This digital signature system is more secure than existing system which uses the DES and blowfish , 3EDS.

REFERENCES:

[1] 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, Communications of the ACM”, vol. 53, no. 4, pp. 5058, April 2010

[2] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song,” Provable Data Possession at UntrustedStores, in Proc. ACM Conference on Computer and Communications Security (CCS)”, 2007, pp. 598610.

[3] C.Wang, Q.Wang, K. Ren, andW. Lou, “Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing, inProc. IEEE International Conference on Computer Communications (INFOCOM)”, 2010, pp.525533.

[4] R. L. Rivest, A. Shamir, and Y. Tauman,”How to Leak a Secret, in Proc. International Conference on the Theory and Applicationof Cryptology and Information Security (ASIACRYPT)”. SpringerVerlag, 2001, pp. 552565.

[5] M. Sudha Dr.Bandaru Rama Krishna Rao,M. Monica, A Comprehensive Approach to Ensure Secure Data Communication in Cloud Environment, International Journal of Computer Applications (0975 – 8887) Volume12– No.8, December 2010.

[6] Akhil Behl, Emerging Security Challenges in Cloud Computing, presented at World Congress on Information andCommunication Technologies,2011.

[7] Wang Junxiang, Liu Shengli, Dynamic Provable Data Possession with Batch-Update Verifiability,