ISSN 2348 – 9928
IJAICT Volume 5, Issue 3, March 2018 Doi:01.0401/ijaict.2015.11.03 Published on 05 (3) 2018

AN INVESTIGATION ON CERTIFICATE LESS ENCRYPTION FOR SECURE DATA SHARING IN PUBLIC CLOUDS

Mr. A. Gnana Sundhar
UG Student,

Mr. C. Arun
UG Student,

Mr. Palanivel
UG Student,

Ms. Mishmala sushith
Associate professor

Information Technology,
Kalaignar Karunanidhi Institute of Technology,
Coimbatore, Tamilnadu, India

Abstract— It is a mediated certificate less encryption method not using pairing of keys and is used for securely distributing sensorial data in public clouds. The algorithm used in this paper is Mediated certificate less public key encryption (MCL-PKE) .It is used to solve the key escrow problem and the immediate revocation problem. The existing approach is to make use of a pairing of keys between the users and the cloud owner but this approach is inefficient. So for removing these security problems the new method called (MCL-PKE) is constructed to solve the securely distributing data in the public clouds. In our method the cloud is s as a two way system 1) secure storage 2) key generation center. Here the cloud owner will encrypt the important data of registered users and sends the encrypted data to cloud database with their public keys. The cloud will partially decrypts the data at the time of users download but it fully decrypts at the time of applying the private keys of each registered user. So it is a well secured overall cloud database to improve the performance and the security issues.

Keywords— Cloud Computing, Accountability, Centralized Data, Authorization, Obliviou.

I. INTRODUCTION

Cloud is currently expanding computing technology. The cloud allows a centralized data storage and online access to computer services. Clouds can be classified as public, private or hybrid. Many organizations have been adopted public cloud services namely MICROSOFT SKY DRIVE, DROPBOX because of the applications of public cloud storage. The public cloud storage want to solve the critical issue of data confidentiality so the common method is to encrypt the data before uploading it to the cloud it provides more security to the data. Next the fine grained encryption access control of the data is processed with the symmetric key based mechanisms but it had a major problem is high cost for the key management.

In order to remove the key management problem the public key cryptosystem is used. In this system the CERTIFICATE AUTHORITY (CA) is issue the digital certificate to the user's public keys. But this certificate management is very costly and complex. So the new system as Identity Based Public Key cryptosystem (IB-pkc) was introduced but it had a key escrow problem. It means the key generation server knows the private keys of a user it is a big threat. Next the Attribute Based Encryption (ABE) has been used to allow encrypting the data but the revocation problem is aroused. Al-Riyami and Paterson developed a new cryptosystem called Certificateless Public Key Cryptography (CL-PKC).

Then the CL-PRE (Certificate less Proxy Re-Encryption) mechanism for secure data sharing in public cloud environments but this mechanism is based on CL-PKC to solve the key escrow problem and certificate management although uses pairing operations. In this paper, we analysis the previous approaches and propose a mediated Certificateless Public Key Encryption (mCL-PKE) algorithm but it no use pairing operations. Hence it is based on bilinear pairings so very costly to work. The new idea in this system is that when the user gives the data to be uploaded in the cloud by the cloud owner a public key must be used to encrypt.

After that the data in cloud database can be downloading and decrypt with the help of the users private keys. An another change in this system is that the along with the private key an Intermediate key is used to decrypt the data from the cloud but it will be send to the user's by the cloud owner. There is a secure transmission line is established between the user and the cloud owner with in that line the intermediate key will be send to the user for the secure data sharing.

II. CLOUD PRIVACY AND SECURITY

Cloud computing has raised a range of important privacy and security issues. Such issues are due to the fact that, in the cloud, users' data and applications reside at least for a certain amount of time on the cloud cluster which is owned and maintained by a third party. Concerns arise since in the cloud it is not always clear to individuals why their personal information is requested or how it will be used or passed on to other parties. To date, little work has been done in this space, in particular with respect to accountability [13] .Pearsonetal

which has proposed accountability mechanisms to address privacy concerns of end users and then develop a privacy manager. Their basic idea is that the user's private data are sent to the cloud in an encrypted form, and the processing is done on the encrypted data. The output of the processing is deobfuscated by the privacy manager to reveal the correct result. However, the privacy manager provides only limited features in that it does not guarantee protection once the data are being disclosed. In the authors present a layered architecture for addressing the end-to-end trust management and accountability problem in federated systems. The authors' focus is very different from ours, in that they mainly leverage trust relationships for accountability, along with authentication and anomaly detection. Further, their solution requires third-party services to complete the monitoring and focuses on lower level monitoring of system resources.

