Efficient Data Sharing Techniques To Improve The Security Usingnetworks

K. SOWMIYA

SCHOOL OF INFORMATION TECHNOLOGY, VIT UNIVERSITY,
VELLORE, TAMILNADU, INDIA
Sowmiya.k2012@vit.ac.in

Abstract: The present trends and spreads in data sharing in the internet and in social networks is unsecure .So nowadays people demanding for security .In such case, this paper helps to share the data in a secure way by encrypting the data and decrypt it .Though it has several features in decryption and encryption. Nowadays decryption done by using private keys .This common thing that is used is for security purpose .Thecypher textingis a new technique that is used forcryptographic purpose .Throughits work well it has only one drawback that is escrows problem. This problem can be solved easily by introducing new SFTP protocol.Hence implementation and proposed plan will manage and it will share the data securely on the internet .

1. Introduction:

The recent growth of networking ,people can store and share their data through online .By sharing the photos in an online, while chatting with friends and colleges or by sharing their own medical records in online with their private doctors for verification .Aspeople use these technologies , they only anxiety about security .Inappropriate usage of data by severingor unwanted people can use the data .People would like to make their personal data visible only with their qualified they mentioned. The encryption helps for cryptographic purpose and it also provides attribute base encryption this involves over many people that decrypts the ciphertext, and obligated in their own material . It involves the different users and allows to decrypt it based on their policies .Thus, every user can decrypt their own data with security .By applying a new technique like generating the keys that can be only private keys of users.

2. LiteratureSurvey:

In the previous paper they founded best method for sharing the data in secure way the is attribute base system though it works fine it has drawback called escrows problem .To overcome this problem we can introduce new protocol .It will generate user secret key to perform a two way communication .This acts between only to the client and the server side .With the bases of attribute encryption it deals with the huge difficulty and other obtrusion , the security maintenanceon a specific host is difficult .To solve this problem the encrypted data should be stored in the server .

3. Existing System:

Sharing the data in online enables to data owner to define about the owner access over the user attribute and their own policies should be distributed .And another thing is user manual , this method enable encrypted message at a certain time .And these application have some mechanism by changing the lock . However the manual user should generate their own secretkeyinput of data server , and it could be decrypted the cybhertexts which is received by the users by decrypting the ciphertexts .Hence the escrows problem exists in this method.

3.1 Proposed system:

To overcome the escrows issues in encryption,protocol key issuing is used during data sharing and it also generates the secret keys in the two way communication protocols by generating the keys and sharing Contributions: In this paper,the proposed method is encrypting the data and share it in a secure way ,which has the following feats . In this first thing escrows issues determined by finding the new protocol and it also has some features like , it can perform two way communication in storing data .This protocol determines to acquire any secret detailed information .

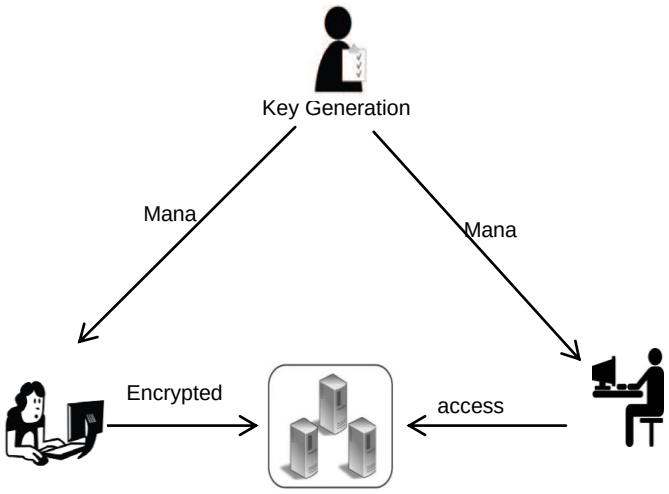

Fig .1. Data sharing system Architecture

3.2 Modules:

These organizing is divided into various sections .It pacts about the protected in desires and another section describe about the cryptographic work , this analyze the efficient secure proposed scheme .Similar way all sections involve like this in security purpose

3.2.1 Architecture for sharing the data :

In this , it briefly explains about the sharing the data in a form of security

3.2.2 Managing keys and description:

(1) Generating the keys it has the separate sectors,it invokes the users to update the keys about it .It has the various access in a single user on the basis of attribute .

