A secure Zero Knowledge Free Re-Authentication Mechanism in AnonyControl Scheme

Ms.S.Kokila[1], Mrs.D.Vinotha[2]
PG Scholar[1], Research Scholar[2]
[1]M.Tech., Dept. of Computer Science & Engineering, PRIST University,Vallam ,Thanjavur.
[2]Assistant Professor, Dept. of Computer Science & Engineering,PRIST University,Vallam ,Thanjavur.

Abstract— cloud computing is a innovative computing standard,which enables supple,on-demand and low-priced usage of computing resources , but the data is outsourced to some cloud server and various concerns appear from it. A variety of scheme based on triple- DES algorithm have been proposed to secure the cloud storage.In this paper, present a anony control scheme to address not only the data privacy,but also the user identity privacy.In this project a new decentralized access control scheme for secure data storage in clouds that support anonymous authentication. Re-authentication machanism in anony control scheme user details among other clients.Re-authentication process to access the cloud with zero knowledge protocol.

Keywords— anonymity, centralized, decentralized, triple-DES, re-authentication, zero knowledge protocol.

I. INTRODUCTION

Cloud computing is a technology that uses the internet and pivotal remote servers to preserve data and applications. Cloud computing allows enjoyer and businesses to use applications deprived of installation and access their personal files at any computer with internet access. This technology grants for much more energetic computing by centralizing storage, memory, processing and bandwidth.

Cloud computing is a wide-ranging solution that delivers IT as a service. The flexibility of cloud computing is a function of the allocation of assets on demand. Before cloud computing, websites and server-based applications were executed on a specific system. Cloud computing is broken down into three segments application, storage and connectivity.

The cloud computing perform both centralized and decentralized approach. The centralized means only one authority to perform all process. The decentralized means multi-authority process. The decentralized approach better then the centralized approach. The decentralized approach is easy to maintain the all process. It reduces the time consuming.

The cloud computing only valid user to be access the cloud server, that means authorized person. Only valid user to decrypt the stored information from cloud storage. Number of user to be access the cloud computing process. Then the process and time consuming to large.

The proposed a decentralized approach is used to access the cloud. It is easy to handle the number of user in cloud computing. Then use the anonycontrol scheme, it is address not only the data privacy also the user identity. The proposed the main process of re-authentication mechanism using zero knowledge protocol in cloud computing.

II RELATED WORK

It is used in centralized approach, to access the cloud storage. Then its use attribute based encryption (ABE) algorithm. The algorithm to perform a symmetric key approach and does not support authentication. It is a centralized approach where a single key distribution center (KDC) distributes secret keys and attributes to all users. Regrettably, a single KDC is not only a single point of failure but difficult to maintain because of the large number of users that are supported in a cloud environment. Then it is perform the privilege access control scheme. It is only address the data privacy. First introduced in this process by Shamir that is identity based encryption (IBE) algorithm. Then it is not secure the data privacy and user identity. Then the process is very slow. It is not maintain the large number

of user to access the cloud storage. The computational cost is to high.

III PROPOSED METHOD

In this proposed system, a user revocation based on re-authentication approach based anonycontrol scheme is used. These techniques authenticate new users based on valid keys, user accessing the cloud proposed a distributed access control mechanism in clouds using anonyms. Admin can create and store a file with encryption based and two server based users can only read the file and the sender identity is hidden. The new users access the cloud using two server clients. The user process is left out from the cloud, server user provide secret key to authenticate cloud. Using this key the user's re-authentication process to access the cloud with zero knowledge protocol.