III. SEARCHABLE ENCRYPTION REVISITED CONSISTENCY PROPERTIES, RELATIONS TO ANONYMOUSIBLE, AND EXTENSIONS

In this paper the mechanism of identifying and filling the unused spaces with regard to consistency (the duration to faulty pictures are generated) for public-key encryption with keyword search (PEKS)[1]. It determine the estimated and numerical relaxations of the current approach of perfect consistency. Then the system provides a revolution an unidentified ordered identity-based encryption (IBE) scheme to the protection of PEKS scheme. Here the three extensions of the basic approach considered here such as 1) unidentified hierarchical identity-based encryption, 2) public-key encryption with temporary keyword search, and 3)identity-based encryption with keyword search.

3.1 Fine-Grained Control of Security Capabilities

In this paper a fine grained control over the guaranteed users and focus on the online semi-trusted mediator (SEM). The SEM can need the another method called threshold variant of RSA cryptosystem (mediated RSA) [2]. The main advantages

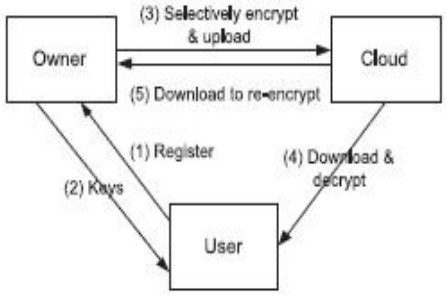

Fig 1: SymmetricBasedFine-Grained Encryption

in this system are reduced verification of digital signatures, valuable certificate revocation of old systems. This paper explains both the architecture and the implementations of our method with a high performance and experimental outputs.

3.2 Conjuctive, Subset, and Range Queries on Encrypted Data

The encryption techniques has a different types of queries applied on the encrypted data. The creation of the public key system on accordance of comparison queries ($X \geq a$) on cipher text and more general queries are subset queries (x€s). It also supports arbitrary conjunctive queries ($P_1 \square \wedge \square \cdots \square \wedge \square P_\ell$) without leaking the data on personal conjuncts[3]. The proposed idea is a general infrastructure for creating and evaluating public key systems support queries on cipher text.

3.3 Oblivious Transfer with Access Control

This paper gives an protocol for unidentified usage of database of having different security authorizations mechanism. The main security purposes are attributes, rules and rights that user want to use the data [4]. This protocol has some conditions and assures maximal security for database and users such as 1) registered users can access the data. 2) The database owner will not know about which data the user access. 3) The data owner will not know the rules of users accessing data. This protocol works with the bilinear Diffie-Hellman and strong Diffie-Hellman theory.

3.4 Security- Mediated Certificate less Cryptography

In this paper the approach called security mediated certificate less (SMC) cryptography. It allows many insignificant versions of mediated cryptography on the same time of accessing repudiation of keys. This solution will avoid the key escrow problem [5]. It provides the security against the cipher text hacker. The proposed idea in this paper is a generic creation and detailed algorithm based on bilinear pairings. This technique is more efficient than identity based mediated encryption scheme of Baek and Zheng in pkc 2004.

3.5 Controlling Access to an Oblivious Database Using Stateful Anonymous Credentials

In this paper the new method of allowing service provider to implement complicated access authority on unfamiliar protocols with unidentified users. In old approach data owner restrict to what data the users can access without knowing the users details[6]. So in the proposed the users database access history is implemented. Our architecture supports many access control policies such as efficient and private realizations of Brewer-Nash (Chinese wall) and Bell-LaPadula (multilevel security) these are used for Economic and military applications.

ISSN 2348 – 9928
Doi:01.0401/ijaict.2015.11.03 Published on 05 (3) 2018

IV. ATTRIBUTE-BASED ENCRYPTION FOR FINE-GRAINED ACCESS CONTROL OF ENCRYPTED DATA

As more cognizant data is shared and stored by an mediator sites on the Internet, there will be a need to encode data stored at these sites. One drawback of encoding data, is that it can be judiciously shared only at a coarse-grained level. We develop a new encoding scheme for fine-grained distribution of encrypted data that we call Key-Policy Attribute-Based Encryption (KPABE)[7].In this phase, the encoded versions are labeled with sets of traits and private keys are integrated with access enablers that control which encoded versions a user is able to decrypt. We demonstrate the associability of our creation to allocating of analyzing-log details and telecast encryption. Our creation enables replacement of private keys which involve Hierarchical Identity-Based Encryption (HIBE).

