IMPLEMENTAION OF PRIVELIGE DATA IN CLOUD COMPUTING BY DOUBLE ENCRYPTION CONCEPT

Govindaswamy H R, Bhanu K N
Department of MCA, Rajarajeswari College of Engineering, Bangalore, India
govindaswamy.hr@gmail.com,bhanu.kn@gmail.com

ABSTRACT-This paper implements secure data in cloud computing by double encryption method using RSA. Double Encryption for secure outsourcing data in the cloud. This method solves key escrow problem and Data reveal problem by RSA algorithm of asymmetric key approach. In existing mCL-PKE method, there is Certificate-less Encryption and also single encryption and it is half disrupted by the "CLOUD" and remaining half is decrypted by the user but in my method there will be certified for the User and two layer encryption. The cloud will going to decrypt the outer layer encryption and user will going to fully decrypt inner layer encryption only for doing this we can secure the data / information well be highly secured.

Index Terms— DEA, Decryption center, RSA algorithm, cloud computing, Asymmetric key, Two Layer Encryption

I. INTRODUCTION

In this newly environment of double encryption concept. certification of the users provide high security to the data and asymmetric key approach (RSA) is very convenient in key distribution. The implementation method is that RSA can also be used for performing digital signature. In Existing system Two Layer Encryption and it is extended from the previous method of mCL-PKE. mCL-PKE works on certificate-less encryption and user are not certifie by any authorize entity, but in my method, there will be certified for user, certification of the user also provides security of the information in the cloud, due to this only permitted user can use the data as mentioned in [1],[2]. The Double Encription Approach (DEA) this two layer encryption approach addresses the drawbacks of the mCL-PKE . In DEA approach user will have to get register to the participants to get the secret key for decryption of the encrypted documents. The basic method is, owner encripts the documents and send these encrypted documents to the cloud, now cloud decript the outer-layer of the encripted content and send these document to the register users, now user fully decripts the encrypted contents ,it shows an inner layer of the encription of the secret keys.

II. SYSTEM ARCHITECTURE

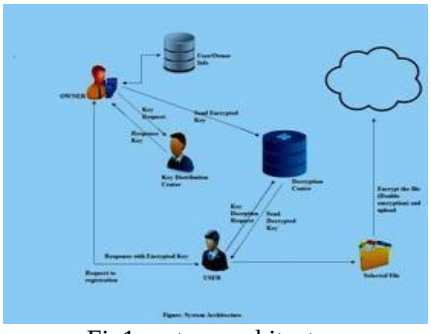

Fig1.system architecture

In this paper the proposed method is divided into three main parts they are:

1) Owner

2) Cloud

3) User

Cloud is further divided into three subparts Encrypted Storage(ES),DecriptionCenter(DC)KeyGenerationCenter(KG)ThecloudhasthreesubpartsEncriptedContentStorage,K eyGenerationCenter(KGC),andSecurityMedeationServer(SEM).Encripted Content Storage is going stores the encrypted documents KeyGenerationCenter,is going to generate the KGC key for encryption and Security Mediation Server partially is going to decrypts the encrypted information.Cryptography is the art and science of achieving security bye encrypting/encoding. And also it used for securing the data to non readable longuage,the process of encoding plain text messages into secret message is called as encryption, for encrypt the data there are many techniques are there. Encryption is one of technique to protect the data from spiteful and not registered users, encryption of the documents can be more than one layer.

III. RSA ALGORITHM

In double encryption technique the RSA algorithm is one of the best algorithem.On this algorithm we are going to use two important keys that private key and public key,public key is used for encrypting the information in the form of non readable language and private key is used for decrypting the encrypted document/information. the In the real-world public-key cryptosystems RSA algorithm is one of the best algorithm and is widely used to secure data transmission. In such a cryptosystem, the user can easily view the encryption key because it is public but decryption key is kept as top-secret. In RSA, this asymmetry is based on the real-world difficulty of distributing the product of two large prime numbers. Basically RSA algorithm works slow. and because of this

commonly used to directly encrypt user data as mentioned in [5] RSA pass the encrypted shared keys for symmetric key cryptography, which can start doing encryption-decryption of information very fastly.observance is the important thing in RSA algorithm impotent thing is to find the three large positive integers that is d,e and n such that with modular exponentiation for all m and even knowing m and n even m can be extremely difficult to find d.

IV. DOUBLE ENCRYPTION

The implementation of double encryption method is to secure the TEXT Data Items of the Data-Owner by Double Encryption in Cloud Computing. The basic method is Double Encription of the documents means there is two layer encryption of the data orinformation. I extend the previous mCL-PKE method but in my system there is certification of the users. The simple method is owner will encrypt the contents two times using thegenerated key and store the document to theEncripted Storage when user request any document thedecription center fetche the requested document and decrypts the outer layer of encryption and gives to the user,now user fully decrypts the document.

In this section I propose the basic mCL-PKE method then my improved method, the basic public key encriptioniscertificate-less method, in which users certificationisnotnecessarywhichreducesthemanagementco st.Butthis method compromises to the malicious users, any malicious user can access the data for malicious use. The shortcomings of this is addressed by the improved method in my paper, in which user must have to register to the owner then only user can access the information. So this ideology enhances the security of the data. The basic mCL-PKE method is going to do single encryption and half decrypted by the cloud and remaining information will be decrypted by the user, this method is proposed to reduce the decryption time of the user, but partially decryption of the data reduce the security of the content, but in this method there is double encryption of the data, there is two layer of the encryption, in which the cloud will going to encrypt thr outer layer decrypted by the cloud and inner layer encryption is decrypted by the user, hence security is high in my improved method. The overall result comes that securityis very high in my system as compare to previous mCL-PKE method.

.