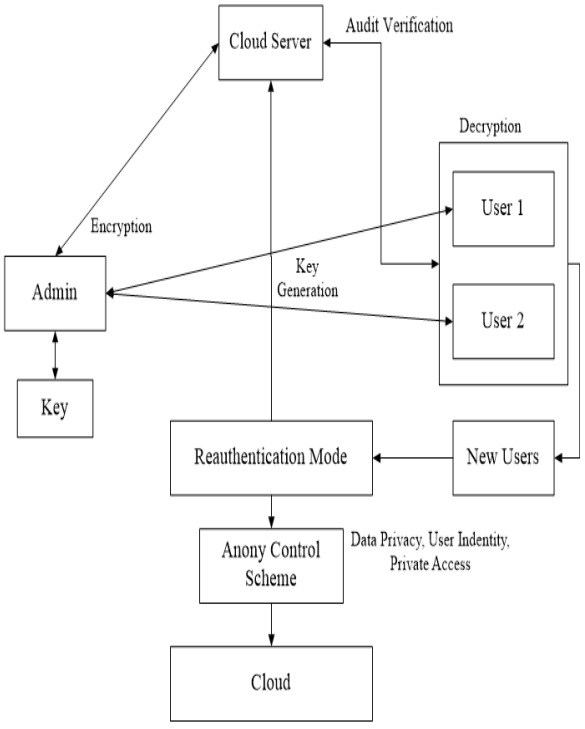

Fig 1: System Architecture

Then it is perform the four main process in the proposed system

A. User subscription and cloud registration

The subscription of business model where a user must pay a subscription price to have access to access the cloud. Cloud storage is a model of data storage where the digital data is stored in logical pools, the physical storage spans multiple servers (and often locations), and the physical environment is typically owned and managed by a hosting company. These cloud storage providers are responsible for keeping the data available and accessible, and the physical environment protected and running. People and organizations buy or lease storage capacity from the providers to store user, organization, or application data. Cloud registration is accessed through servers for storage with privacy identity.

B. Data transformation in cloud with user identity and data privacy

We emphasize that clouds should take a decentralized approach while distributing secret keys and attributes to users. It is also quite natural for clouds to have many KDCs in different locations in the world. The user send the information to the cloud, the data privacy and user identity is secured. The architecture is decentralized, meaning that there can be several KDCs for key management. Cloud Privileges is used to access the cloud for data transformation and storages.

C. Grant privileges access control

The most attractive part of the cloud computing is the computation outsourcing, it is far beyond enough to just conduct an access control. More likely, users want to control the privileges of data manipulation over other users or cloud servers. This is because when sensitive information or computation is outsourced to the cloud servers or another user, and user identity must secured in this transformation. But, the data information will be send through access control.

D. User revocation based on re-authentication mechanism in Anonycontrol

In computing security privilege revocation is a measure taken by a privileges to protect the cloud user against itself. Privilege revocation is a variant of privilege separation whereby the user terminates the privileged part immediately after it has served its purpose. If a program doesn't revoke privileges, it risks the escalation of privileges. Re-authentication is used for the user privacy and secured user details among other clients. The verification process to the cloud, it relieves the individual users from time consuming verifications. When a reader wants to read

some data stored in the cloud, it tries to decrypt it using the secret keys it receives from the KDCs.

IV RESULT

In this main process is re-authentication mechanism using zero knowledge protocol. It is easy to find the existing user in cloud sever. If any user exist the cloud process and that existing user to access the cloud through the re-authentication process. Finally the user to access the cloud.

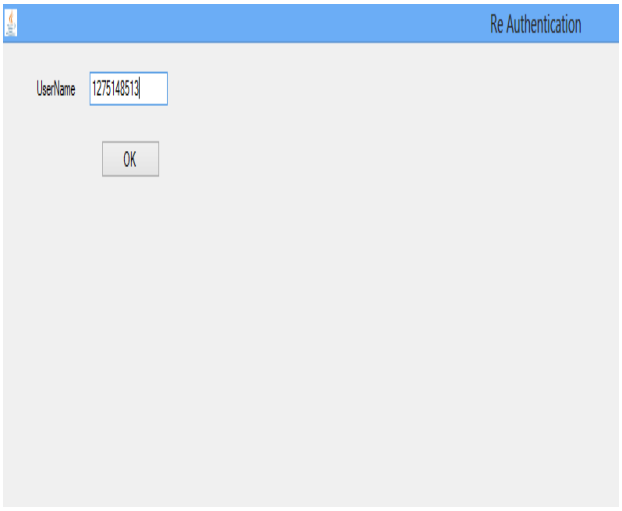

Fig 1 – Re-authentication process

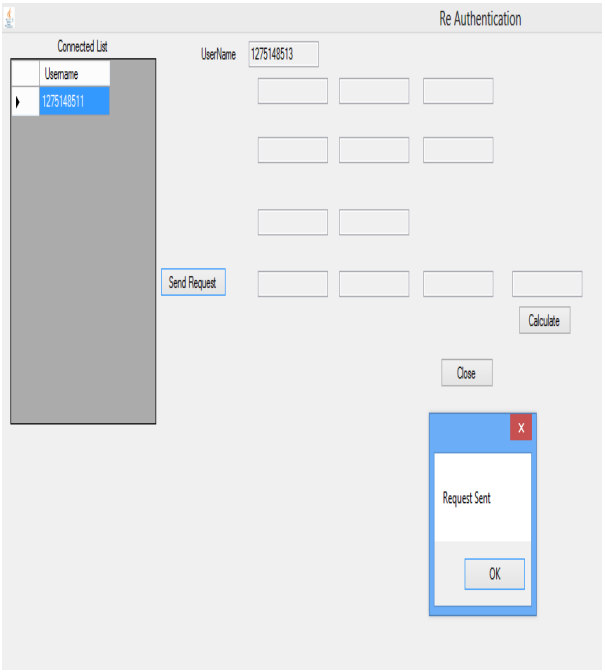

Fig 2 – Send the request to active user

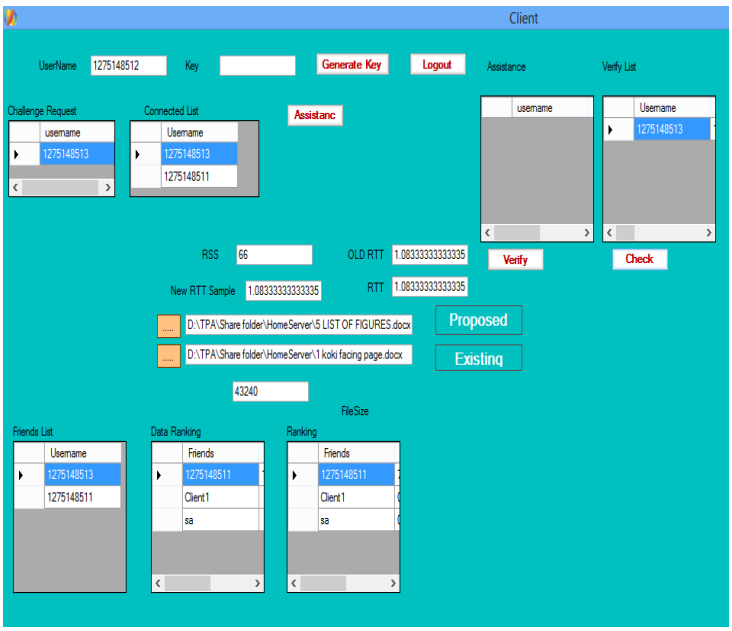

Fig 3 – Finally the user to access the cloud

IV CONCLUSION

This paper proposes a user revocation based on re-authentication approach used zero knowledge protocol. The cloud server easily to identify the existing user in the cloud processer using zero knowledge protocol. It used in the triple-DES algorithm. The encryption and decryption process to perform the three times in secure communication of client and cloud server. It is use a anonycontrol scheme, to address not only a data privacy also a user privacy and user identity. Secure ways to re-authenticate perform the cloud server.

REFERENCES

[1] M. Chase, "Multi-authority attribute based encryption," in Theory of Cryptography. Berlin, Germany: Springer-Verlag, 2007, pp. 515–534.

[2] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for finegrained access control of encrypted data," in Proc. 13th CCS, 2006, pp. 89–98.

[3] M. Chase and S. S. M. Chow, "Improving privacy and security in multi-authority attribute-based encryption," in Proc. 16th CCS, 2009, pp. 121–130.

[4] A. Shamir, "Identity-based cryptosystems and signature schemes," in Advances in Cryptology. Berlin, Germany: Springer-Verlag, 1985, pp. 47–53.

[5] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute- based encryption," in Proc. IEEE SP, May 2007, pp. 321–334.

[6] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Advances in Cryptology. Berlin, Germany: Springer-Verlag, 2005, pp. 457–473.

[7] H. Lin, Z. Cao, X. Liang, and J. Shao, "Secure threshold multi authority attribute based encryption without a central authority," Inf. Sci., vol. 180, no. 13, pp. 2618–2632, 2010.

[8] V. Božovic´, D. Socek, R. Steinwandt, and V. I. Villányi, "Multi-authority attribute-based encryption with honest-but-curious central authority," Int. J. Comput. Math., vol. 89, no. 3, pp. 268–283, 2012.