(2) (2)Storing the data in a particular center in a specific service it controls the users by storing the data and provide the services,and it also has authority to create the user key

(3) Ownership of data, it is the client side informationit, if it wishes to upload external data storing it will reduce the cost and savings, it enforces its own data by encrypting the data

(4) If the user wants to access the data, they should stratifies some kinds of attributes by encrypting the data in a specific group

Since it manages the key and stores the data into a center,it should be in plain text so that data will be shared easily .Still it has some problemsecrete keys to users. By introducing a new protocol the keys of ownership will be independent to the user.

3.2.3 Security in conspiracy and resistor:

It is intensely proved that security for the proposed scheme that is discussed in the previous organizing section .This security policy is based on encryption and this technique is related to private keys.and the personalized values are selected and it be combined in a particular proposed method .If the user wants to decryptit, theconspirators should be recovered. For that purpose it should have a private key method .Anyhow it will take the result in the form of values. This value is designed according to keys this will help to fulfill shared technique. Confidential data must be shared against the explicit users it will not enough attributes so it is partially guaranteed to the users.

4. Result :

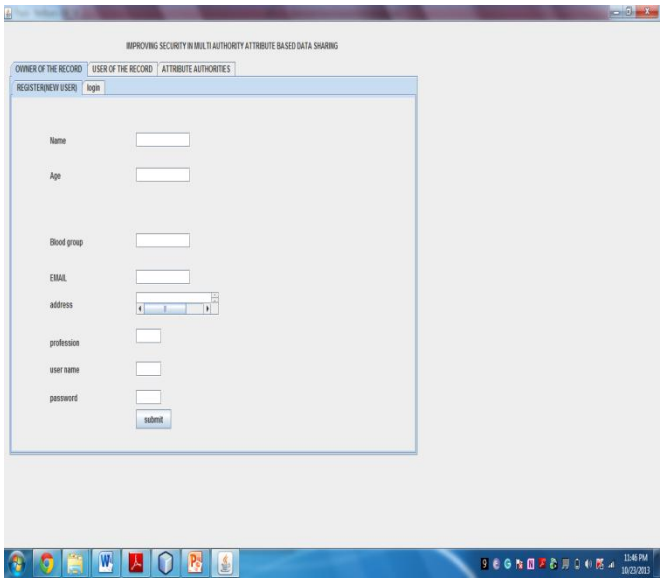

Fig .2 . improving the security in data sharing

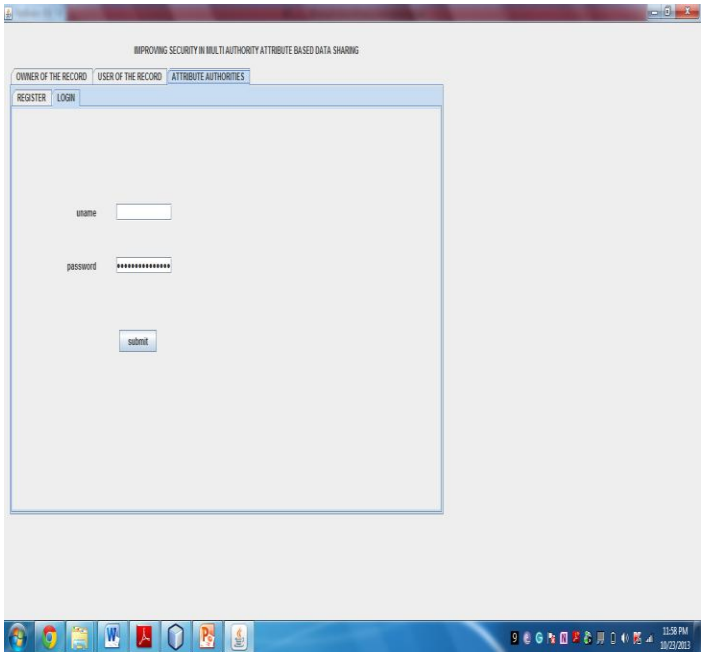

Fig .3. login for existing user

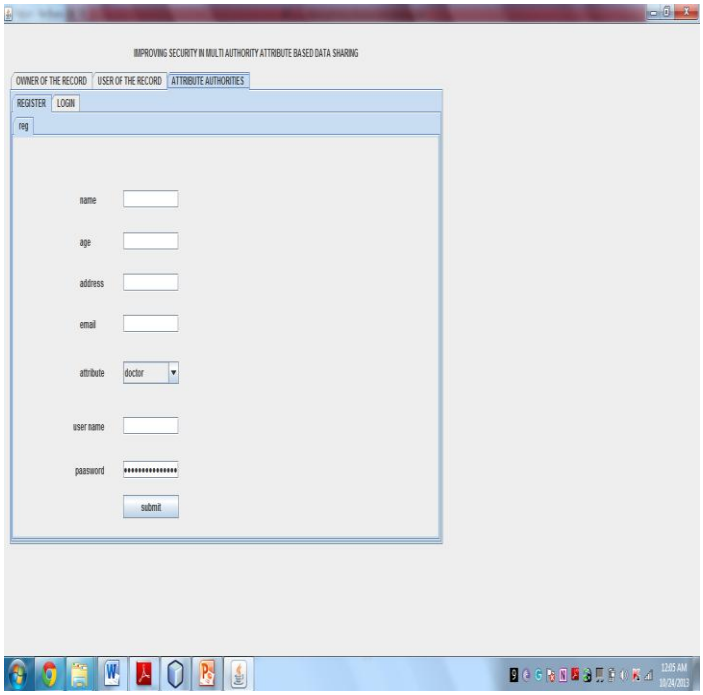

Fig .4. regstration for new user

5. Conclusion :

This application deals about the information security and its streamline which is very crucial outfit for sharing the data .In this paper the proposed method featuring the issues about encrypted keys and this can be solved using generating a new keys .That is more secure than the previous way it is very helpful for between the client and server. Thus the proposed method elevate the data in a secure way while sharing the data. Therefore this method attain security and privacy so this method is more climbed to manages the data while sharing in the network work .

6. References:

[1]. Attrapadung H. Imai, “conjunctive broadcast and attribute based encryption ,” proc paring 2012

[2]. D.Boneh ,M.K Franklin ,”identify based encryption from the weli paring ” proc CRYPTO 2010,LNCS Vol,2139,pp.243

[3]. M Chase , .S.S.M chow, “improving privacy and security in multi authority attribute based encryption ”proc .ACM conference on computer and communication security pp.134-130,2012

[4]. C.Dong,G.Russello, and N.Dulay, ” Shared and searchable encrypted data for untrusted servers ” in journal of computer security 2011

[5]. S.Yu,C.Wang ,K.Ren and W.Lou “ Achieving secure and scalable and fine grained data access control in cloud computing ”,in IEEE INFOCOM’10, 2011

[6]. S.Rafaeli, D.Hutchison,”A survey of key management for secure group communication ”, ACM computing surveys

[7]. K.C.Almeroth,M.H.Ammar,”multicast group behavior in the internet multicast backbone “,IEEE communication magazine

[8]. M.Pirretti, P.Traynor,P.McDaniel, B.Waters,”secure attribute based system “, proc. ACM,conference on computer and communication security 2008.

[9]. S.S.M.Chow ,”Removing Escrow from identify based encryption ”, proc PKC 2010

[10]. M.Belenkiy , J.Camenisch,M.Chase,M. Kohlwesis , A.able Anonymous Credentials ,”proc Crypto 2009