4.1 Information Security and Cryptology

The bilinearity of combining allows conductive impression attestation for indication schemes based on discrete logarithm type problem and often provides valuable additional activities to impression schemes. In recent years, bilinear combining have been widely used to create impression schemes [8]. But the bilinearity can also be an invading point in uncarefully designed courtesy. We show that the imprudent use of a bilinear pairing spark to uncapturable group signatures.

4.2 Predicate Encryption Supporting Disjunctions, Polynomial Equations, and Inner Products

Predicate encryption is a new approach for public-key encoding that discovers identity-based encryption. In predicate encryption, secret keys indicate to predicates and encoded versions are blended with peculiarity. Here we assume a scheme for predicates indicates to the some large integer N[9]. This, in turn, enables besides plating as a eloquent step leading in the theory of predicate encryption.

4.3 CL-PKE : A Certificate less Proxy Re-Encryption Scheme For Secure Data Sharing In Public Cloud

We assume a certificate less proxy re-encryption technique for unharmed data splitting with civic cloud. In CLPRE, a data originator encodes shared file in nebula with an encryption key, which is again encoded and converted by cloud, and then supplied to canonical beneficiary in accordance with course limit [10]. The cloud-based conversion greases re-encryption keys derived from individual key of data originator and public keys of receipts, and excludes the key bond problem in coherence based cryptography and the need of documentation. While conserving data and key secreacy from semi-reliable cloud.CL-PRE leverages maximal cloud resources to exclude the communication cost of data originator.

4.4 Paring Based Cryptogarphy

Episoidal cryptography is widely used in cryptography decorum. The main asset is paralyzing no of protocols. Combining based protocols are used has its application in ID-based schemes [11]. We create versions of Diffie Hellman, to deal with security issues in cryptography.

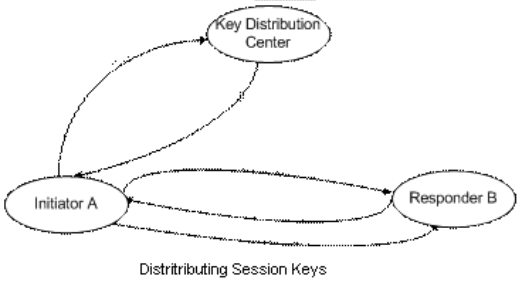

Fig 2 : Key Generation Using Diffie-Hellman

4.5 Controlling Access to Published Data Using Cryptography

An essential case in public clouds is how to efficiently share data's based on fine-grained aspect based policies. Here we encode documents to fascinate various policies with numerous keys using a public key cryptosystem such as attribute based encryption (ABE).This has some drawbacks as it cannot adequately handle adding/quash users changes. A direct implication of a symmetric key cryptosystem is to satisfy and assign unique keys .Based on this case, we assign a new key management scheme called broadcast group key management (BGKM)[12]. The idea is to give some privacy to users based on the identity aspects . A key advantage of the BGKM scheme is that adding new member/removing users or modifying access control policies can be performed by modifying only some public datas.

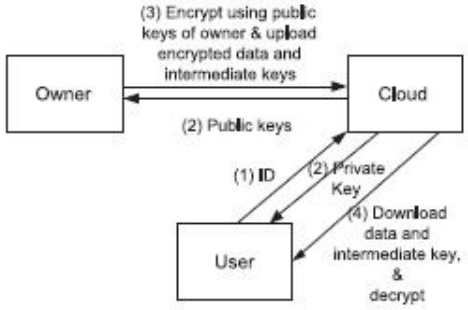

Fig 3 : CL-PKE Intermediate Key Based Fine-Grained Encryption

V. CONCLUSION

In this paper we have proposed the first mCL-PKE scheme without pairing operations and provided its formal security. Our mCL-PKE solves the key escrow problem and revocation problem. Using the mCL-PKE scheme as a key building block, we proposed an improved approach to securely share sensitive data in public clouds. Our approach supports immediate revocation and assures the confidentiality of the data stored in an entrusted public cloud while enforcing the access control policies of the data owner. