Advanced Multi-Encryption Technique in Cloud Computing

SHRIDHAR.B*
CSE ,Viswesvaraya Technological University,
Rajiv Gandhi Institute of Technology,Bangalore,
shridhar.ramesh@gmail.com

PAVAN GUJJAR PANDURANGA RAO
Research Scholar ,Dept.of CSE , Andhra University ,
Vishakhapatanam,Andhra Pradesh Karnataka ,India
drgppavan@yahoo.com

Abstract— ***Cloud Computing is one of the latest technology and it is growing rapidly .Cloud Computing provides service over the internet. In the existing approach the revoked users are not tracked properly and there is no extra protection on the data that is uploaded to the cloud server. The users are not authenticated properly. The best approach is that the users are authenticated twice. Once with the help of password users are authenticated and then the secret code will be sent to the authenticated users mobile with the help of interfacing technology like GSM and then the user's should enter the secret code to authenticate they are the valid users. In this paper the data that is uploaded to the cloud server is encrypted twice by the data-owner and that data is later re-encrypted by the cloud server. Multi- layer encryption technique is performed in order to provide extra security for the data that is uploaded to the cloud server. The data that is uploaded to the cloud server is highly secure and user's authentication is validated twice so that the valid user can access data flexibly and reliably.***

Keywords— Cloud Computing, Multi-encryption, Revocation Tracking, Authenticated Users, Interfacing Technology

I. INTRODUCTION

Cloud Computing is a style of computing [2] where applications are provided to users as services over the web. It provides the users to access the [3] data globally in an efficient way. Cloud Environment presents the opportunity to enhance the user experience by providing a boarder communication path for reaching out the user or for providing a series of business services to the user with respect to the application features. The [1] Services that the cloud provides is security and availability. Users in the remote places can access the data from the cloud. In the military applications the data that has been uploaded to the cloud should be highly secure and confidential. The data that has been uploaded to the cloud server is not secure and the files that are uploaded to the cloud server may be attacked by hackers. Current approaches in the cloud computing there is no security and confidentiality for the data public cloud is a shared computing infrastructure that anyone can access so that the users authentication should be validated thoroughly. Cloud Computing provides storage as a service in which it provides the space for the data. Privacy of the users is the important concern about cloud computing. The different reason for adopting the cloud is web-scale infrastructure, [8] dynamic allocation, no hardware or software to install. The major benefits are to deliver the services in less costly manner.

The major drawbacks [1] in the existing approach:

1. If the unauthorized user tries to access the authorized users data by hacking the users password then the data may be modified.
2. If the data is highly confidential then that data should be protected.
3. There is no means of knowing who has attacked the file or who has modified the file.
4. There is no extra protection for the data that is highly confidential.
5. If the data owner has [1] lost the data then the data owner needs to download the data from the cloud server which leads to very high costs.
6. Anyone can upload the data to the cloud server so that the data owners should be registered or the data should be encrypted.
7. There is no [4] revocation tracking so that if the users get the password of the users they can access the data.

In this paper the major task or the challenging task is to maintain the security for the data that is uploaded and the challenging issue is to allow only the authorized users to access the data from the cloud. Then the unauthorized users should be blocked or should not be allowed to access the data. In this paper multi-encryption technique is introduced to provide the extra security for the data. Thrice the encryption is performed. The double-encryption is performed by the owner and the single-encryption is done by the cloud server. If the user has to access the data then three-layer decryption should be done so that the security and confidentiality of the data is high. The challenging issue is to monitor the attackers and to keep track of revoked [5] users.

Another task is to protect the data by performing multi-encryption on the owner and the cloud encrypted data. This is helpful if the data is highly confidential. Privacy of the users is taken in to account and only the authorized users are allowed to access or download the data to the cloud. Cloud Admin issues the token and maintains the keys of the users.

The advantages of using proposed system is:

1. It allows only the authorized users to access the data by authenticating or validating the users twice. Once it authenticates the user with the help of username and password and once again it asks for secret code that will be sent to the users mobile so that the users enter the secret code and the users will be re-authenticated and allowed to access the data from the cloud server.
2. The data owner encrypts the data twice so that the data is confidential from the cloud.
3. Automatic Messages will be sent to the cloud admin so that the there is a way of identifying the revoked users easily. The revoked users will be blocked by the cloud admin. The data owner gets the acknowledgement about the blocked user. So that there is a way of identifying the revoked users without the intervention of the owners.
4. After the data owner encrypts the data twice later the cloud server re-encrypts on the owner data and provides the extra protection on the data that has been uploaded by the cloud owner.
5. If the data owner has lost the data then the data could be downloaded from the cloud server and re-encryption is performed and a copy of the data can be retained.
6. Only the registered users are allowed to upload the data to the cloud server and only the authorized users are allowed to access the data in a reliable manner.
7. The Revocation [5] is tracked with the help of interfacing technology called as gsm.

II. RELATED WORKS

In [4] it is difficult to manage the databases for large-scale industries.Cloud provides the service as data storage for large-scale industries. Based on the attribute of the storage systems. The data plays a important role in any of organization so it should be protected .Internet plays a very vital role in an organization so the privacy and security of the users should be maintained. In the Bank there will be cashier and accountant and clerk each and every role should access the data based on their related work. So the attributes are divided. Only the related attributes groups should access the data. In this paper encryption is performed base on the role of the attributes. The relates secret keys are generated so that the users can access the data easily and reliably. In [6] it is difficult if the users in the group are blocked then if a new user is added to the group.A new keys should be generated for each and every user. So a technique is used called as broadcast encryption. So that all the users in the group will get the intimation that the users are blocked and the keys are distributed to the users with the help of technique called as broadcast encryption. In [7] the log files are used to store the attacker's details so it not dynamic this drawback is overcome in this paper dynamically with the help of technology called as GSM.It is difficult to maintain the log files. In this paper an approach has been proposed in which the revokers details are dynamically monitored by the cloud admin. The cloud admin sends the acknowledgment messages about the revoked users .cloud admin blocks the users. In [8] cloud servers the hackers or attackers are not blocked automatically. The data is stored in untrusted clouds. The security is very less in the mono layer encryption technique. In this paper a multi-layer encryption is performed so that the data is protection is high. The confidentiality of the data is maintained from the cloud server. In [10] symmetric keys are used so that if the attackers get a single symmetric key he can download the data from the cloud server. In this paper symmetric keys are not used to encrypt the data. Based on the attributes of the users the keys are divided and they are allowed to get the data. The drawback with this approach is that if the user in the group shares the symmetric key with others any one can retrieve the data.

III. AUTHENTICATION AND DATA SECURITY

In this paper remote users needs to be registered after that they are validated with the username and password in the first step authentication. In the second step with the help of gsm, messages are automatically sent to the authorized mobile phone. In second step verification users are allowed to enter the secret code that is sent to your mobile for validation. After successful login user will request for two secret keys from the data owner and one secret key from the cloud server so that they can decrypt the data that is existing in the cloud server. The proposed work provides the security for the data that has been uploaded with the help of multi-encryption technique. Double-Layer Encryption is done by the data owner so that the data that is uploaded to the cloud server is confidential and secure. Single-Layer Encryption [1] is done by the Cloud Server. Data protection is very high. If the users are not able to successfully login then the message will be sent to the cloud admin so the cloud admin can block the unauthorized users.

The cloud server can unblock the blocked users. With the help of secret question that has been entered during registration is asked if that answer matches with the user enter answer. Then the users are unblocked.

IV. ARCHITECTURE

The architecture of the proposed work consists of data owner, cloud server, cloud admin, remote users, and gsm:

A. *Data Owner*

Data owner uses the technique of double layer encryption in which the users needs two secret keys to decrypt the data. Cloud server uses the technique of mono layer encryption in which re-encryption is done on the owner encrypted data. Once again the user needs to request for one more secret key so that the decryption of the data can be done.

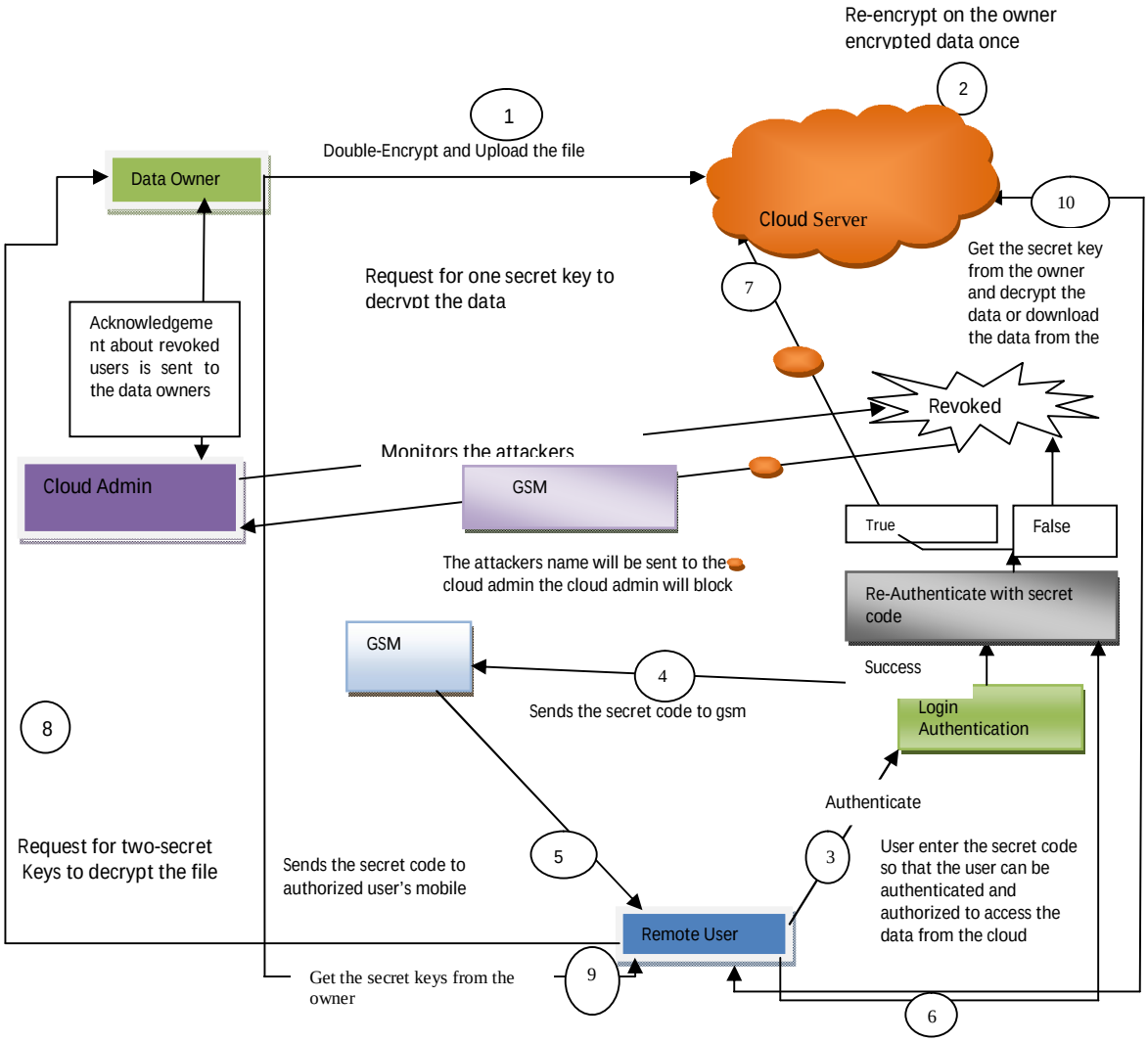

Fig. 1 Multi-Encryption technique architecture

Data Owner can view the privileges of the users and send metadata to the cloud server and verify the files and delete the file.The user privileges can be viewed by the data owner.

B. *Cloud Server*

Cloud Server performs encryption operation on the owner encrypted data. A mono-layer encryption is performed by the cloud server. Cloud Server provides one secret key to the user upon request from the authorized user.Cloud Server can view all the owner files, Modify Owner file. Server can unblock the blocked users. Server can view the privileges of the user.

C. *Remote User*

Remote Users before accessing the secret keys from the owner and cloud server. User authentication is checked twice before accessing the secret keys. Once user validation is performed with login authentication and second time the users authenticate is done by sending the secret code to the users mobile.If the user is revoker then the cloud admin automatically blocks the unauthorized users. Second type of validation is checked by using interfacing technology

called as gsm.Gsm is used to send the messages to the users as well as to the cloud admin.Remote User should request two secret keys from the cloud owner and one secret key from the cloud server so that the data that is encrypted can be decrypted.

D. Cloud Admin

Cloud Admin monitors that attackers and automatically blocks the attackers. Cloud Admin can keep track of the revoked users. Automatically when the revoked users try to login, name of the revoked user is automatically sent to the Cloud Admin.Cloud admin can create the role of the users and the data owners.

V. PROPOSED WORK

In this paper we are performing multi-layer encryption on the data that is uploaded to the cloud server. Data is more secure and confidential. The challenging issue in this paper is to authenticate the authorization of the users two times. In the proposed work three-layer of encryption is done for providing more protection for the data and two types of login authentication or verification is done. First the users are validated with normal login name and password and in the second step verification the secret code is sent to the authorized users mobile to authenticate he is the authorized user. If the users enter the valid secret code then he is allowed to access the data from the cloud server. In this paper cloud admin keeps track of the revoked users who try to attack the file. If the second step authentication fails then the unauthorized users name is automatically sent to cloud admin with the help of an instrument called as modem. The Cloud Admin blocks the users and sends the acknowledgment of the blocked users to the owners. In this paper the Data Security, Data Availability, Data Protection, Authentication and Revoked users are tracked and blocked. User Authentication is done twice so that only the authorized users are allowed to get the data from the cloud server. Blocking of unauthorized users is done automatically no log files are maintained. Privacy of the users is maintained which is the critical important task in cloud is computing.

VI. CONCLUSIONS

In this paper the multi-layer encryption technique is introduced so that the data security and data confidentiality is achieved. For Confidential data more security is provided. By authenticating twice we are allowing only the authorized users to access the data. Only the unauthorized users are tracked and blocked. Revoked users are monitored thoroughly and blocked so that the attacks on the files can be reduced. Two-step verification process is included to allow only registered users are allowed to get the data from the cloud.

REFERENCES

[1] M.Nabeel, E.Bertino," Privacy Preserving Delegated access control in Public clouds", June 2013.
[2] M.Nabeel and E.Bertino, "Attribute based Group Kay Management Scheme", IEEE Transactions on Dependable and Secure Computing.
[3] A.Fait and M.Naor, "Broadcast Encryption". In Proceedings of the 13th Annual International Cryptology Conference.
[4] D.Naor,M.Naor and J.B.Lotspiech "Revocation Tracing Schemes for stateless receievers",in proceedings of the 21st Annual International Cryptology,2001
[5] X.Liu, Y.Zhang ,B.Wang,J.Yan,"Mona:Secure Mutli-owner Data Sharing in the group"
[6] M.Nabeel and E.Bertino,"Towards attribute based key Management" ,"IEEE Tran. On parallel and distributed systems.
[7] Brown, L. D., Hua, H., and Gao, C. 2003. A widget framework for augmented interaction in SCAPE.
[8] Y.T. Yu, M.F. Lau, "A comparison of MC/DC, MUMCUT and several other coverage criteria for logical decisions", Journal of Systems and Software, 2005, in press.
[9] Spector, A. Z. 1989. Achieving application requirements. In Distributed Systems, S. Mullen

