Volume 4, Issue 11, November 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Security Schemes in Distributed Data Storage Using Proxy Re-encryption

G. Srilakshmi*
PG Scholar, Dept of CSE,
Kakatiya Institute of Technology and Science,
Warangal, India

M. Preethi
Assist. Prof. Dept of CSE,
Kakatiya Institute of Technology and Science,
Warangal, India

Abstract: ***Present days many users store their important data in cloud. To ensure that the security of the cloud stored data users need to encrypt the important data. The point of data security which has always been important aspect of quality, cloud computing cause a new security threats. In cloud computing the stored data owner can outsource his data on cloud server and only the authorized user can access that data .This type of service is called as Database-As-A-Service [1],[2]. The storing of data in cloud computing different issues related to confidentiality, correctness and access permission of outsourced data because Cloud is managed by third party. The stored data persons always suspected about security of the data. The existing system does not provide security attacks for storing data in clouds, but the propose system can provide security against for Collusion attack, DDOS attack. Using this concept re-encryption the data get more secure and access permission that who will access the data is decided by only the data stored person or owner. We propose an identity based data storage scheme where both queries from the intra domain and inter domain are considered and collusion attacks can be resisted [7]. The propose system application which will access from Android based devices. In existing system to provide better security data stored person has to be online all the time so our propose system will be helpful for data stored persons by providing notification about request of user.***

Keyword: Proxy server, data owner, IBDDS, DDOS, re encryption key.

I. INTRODUCTION

In Cloud computing technology includes many technologies like autonomic computing virtualization, computing and service oriented architecture. The purpose of all these technologies to provide shared resources and providing services. The cloud is a service is referred to as providing a service over the network. There are three types of services. Software as a Service and Infrastructure as a Service. All these services are based on policy of on demand in which users can pay only to for their required usages. Present days many cloud service providers such as Amazon's, Microsoft's Windows Google's App Engine providing the facility to different users. Users who cannot afford such high cost to build their own large infrastructure. So they can have their work done by the help of clouds at low cost. the users type and the hosting of environment [8] the cloud architecture can be divided into four types.

1. Public Cloud
2. Private Cloud
3. Hybrid Cloud
4. Community Cloud.

1. Public cloud- The Public cloud provides services are hosted for public usage and anyone can have their data stored. In this Data security is most important.
2. Private Cloud- In Private cloud where the data access and service usage are restricted to one authority.
3. Hybrid Cloud- In Hybrid cloud data or files shared by a less number of organizations and it combined the features of both public and private clouds.
4. Community cloud- In Community clouds are the private clouds. In community clouds data or files are shared among the similar entities of the one organization. This data owner or stored person can outsourced his data on cloud server for reducing space cost as well as maintenance cost. The authorized user can request that data or file. The uploading data before on cloud server's data owner has to be encrypting his personal data. The Proxy servers can perform some functions on the stored cipher text without knowing about the actual data or file. The Cloud server is UN trusted server because it managed by third parties. Here the issues like confidentiality came into existence. Data stored persons mostly concerned on the security from unauthorizing access of data. The data should not be modified by un authorized user or the proxy server. This is the main reason that it becomes major research problem among research community and growing daily. In this we propose a system for security enhancement of cloud computing using identity based encryption[6]. It has following properties.
a) The access permission without using the private key generator the file owner can decide independently.
b) For a single request a receiver can only access one file instead of all files.

c) Secure against collusion attacks. Even if the receiver can compromise the proxy servers he cannot obtain the owner secret key.

d) We can get the notification about user request on his android based device which is not possible in present system.

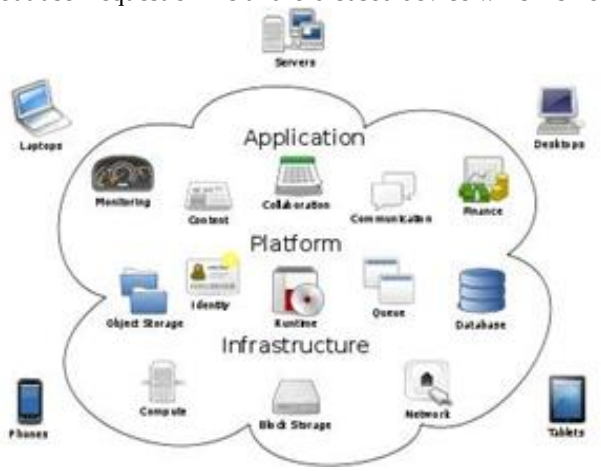


Fig: Cloud Computing

II. TRADITIONAL SYSTEM METHODOLOGY

The Cloud computing System providing users with a convenient mechanism to manage their files or data with the notion called database as a service. In database as a service schemes. A user can outsource his encrypted data to un trusted proxy servers [3]. The Proxy servers can perform some functions on the outsourced cipher texts without knowing anything about the original data or files. The main reason is users are especially concerned on the confidentiality [5],integrity of the outsourced files as cloud computing is a lot more complicated than the local data storage systems, as the cloud is managed by un trusted third parties. After outsourcing the data to proxy servers the user will remove from his local system. Then the outsourced files are not accessed by the unauthorized users and not modified by proxy servers. It is an important problem that has been considered in the data storage system. Further how to guarantee that an authorized user can query the outsourced files from proxy servers is another concern. The proxy server only maintains the outsourced cipher texts consequently research around these topics grows.

1) Identity based proxy encryption:-

Identity based proxy encryption in which they presented security model for both unidirectional and bidirectional Identity based proxy encryption schemes [2]. In these schemes the master secret key used to extract secret keys divided into two parts. First one is sent to the proxy server and the second is sent to users. The user can decrypt a cipher text for him with the help of the proxy server. The disadvantage of this system is that it is not collision safe.

2) Identity based proxy re- encryption:-

The first identity based proxy re encryption was developed by Green and Ateniese [9]. Where the proxy server can transfer a cipher text for the data stored person to a cipher text for the user after he gets a re-encryption key from the former. The identity based proxy re encryption schemes divides into the following two types based on the generation of the re encryption key.

a) The re encryption key will computed by the owner or stored person.

b) The re encryption key can be computed by Private Key.

3) Identity based storing Secure Distributing Data:-

Identity-based Secure Distributed Data Storage was proposed by Willy Susilo and Yi Mu [4] a user identity can be an arbitrary string and two parties can communicate with each other without checking the public key. The file owner encrypts his files under his identity based. Then the corresponding files send the cipher texts to the proxy servers [4]. The proxy servers can transfer a cipher text encrypted under the identity of the owner to a cipher text encrypted under the identity of the receiver. After they has obtained an access re encryption key from the file owner.

Propose method provides the following properties.

1. Unidirectional- After receiving access permission the data will be access the proxy server can transfer a cipher text for Alice to a cipher text for Bob while he cannot transfer a cipher text for Bob to a cipher text for Alice.

2. Non interactive- The access permission can be created by the stored person or file owner without any trusted third party and interaction with him.

3. Key optimal- The size of the secret key of the receiver is constant and independent.

4. Collusion safe- The secret key of the owner is secure from users even if the receiver can compromise the proxy server.

5. Non transitive- to receiving the access permissions computed by A for B and B for C. The proxy server cannot transfer a cipher text for A to C.

6. File based access- For one request the receiver can only access only one file. This can improve the security of the outsourced files and access record.

III. PROPOSED WORK

For secure data transfer in cloud we introduce conditional proxy re encryption. The construction of conditional proxy re encryption scheme offers many advantages over previous systems including chosen cipher text security, uni directional and collusion resistance. In this we propose a system for cloud computing where the receiver can only access one file instead of all files. The access permission can be decided by the data owner instead of the trusted party. Further our schemes are secure against the collusion attack and will also detect the distributed DOS attack which possible on proxy server in which server can't proceed to legitimate work and this system will available to owner on his/her android based device and also can get notifications. To enhance the security level we provide secret key on android devices. Our proposed work based on: The access permission is decided by the data stored person or owner. therefore the proposed work secure against all collusion attacks. The existing scheme is not detect the distributed Denial of service attack which possible on proxy server to make the server busy and stop to respond to authorized user by sending request repeatedly . The proposed work makes the system DDOS free. This propose work provides the facility to system users to access the system and can get the request notification on android based devices.

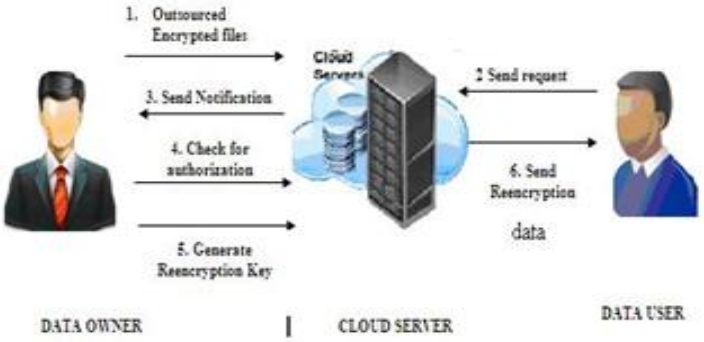


Fig: System Architecture.

IV. ALGORITHMS USED FOR IMPLEMENTATION

a) Algorithm:- Encryption and decryption algorithm.
Input: Message or data/cipher text.
Output: cipher text/original data
(1) Advanced Encryption algorithm.

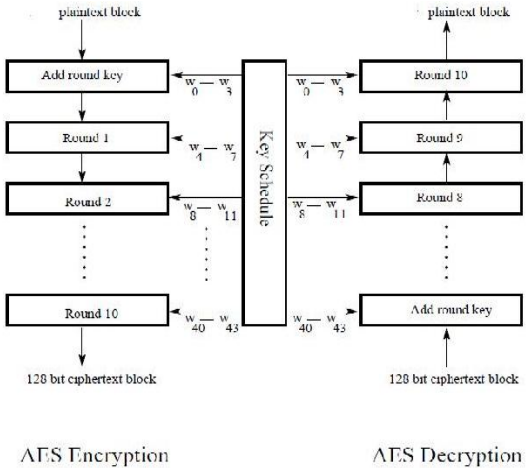


Fig 2: structure of AES algorithm

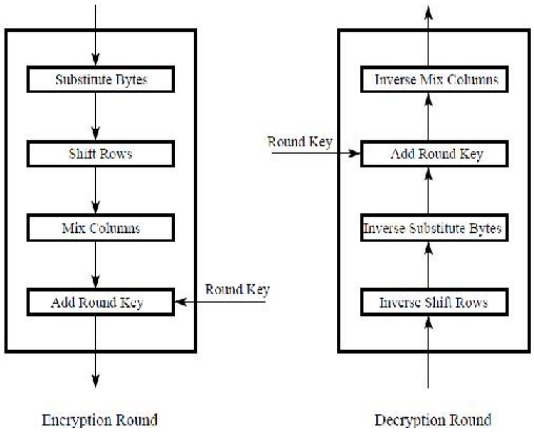
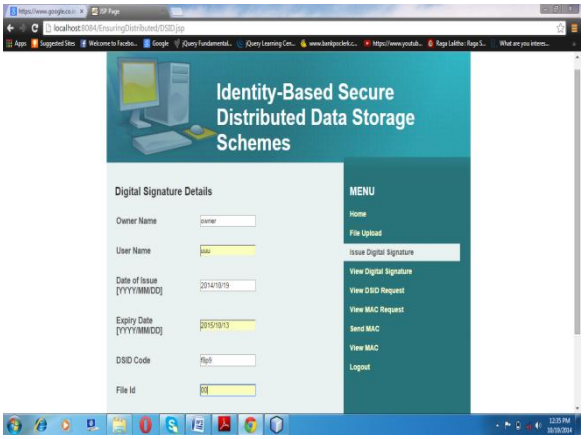


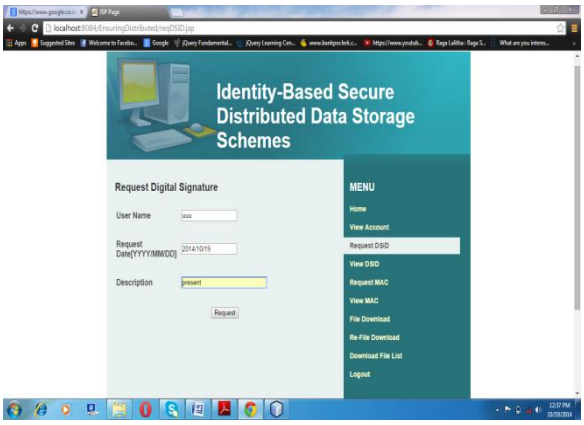
Fig 3: different steps

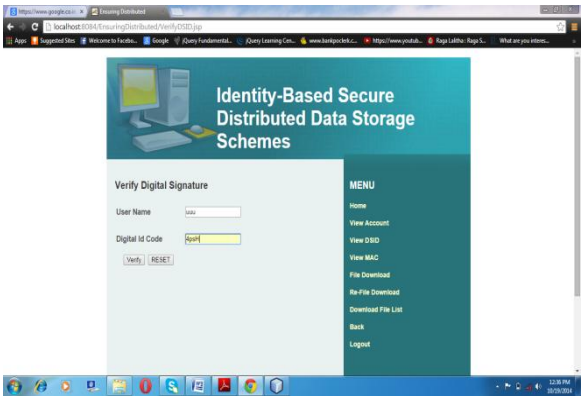
b) Key generation algorithm:-
Input: ID of the owner and User
Output: Secret Key.

c) Base 64 Algorithm:-
Base64 algorithm is designed to encoding the binary data, stream of bytes into a stream of 64 printable characters. In which the binary data is transformed to ASCII text. This can be transported in email without problems. In the recipients side the data is decoded and the original file is rebuilt.
The Base64 encoding process is to:
Step 1: Divide the input bytes into blocks of 3 bytes.
Step 2: Divide 24 bits of each 3-byte block into 4 groups of 6 bits.
Step 3: Map each group of 6 bits to 1 printable character based on the 6-bit value using the Base64 character set map.
Step 4: If the last 3-byte block has only 1 byte of input data, pad 2 bytes of zero (\x0000). After encoding it as general block and over ride the last 2 characters with 2 equal signs (==). So the decoding process knows 2 bytes of zero were padded.
Step 5: If the last 3-byte block has only 2 bytes of input data, pad 1 byte of zero. After encoding it the normal block override the last one character with one equal signs (=) so the decoding process knows 1 byte of zero was padded.
Step 6: Carriage return and new line are inserted into the output character form. They will ignored by the decoding process.

V. RESULTS







VI. CONCLUSION

Cloud computing is a distributed system where users in deferent domains can share data among each other. Identity-based proxy re-encryption schemes have been proposed to outsource sensitive data from the owner to an external party. Cloud computing is a distributed system. Where different users in different domains can share data or file among each other. Different Identity-based proxy re-encryption schemes have been proposed to outsource sensitive data from the owner to external parties. They cannot be employed in cloud computing process. As security of data or file storage is important and also the security of data transfer is important. The security of data transfer by introducing the identity based secure encryption and re encryption. It will provide many advantages like collusion-resistance over the previous schemes and will get the notification of user request on android based device and will also provide security against Distributed Denial of Service attack and it provides secure model of cloud storage with safe data forwarding.

REFERENCES

[1] Bouganim L, Pucheral P. Chip-secured data access: Confidential data on untrusted servers. In: Proceedings: International Conference on Very Large Data Bases - VLDB 2002. Hong Kong, China: Morgan Kaufmann 2002: 131-142.

[2] Maheshwari U, Vingralek R, ShapiroW. How to build a trusted database system on untrusted storage. In: Proceedings: Symposium on Operating System Design and Implementation - OSDI 2000. San Diego, California, USA: USENIX; 2000: 135-150.

[3] Ivan and Y. Dodis, "Proxy cryptography revisited," in Proc.Network and Distributed System Security Symposium - NDSS'03, (San Diego, California, USA), pp. 1–20, The Internet Society, Feb. 2003 .

[4] Han, J., Susilo, W. & Mu, Y. (2013). Identity-based data storage in cloud computing. Future Generation Computer Systems: international journal of grid computing: theory, methods and applications, 673-681.

[5] L. Wang, L. Wang, M. Mambo, and E. Okamoto, "New identity based proxy re-encryption schemes to prevent collusion attacks," in Proc. Pairing-Based Cryptography - Pairing'10, vol. 6487r, Dec. 2010.

[6] M. Green and G. Ateniese, "Identity-based proxy re-encryption," in Proc. Applied Cryptography and Network Security - ACNS'07 , vol. 4521, pp. 288–306, Springer, Jun. 2007.

[7] Qin Liu, Guojun Wang and Jie Wu, "Efficient Sharing of Secure Cloud Storage Services," 10th IEEE International Conference on Computer and Information Technology, 2010

ABOUT AUTHORS

G. Srilakshmi is currently pursuing her M.Tech Computer Science & Engineering Department in Kakatiya Institute of Technology and Science, Warangal. She received her B.Tech in Information Technology from Vaagdevi Engineering college, Warangal. Her area of interests includes Data mining and Network security.

M. Preethi is working as Assistant Professor in the Department of CSE, KITS, Warangal. She received M.Tech. Computer Science from Kakatiya institute of technology & science. Her area of interests includes Data mining and Software Engineering.