V. IMPLEMENTATION OF DOUBLE ENCRYPTION PROCESS

Fig 5 shows the user registration form user as to register with administrator .the owner will going to give the permission to the user to access the file. In our paper the user request the owner for registration purpose and the same user request the decryption centre for decrypting the key which is provided by key distribution centre. Owner plays an important role in our project, he request key from key distribution center for a user and encrypts that key and sends it to decryption centre. The owner also stored the doubly encrypted file. After registration the user choose file and encrypt that file use the key provided by owner and stored the encrypted file in cloud.

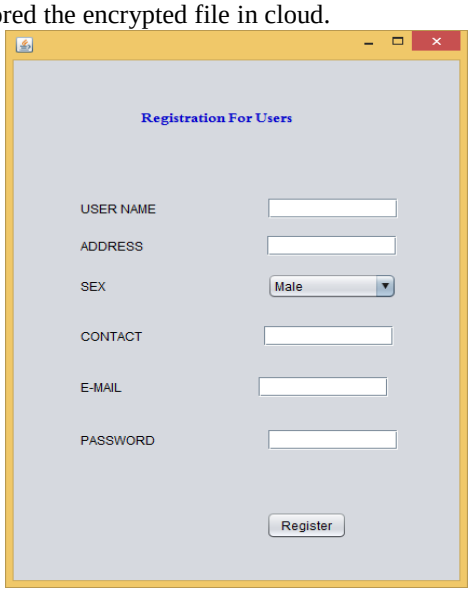

Fig2.user registration form

Fig3.owner home page

Ofter the user is registered the owner will going to check who are all the clints are registerd and the owner will going to send the keys to that user for doing their work.

```
mysql> desc data_owner;
+---------------+-------------+------+-----+---------+-------+
| Field         | Type        | Null | Key | Default | Extra |
+---------------+-------------+------+-----+---------+-------+
| owner_name    | varchar(22) | NO   |     | NULL    |       |
| owner_address | varchar(50) | NO   |     | NULL    |       |
| sex           | varchar(10) | NO   |     | NULL    |       |
| contact       | varchar(12) | YES  |     | NULL    |       |
| email         | varchar(30) | NO   |     | NULL    |       |
| department    | varchar(30) | NO   |     | NULL    |       |
| password      | varchar(15) | NO   |     | NULL    |       |
+---------------+-------------+------+-----+---------+-------+
7 rows in set (0.01 sec)
```

Fig4.description of data owner table

The above figure shows the description of data owner table this table contains owner name,adress contact, email and password .it cintains the complete details of owner .ofter owner registration completed the owner details will be stored in this table.

```
mysql> desc owner;
+----------+-------------+------+-----+---------+-------+
| Field    | Type        | Null | Key | Default | Extra |
+----------+-------------+------+-----+---------+-------+
| owner_id | varchar(15) | NO   |     | NULL    |       |
| password | varchar(15) | NO   |     | NULL    |       |
+----------+-------------+------+-----+---------+-------+
2 rows in set (0.04 sec)
```

Fig5.description of owner table

The above figure contain the owner_id and Password. The owner_id and Password will be stored in owner table.

Fig6.verifyication page

In this form verifying the user information whether the user has enterd correct email and mainly encrypted key and also offer verifying the details it generate the decrypt key. contains owner name, dress contact, email and password .it contains the complete details of owner .ofter owner registration completed the owner details will be stored in this table.

VI. Conclusion

The implementation of the double encryption process is going to provide certification for the user to highly secure the data or information. In this process we are using an asymmetrical Key approach that is Ron Rivest, Adi Shamir, and Leonard Adleman (RSA) algorithm for key distribution. The future enhancement of this double encryption process and RSA can use for performing digital signature and it has also helped full for providing high security in future. In this method I'm using basic Mediated certificate less public key encryption (mCL-PKE) key for Key distribution and also I'm using two important key that is public and private key .public is for encrypting the document / information in the form of non-readable language means it will going provide security for that document or information. The shortcomings of this method are addressed by the improved method in my system, in which user must have to register to the owner then only user can able to access the information. So this ideology enhances the security of the data.

VII. Acknowledgement

The authors of this paper are thankful to the Management, RRGI,Bengaluru and Principal, RRCE, Bangalore for their continousencouragement and support throughtout the work.

References

[1].Mr. Bhavesh Rahulkar received the BE (ComputerTechnology) From RTM Nagpur University, Nagpur (M.H.) in 2008Mr.

[2]. Praveen Shende, Asst. Prof.,CSE Dept. C.S.I.T.Durg, India, received B.E. (Computer Sc.) in year 2009

[3]. Mohamed Nabeel, Elisa Bertino, Seung-Hyun Seo, Xiaoyu DingMembers of IEEE –An Efficient Certificate-less Encryption for Secure DataSharing in Public Clouds‖ June 2013.

[4]. Zhiguo Wan, Jun"e Liu and Robert H. Deng. Senior Member, IEEE–HASBE: A Hierarchical Attribute-Based Solution for Flexible and ScalableAccess Control in Cloud Computing‖ April 2012.

[5]. https://en.wikipedia.org/wiki/RSA_(cryptosystem).

Govindaswamy H R is currently as PG student of Rajarajeswari College of Engineering pursuing final year of Master of Computer Application.

Bhanu K N is currently working as Associate Professor in the Department of Computer Applications. Her research and professional career spans for about 12 years of Teaching and Industrial Experience. She obtained her MCA., from IGNOU, New Delhi, M.Phil., in Computer Science from VMU, Salem and presently Pursuing Ph.D., in Computer Science from Rayalaseema University, AP. Her expertise is primarily in the domains of Wireless Sensor Networks, sensor clouds, Adhoc Networks and Sensor Big data analytics.