ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 2, Issue 4, April 2016

Hybrid Privacy Preserving System for Anonymous Authentication

Kanimozhi.S.G[1], Keerthika.N[2]

PG Scholar, Department of CSE, Vandayar Engineering College, Thanjavur, India [1]

Assistant Professor, Department of CSE, Vandayar Engineering College, Thanjavur, India [2]

***Abstract*— Mediated certificate-less public key encryption (mCL-PKE) is used for providing double encryption scheme which solves the security problem and revocation problem. By using Cipher text policy attribute based encryption (CP-ABE) technique, they provide attribute based encryption and broadcast encryption. In CP-ABE approach they provide AND access policy while accessing data between different users. It can implement fine grained access control approach to provide privacy preserving based constant size cipher text approach. It avoid one to one communication instead of, it should provide one too many communication in effectively. By using hidden access policy the sender can hide the receivers who are all access the sender data. It implement access control mechanism is a policy that allows, denies or restricts access to a system. Privacy and security is the big challenge for stored data into the cloud. Most existing algorithms are very low level of security comparing with mCL-PKE scheme. This scheme gives protection to share sensitive data in public cloud without connecting operation. The scheme has been introduced as efficient certificate less cryptography technique.**

***Index Terms*— Mediated certificate-less public key encryption, Constant size cipher text, Broadcast encryption.**

I. INTRODUCTION

Network Security is prevention and monitor unauthorized access, misuse, modification or denial of a computer and network-available resources. Network security involves the identification of access to data in a network, and which is controlled by the network administrator.

Knowledge-base is characterized by secrecy and includes password. The term password includes single words, expressions and PINs (Personal Identification Numbers) that are firmly kept secrets used for authentication. But there is various liabilities of password-based authentication schemes. The drawback of passwords is that remember able password can often be guessed or searched by an attacker and a long, arbitrary, changing password is challenging to remember. Also, each time it is communal for authentication, so it becomes less secret.

Object-based are represented by physical retention or token. An identity token, security token, access token or simply token is a physical device which provides an authentication. This can be a secure storage device which containing passwords like smart card. A token can provide three advantages when combined with a password.

ID-Based are characterized by exclusive to one person. One advantage of a biometric is that it is less easily stolen than the other users, so it provides a stronger defense against repudiation.

A. CP-ABE CONSTRUCTION

In cipher text policy ABE was proposed with decryption policies in that work consists of the conjunction with number of gates and the threshold of each are determined at encryption time. To construct a CP-ABE scheme in which decryption policies are structured by threshold trees. Here, each node in the threshold tree represent to a threshold gate and each leaf in a threshold tree corresponds to an attribute. If a user's attributes appease the tree, then they can decrypt the cipher text. Another CP-ABE scheme was proposed which decryption policies are limited to a single AND gate. This scheme is easily lengthened to allow for decryption policies consisting of a non- conjunction of AND gates by simply encrypting the plaintext once for each AND. Then implement schemes are used to encrypt data in a way that only a privileged subgroup of users can decrypt the content.

B. mCL-PKE CONSTRUCTION

Storing data on un-trusted storage makes secure data sharing a challenge issue. Data access policies should be used on these storage servers, on the other hand, confidentiality of delicate data should be well guarded against them. A mediated certificate-less encryption (mCL-PKE) scheme which solves the revocation problem and the security problem and preserves the data confidentiality in the cloud. Since most of the mCL-PKE schemes are based on bilinear pairing. mCL-PKE is computationally expensive.

The security mediator supports revocation of compromised or enormous users and act as the policy enforcement scheme. The mCL-PKE scheme with the access control lists is been introduced to overcome the problem of sharing the confidential information in the cloud storage with hidden access policy and it proposes double encryption scheme on data sharing. The access control list maintains the details of the user and this list is produced to the cloud and the data owner for verification purpose. The cloud storage does not perform the decryption operation fully to protect the data confidentiality and also keys information. The extension of

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 2, Issue 4, April 2016

the mCL-PKE approach permit the data owner to maximize the encryption operation in an effective way and also to implement high level independent security in the cloud based system.

II. Related Works

A. Emura.k et al. [3]

The collusion resistant privacy preserving unique authority scheme which have the constant size cipher text also it require fixed number of pairing operation irrespective of attributes while decryption. It necessitates that the attributes in the cipher text must be a subset of user's attributes in his secret key. This approach is based on the AND-gates with multi-valued attributes. Our scheme does not provide recipient's anonymity. An attribute based encryption (ABE) is an effective encryption approach, where users with some attributes can decrypt the cipher text associated with these attribute. The first ABE scheme has been proposed in which is inspired by IBE. Although IBE scheme have a restriction such that an the encrypter can indicate only a single decrypter, in ABE schemes, an encrypter can indicate many decrypter by assigning common attributes of these decrypter.

B. Zhou.Z et al. [8]

In CP-ABE construction, named Constant-size Cipher text Policy Attribute Based Encryption (CCP-ABE), which incurs constant-size of cipher text, regardless of the number of attributes in a logical AND data access policy with wildcard. And the encrypted message and encoded access policy, each cipher text only requires 2 bilinear group elements, which are developed by 300 bytes in total. Due to the new development in CCP-ABE, it proves that the CCP-ABE is CPA protected. To the best of our knowledge, this is the first few such constructions that achieve these properties. Based on discovered CCP-ABE, further provide a new construction which is named as Attribute Based Broadcast Encryption (ABBE) that guides efficient Broadcast Encryption (BE).

Cipher-text Policy Attribute-Based Encryption has an attribute is a definitive string assigned to an entity and each entity may be connected with multiple attributes. Many entities may dividend common attributes, which allow message encrypters to represents a secure data access policy by comprises of multiple attributes by logical operators such as \AND", \OR", etc. To decrypt the message, the decrypter's attributes need to comprise the access policy. These features of CP-ABE solutions must make them engaging in many systems that require the expressive data access control for a large numbers of users.

Using ABBE, an encrypter has the flexibility to encrypt the broadcasted data using CCP-ABE, either with or without the information of each correspond receiver. For example, Alice can represent the access policy: \CS" AND \Student" to restrict the transmitted message to all CS students without indicating the receivers explicitly. ABBE also effectively reduces the storage overhead contrast to many existing BE schemes, whose cryptographic key materials required by encryption or decryption is can be linear depending on the number of receivers. ABBE addresses this key storage overhead problem by increasing the organization of attribute hierarchy to minimize the storage requirement for each user. As a result, ABBE requires minimize the level of stored key materials for each user, and thus it can be used to storage constrained systems.

C. Huang.D et al. [5]

A user's identity is exposed gradually based on receivers' authorized capabilities. At each step, the decrypter needs to satisfy certain attributes to expose next step attributes. Otherwise, decryption fails immediately and the decrypter learns nothing than the attributes he/she is entitled. This is fundamentally different to the concept of adopting hidden policy, "Try to decrypt the entire cipher text, if it is decrypted, the policy will be disclosed, if it cannot be decrypted, no policy will be disclosed". GIE is flexible and it does not need a pre-developed policy agreement. Each user can indicate a GIE scheduler, i.e., a step to expose an identity gradually, based on his/her security requirements without conferring with the message receivers.

D. Lou.W et al. [7]

A more efficient group key management and distribution scheme for dynamically formed multicast groups. It observed that in many cases, a dynamically formed multicast group is not simply an arbitrary combination of unrelated nodes. Alternatively, they are members with few common attributes. In this case, it may used a novel cryptographic primitive called cipher text policy attribute-based encryption (CP-ABE) such that it encrypt the group key under certain attributes and only those who own the destined attributes are able to decrypt it. To provide a high level of membership anonymity, enhance the current CP-ABE construction and design a new algorithm. Membership information are well secured. Multicast is a very important communication function that permits information to be distribute to a group of destinations concurrently and effectively. Multicast services have been widely expanded for applications. In various multicast-based applications will be increasingly deployed.

E. Herranz.J et al. [4]

Attribute-based cryptography has emerged as a promising primitive for digital security. For instance, it gives a solution to the problem of unauthorized user access control. In a cipher text policy attribute-based encryption approach, the secret keys of the users based on their attributes. When encrypting a message, the sender selects which subset of attributes should be managed by a receiver that is to be able to decrypt. All current attribute-based encryption schemes that prefer reasonably expressive decryption policies produce cipher texts whose size based on the number of attributes in the policy. Fist scheme whose cipher texts have constant size. Encryption is the primitives cryptographic which gives confidentiality to digital communications. In a contrast public key encryption approach, a message is encrypted with the public key of the designed receiver, who is the only person

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 2, Issue 4, April 2016

able to decrypt. It is mainly used to resolve security related problems.

III. PROPOSED SYSTEM

mCL-PKE scheme is purely based on double encryption scheme which provide higher security to cloud system. Storing data on un-authorized storage system leads confidential and secure sharing of data a challenge issue. Data access policies should be used on these storage servers, and confidentiality of delicate data should be well guarded against them. A mediated certificate-less encryption (mCL-PKE) scheme which solves the revocation problem and the security problem in the cloud. Since most of the mCL-PKE schemes are based on bilinear pairing. mCL-PKE is computationally expensive.

The security mediator supports revocation of compromised or enormous users and act as the policy enforcement scheme. This scheme with the access control lists is been introduced to overcome the problem of sharing the confidential information in the cloud storage with hidden access policy and it proposes double encryption scheme on data sharing. The access control list maintains the details of the user and this list is produced to the cloud and the data owner for verification purpose. The cloud storage does not perform the decryption operation fully to protect the data confidentiality and also keys information. The extension of the mCL-PKE approach permit the data owner to maximize the encryption operation in an effective way and also to implement security with high-level in the cloud based system.

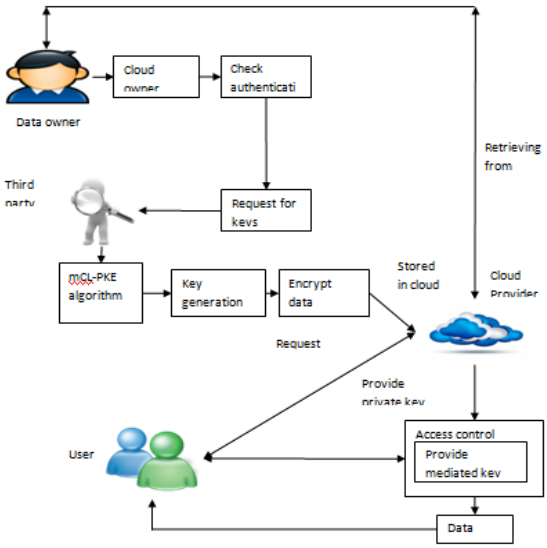

Fig 1 System Architecture

To solve the privacy issue on shared data, we propose an efficient Certificate less Encryption for Secure Data Sharing in Public Clouds proposed Mediated certificate less public key encryption. This algorithm presents a feasible reinstament for public key cryptosystem that requires Certificate Authority to issue digital certificate to append user to their public keys .Certificate authority produces its own signature on each user public keys and manage and manage user certificate, thus complete key management in this system is way too expensive and complex. The newly proposed system uses Attribute Based Encryption. In ABE Access control policy is employed to encrypt each data to solve the security problem Certificate less public key cryptography is introduced which then further improved in Certificate less proxy re-encryption which is based on CL-PKC.

Establish a new privacy challenge in cloud storage, and address a privacy issue during a user confrontation the cloud server for sharing of data, in which the challenged request itself doesn't reveal the user's privacy to obtain whether or not to access the authority. Introduces an authentication protocol to provide a user's access request relates privacy, and the shared access authority is achieved by unauthorized access request matching mechanism.

Apply attribute based access control to understand that a user can reliably access its own data fields, and endorse the proxy re-encryption to give temp authorized data sharing among multiple users. Implement mCKLE – mediated certificate less encryption algorithm which is an emerging favorite because it needs less computational power, communication bandwidth, and memory when contrast to other cryptosystems.

IV. EXPERIMENTAL ANALYSIS

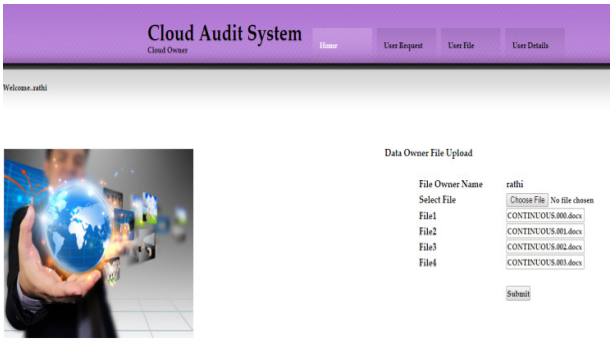

Fig 2 Upload File

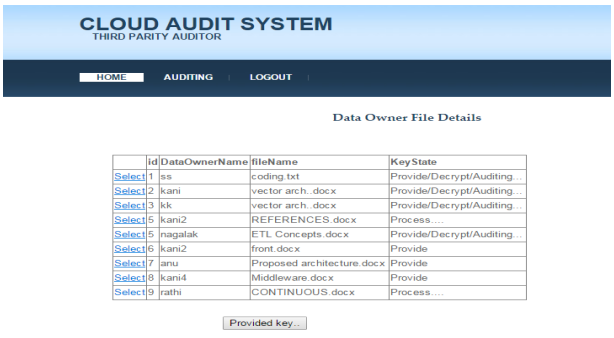

Fig 3 Third party auditor providing key

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 2, Issue 4, April 2016

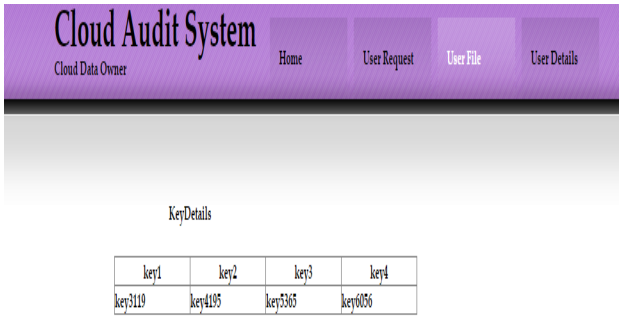

Fig 3 Key Issued

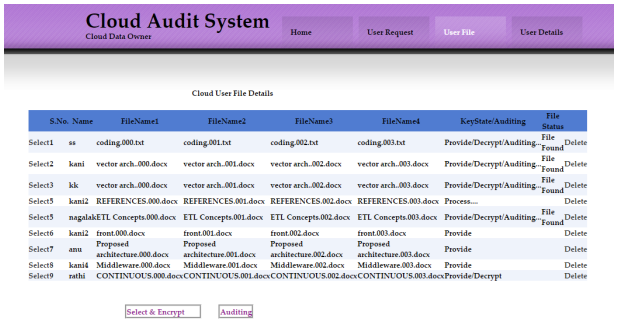

Fig 4 Data Encryption

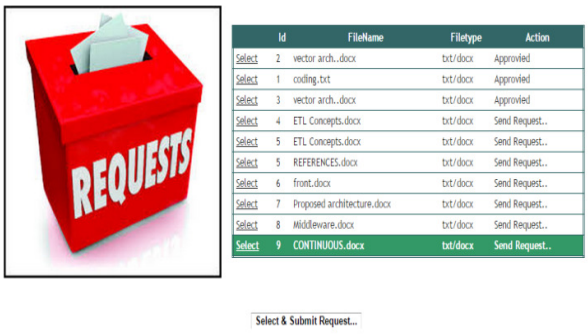

Fig 5 User Request for File

Fig 6 File Provided to User

V. CONCLUSIONS

To facilitate secure data transfer between the sender and receiver implemented mediated certificate less public key encryption (mCL-PKE) approach with double encryption scheme. Based on the user priority they can provide either partial or complete data to user. Also by using hidden access policy, it can hide the accessing user from the other user. It provides efficient access privileges to access files that are in cloud system. In future, it can extend the work to implement in remote cloud storage system with monitoring system to verify the integrity of the system to using heuristic auditing strategy for avoid attackers in decentralized environments.

REFERENCES

[1] Bertino.E, Nabeel.M ,Shang.N, and Paci.F, " A privacy preserving approach to policy based content dissemination apprach", IEEE 26th ICDE, pp.944 -955, 2010.

[2] Cao.D, Hu.Q.L ,Su.S.J, Su.Y.P, and Wang.X.F, "Attribute-based encryption approach", Journal of Software, vol. 6, pp. 1299–1315, 2012.

[3] Emura.K, Miyaji.A, Nomura.A, Omote.K, and Soshi.M, "A ciphertext policy attribute based encryption scheme with constant ciphertext length," in Proc. 5th Int. Conf. Inf. Security Practice Experience. Springer-Verlag,, pp. 13-23, 2009.

[4] Herranz.J, Laguillaumie.F, and Ràfols.C, "Constant size ciphertexts in threshold attribute-based encryption," in Proc. Public Key Cryptography (PKC), pp. 19-34, 2010.

[5] Huang.D, Zhou.Z and Yan.Z, "Gradual identity exposure using attribute-based encryption", in Proc. IEEE 2nd Int. Conf. Social Comput. (SocialCom), pp. 881-888, 2010.

[6] Ji.D and Tang.Q, "Verifiable attribute based encryption"," International Journal of Network Security", vol. 10, no. 2, pp. 114–120, 2010.

[7] Lou.W, Ren.K, and Yu.S, "Attribute-based content distribution with hidden policy," in Proc. 4th Workshop Secure Netw. Protocols, pp. 39-44, 2008.

[8] Zhou.Z, "On efficient ciphertext-policy attribute based encryption and broadcast encryption," in Proc. 17th ACM Conf. Comput. Commun. Security, pp. 753-755, 2010.