The International Journal Of Engineering And Science (IJES)
||Volume||2 ||Issue|| 4 ||Pages|| 58-63 ||2013||
ISSN(e): 2319 – 1813 ISSN(p): 2319 – 1805

Reliable Data Uploading and Distribution in the Cyber Space

[1,] Aruna A [2,] Kiruthika P [3,] Suganya N

[1,] *Assistant Professor , Department of information Technology, SNS College of Engineering*
[2,] *Assistant Professor, Department of Information Technology, SNS College of Engineering*
[3,] *UG Scholar , Department of Information Technology, SNS College of Engineering*

----------Abstract----------

The Distributed considerations are the major acquiring epitome. The domain abbreviates monetary value related on computation. The service provided on scattered location to its users on demand across the cyberspace. The data and other resources used by the user are stored in the open environment. The circumstance issues more on data security and user fear on missing bound on their data. To enrich security on data, the security mechanisms are implemented, though the data integrity is unnoticed to user. To overcome the problem and achieve data integrity the method of auditing is established through Third Party Auditing (TPA). In addition to auditing the sensitive data in uploading over the dispersed area are protected by DES encryption algorithm.

Keywords *- Data Audit, Data Integrity, Data Security, Encryption Algorithm, Third Party Auditing*

Date of Submission: 1, April 2013 Date Of Publication: 20, April.2013

I. INTRODUCTION

Cloud computing is a type of computing that relies on *sharing computing resources* rather than having local hosts or personal devices to handle applications. In cloud computing, the word cloud (also phrased as "the cloud") is used as a metaphor for "*the Internet*," so the phrase *cloud computing* means "a type of Internet-based computing," where different services -- such as servers, storage and applications -- are delivered to an organization's computers and devices through the Internet. Cloud computing is an on-demand service that is obtaining mass appeal in corporate data centers. The cloud enables the data center to operate like the Internet and computing resources to be accessed and shared as virtual resources in a secure and scalable manner. Cloud computing opens up a new world of opportunities for businesses, but mixed in with these opportunities are numerous security challenges that need to be considered and addressed prior to committing to a cloud computing strategy. Cloud computing security (simply referred "cloud security") is a sub-domain of information technology security. In order to protect the cloud data and applications, a set of security policies, methodologies and control technologies are implemented in the associated cloud security infrastructure. To confidently leverage cloud solutions, cloud security is needed.

Major issues are compliance and access control related. Security concerns associated with cloud computing fall into two categories: security issues faced by cloud providers and those faced by customers. This is the main reason why security in the cloud is a shared responsibility: both the provider and the customer must ensure that proper measures are taken in order to protect the client's data and to ensure that the infrastructure is secure. Cloud providers and their clients can negotiate terms around liability, intellectual property and end-of-service when signing the Service Level Agreement. Cloud computing security challenges fall into two broad categories:

- Data Protection: Securing the data both at rest and in transit
- User Authentication: Limiting access to data and monitoring who accesses the data

Implementing a cloud computing strategy means placing critical data in the hands of a third party, so ensuring the data remains secure both at rest (data residing on storage media) as well as when in transit is of paramount importance. Data needs to be encrypted at all times, with clearly defined roles when it comes to who will be managing the encryption keys. In most cases, the only way to truly ensure confidentiality of

encrypted data that resides on a cloud provider's storage servers is for the client to own and manage the data encryption keys. Data resting in the cloud needs to be accessible only by those authorized to do so, making it critical to both restrict and monitor who will be accessing the data through the cloud. In order to ensure the integrity of user authentication, user need to be able to view data access logs and audit trails to verify that only authorized users are accessing the data. These access logs and audit trails additionally need to be secured and maintained for as long as the user needs or legal purposes require.

However, security concerns become relevant as we now outsource the storage of possibly sensitive data to third parties. The security issues are considered, a secure overlay cloud storage system –FADE (File Assured Deletion) provides fine-grained access control and assured deletion for outsourced data on the cloud [2]. The stored data in the cloud is accessed through various techniques, the relevant work is done with role based access control in cloud secure the users data [3]. The data leaving in third parties hand is managed in secure form, to ensure the security authentication mechanism is implemented. The security in the cloud database is attained with hybrid encryption method which concerned about small sized data [4]. The cloud service providers, issues and services are categorized in study [1] which entitles the base level of cloud utility.

The analysis on encryption algorithm details the use of algorithm over cloud based on confidentiality, integrity and availability in best approach manner. The confidentiality on data on the cloud is ensured up with RSA algorithm in earlier [5]. Two –factor authentication technique fulfilled the data integrity measure on the cloud. The fulfillment is achieved through Diffie-Hellman key exchange algorithm [6]. To monitor the usage of encryption algorithms in data security the new cloud environment is designed with java in concern including RSA and MD5 for resource allocation controlled by client and cloud admin [7]. To be effective, distributed data security depends on more than simply applying appropriate data security procedures and countermeasures. This paper guarantees the data security and data accountability on the open environment with beneficial supportive methodologies. Data uploading with encryption is highly beneficial in cloud data security. The TPA automatically logs the usage of data on the cloud with access control policies and authenticated logging mechanism.

II. PROBLEM DEFINITION

Data security is a critical issue in the cloud computing environments. In cloud, the data can be physically located anywhere in any data centre across the distributed network. The cloud nature issues more with user authentication, data integrity and confidentiality. The data hosted in the cloud is completely under the third party control to ensure the data usage in the cloud, the data on the cloud environment is accounted with the programmable JAR files. The framework completes the progress of data accountability over cloud. The security in data is achieved through implementing cryptographic algorithms.

III. DATA SAVING

Cloud data storage provides the way to find the best solution in getting data from any location. It could also be known as the back-up place of data. The stored data under third party control must be guaranteed in correctness and availability. The major issue is to effectively detect any unauthorized data modification. To address this problem regarding security the data to be stored upon cloud must be encrypted and authenticated. The issue is recovered up with erasure code [6] which safeguards from Byzantine failure but the technique occupies more memory.

IV. DATA APPROACH

Approaching data from the outsourced environment should be easy to get into access. The environment should also provide a safe data access. The access is controlled in different categories such as Role Based Access Control [2] and file based access [1]. Access rights are monitored with authentication and authorization techniques in better way to attain security

V. SECURITY ALGORITHMS

To enrich security in the cloud, the various security techniques are available. The data over public network can be protected by the method of encryption. Encryption converts that data by any encryption algorithms using the “key” in scrambled form. Only user having access to the key can decrypt the encrypted data.
Encryption algorithm plays a big role in providing data security against malicious attacks. Encryption

algorithm can be categorized into symmetric key (private) and asymmetric key (public) key. In symmetric key encryption or secret key encryption, only one key is used to encrypt and decrypt data. In asymmetric key encryption, two keys are used: public and private keys. Public key is used for encryption and private key is used for decryption. The data in the cloud allowed being more secure with encryption algorithms and to valid the original data hashing technique is used. The algorithms analyzed are RSA, DES, and AES.

5.1 RSA

RSA is a commonly used public key cryptography algorithm. The first, and still most commonly used asymmetric algorithm RSA is named for the mathematicians Rivest, Shamir, and Adleman. RSA today used in hundreds of software products and can be used for key exchange, digital signature, or encryption of small blocks of data. RSA uses a variable size encryption block and a variable size key. The key pair is derived from a very large number, n-that is the product of two prime numbers chosen according to special rules. Since it was introduced in 1977, RSA has been widely used for establishing secure communication channels and for authentication the identity of service provider over insecure communication medium. In the authentication scheme, the server implements public key authentication with client by signing a unique message from the client with its private key, thus creating what is called a digital signature. The signature is then returned to the client, which verifies it using the server's known public key.

5.2 RSA Encryption Algorithm:

RSA_Encryption (P,e,n) // P is plain text in Z_n
{ //e, n is public key and P<n
C←Fast_Exponentiation(P,e,n)//Calculation of (P^emod n)
return C
}
RSA Decryption Algorithm:
RSA_Decryption(C,d,n) // C is cipher text in Z_n
{ // d is private key
P←Fast_Exponentiation(C,d,n)//Calculation of (C^d mod n)
return P
}

5.3 DES

Data Encryption Standard (DES) is a widely-used method of data encryption using a private (secret) key. DES originated at IBM in 1977 and was adopted by the U.S. Department of Defence. It is specified in the ANSI X3.92 and X3.106 standards and in the Federal FIPS 46 and 81 standards. There are 72 quadrillion or more possible encryption keys that can be used. For each given message, the key is chosen at random from among this enormous number of keys. Both the sender and the receiver must know and use the same private key. DES applies a 56-bit key to each 64-bit block of data. The process can run in several modes and involves 16 rounds or operations.

5.4 Pseudo Code: Data Encryption Standard

INPUT: plaintext m1 . . . m64; 64-bit key K=k1 . . . k64 (includes 8 parity bits).
OUTPUT: 64-bit cipher text block C=c1 c64.
1. (key schedule) Compute sixteen 48-bit round keys Ki, from K.
2. (L0, R0) ß IP(m1, m2,. . .m64) (Use IP Table to permute bits; split the result into left and right 32-bit halves L0=m58m50 . . . m8,R0=m57m49 . . . m7)
3. (16 rounds) for i from 1 to 16, compute Li and Ri as follows:
3.1. Li=Ri-1
3.2. Ri = Li-1 XOR *f* (R i-1, Ki) where *f*(Ri-1, Ki) = P(S(E(Ri-1) XOR Ki)), computed as follows:
(a) Expand Ri-1 = r1r2 . . . r32 from 32 to 48 bits, T ßE(Ri-1).
(b) T ' ßT XOR Ki. Represent T ' as eight 6-bit character strings: T '= (B1 . . . B8)
(c) T " ß(S1(B1), S2(B2), . . . S8(B8)). Here Si(Bi) maps to the 4-bit entry in row r and column c of Si
(d)T"' ßP(T"). (Use P per table to permute the 32 bits of T"=t1t2 . . . t32, yielding t16t7 . . . t25.)
4. b1b2 . . . b64 ß (R16, L16). (Exchange final blocks L16, R16.)
5. C ß IP-1 (b1b2 . . . b64). 6. End.

5.5 AES

The Advanced Encryption Standard (AES) is a National Institute of Standards and Technology specification for the encryption of electronic data. AES is a new cryptographic algorithm that can be used to protect electronic data. Specifically, AES is an iterative, symmetric-key block cipher that can use keys of 128, 192, and 256 bits, and encrypts and decrypts data in blocks of 128 bits (16 bytes). Unlike public-key ciphers, which use a pair of keys, symmetric-key ciphers use the same key to encrypt and decrypt data. Encrypted data returned by block ciphers have the same number of bits that the input data had. Iterative ciphers use a loop structure that repeatedly performs permutations and substitutions of the input data.

5.6 DATA ACCOUNTABILITY

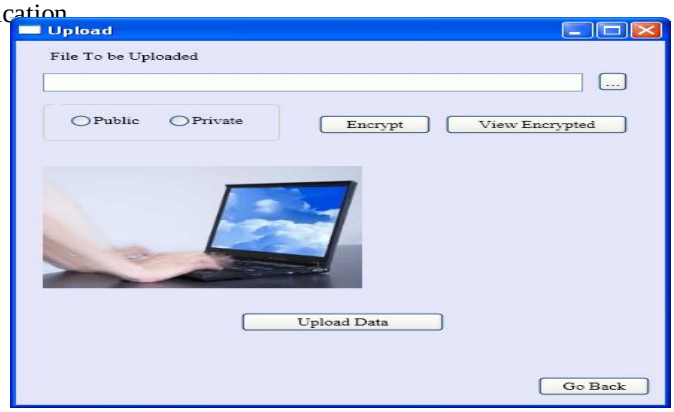
Data uploaded in the cyberspace is utilized only whenever required. Until then the data on the cloud must be secure. In the same time the user of the data in need of monitoring the access over the sensitive information which get shared on the third party environment. The access rights on the data in the cloud are provided by the owner. Though the access rights are set there is essential to get notice on time of access and to maintain log.

VI. EXECUTION

To enrich the data security the proposed concept includes an idea of auditing the data by taking out different sets of file. The framework allows uploading files in public and private forms and the authentication mechanism is managed to monitor the logs.

6.1 Data Uploading

The uploading data in the cloud is being in two different sets. The data which is more sensitive is authorized to encrypt before adding into the cloud circumstances which is meant as Private data. The private data is encrypted using DES algorithm which the key generated is shared to download the data. The DES algorithm aid high-level security, efficient and economical manner. The public data is uploaded as such in the same format without any modification.

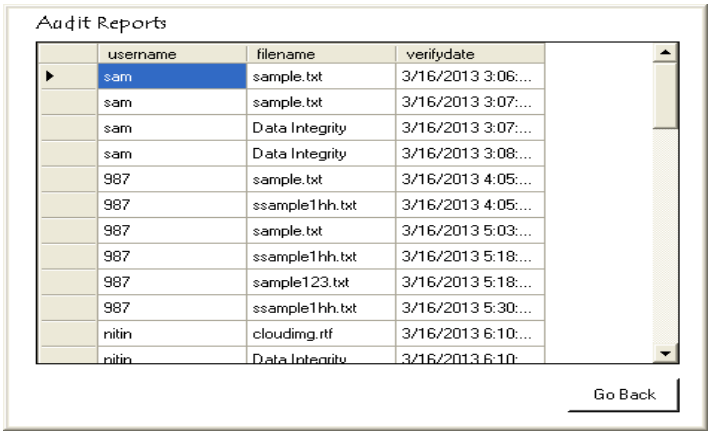


5.5 Access Rights

The access rights on the data are provided by the data owner. The access rights on data sharing comprise view mode and modify mode. The view mode is which allow the members who get shared with data only possible to view the contents unable to download or modify. The modify mode is download enable mode where the member with data access can download and modify the data as specified by the owner.

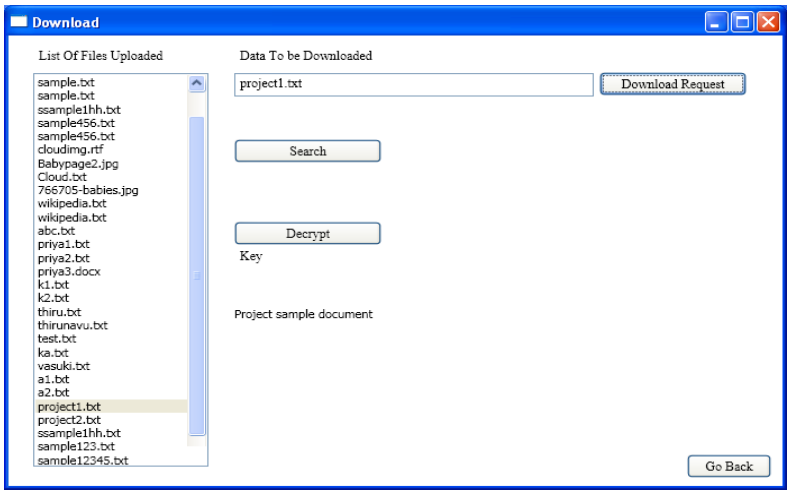
5.6 Log File Mechanism

The data accountability is maintained with the log file created in every access on the data. The generated log files are the monitor display at the owner side. The mechanism maintenance is attained by the Third Party Audit (TPA). The TPA has rights only on authenticating the access. The log file includes the contents of data access time, unauthorized access, modification details.



5.7 Data Download

The owner of the data is only supposed to download the log file which has an entire access record on the data being shared or rest on the cloud circumstances. The private data download includes simple steps as on data upload. The encrypted data is decrypted using the key generated while uploading the content. This decrypt on data validates the integrity of the original data. This ensures data security.



VII. CONCLUSION

The Cyberspace provides an enormous facility in taking challenges over the data in the concept of whenever and wherever required. The problem with data security issues in cloud data storage and data transfer. The DIA framework attains idea on security on data in rest as well as in transit. The data storage is secured with DES algorithm, access rights are authenticated with logging mechanism and the data integrity is achieved through accountability method. Provision of security to the users' data on the cloud will definitely encourage the data owner to outsource the data and utilize the service beneficially.

REFERENCES

[1] Yang Tang, Patrick P.C.Lee, John C.S.Lui, Radia Perlman, "Secure Overlay Cloud Storage and Assured Deletion", IEEE Transaction on Dependable and Secure Computing , Vol.9 No.6-2012
[2] Lan Zhou, Vijay Varadharajan and Michael Hitchens, "Enforcing Role-Based Access Control for Secure Data Storage in the Cloud", Vol.54 No.10,2011
[3] S.Sajithabanu, Dr.E.george Prakash Raj, "Data Storage Security in Cloud", Vol.2,2011
[4] Amanjot Kaur, Manisha Bhardwaj, "Hybrid Encryption for Cloud Database Security", Vol.2,2012
[5] Sowmya Naik.P.T, Vrushali W.Basatwar, Aisha Begam and Mushtaq Ahmed D M, "Evaluation of Security and Performance of Dependable Data storage in Cloud Computing",2011

[6] K.Valli Madhavi, R.Tamilkodi, R.BalDinakar, "Data Storage Security in Cloud Computing for Ensuring Effective and Flexible Distribution System", 2012
[7] Veerraju Gampala, Srilakshmi Inuganti, Satish Muppidi, "Data Security in Cloud Computing with Elliptic Curve Cryptograohy", Vol.2, July-2012
[8] Parsi Kalpana, Sudha Singaraju, "Data Security in Cloud Computing using RSA Algorithm", Vol.1,September-2012.
[9] D.H.Patol, Rakesh R. Bhavsar, Akshay S. Thorve, "Data Security Over Cloud", 2012
[10] Dubey A.K, Namdev.M, Shrivastava S.S, "Cloud-User Security based on RSA and MD5 algorithm for resource attestation and Sharing in Java Environment, Vol.2,February-2012.

BIOGRAPHIES

***Aruna.A* B.Tech, M.E;** is currently working as an Assistant Professor at SNS College of Engineering, Coimbatore. She is a member of Computer Society of India (CSI). She has published her work in Journals and presented four papers in International Conferences, three papers in National Conferences. She has five years of experience in Teaching.

***Kiruthika P,* B.E** is currently pursuing her **M.E** and working as an Assistant Professor at SNS College of Engineering, Coimbatore. She is a member of IEEE. She has published her work in Journals and presented four papers in National Conferences and one International Conferences. She has four years of experience in Teaching.

Suganya N is currently pursuing **B.Tech (IT)** Final Year at SNS College of Engineering, Coimbatore. She is a member of Computer Society of India (CSI) Student Chapter. Her Research area interest includes Software Testing and Security in Distributed Environments.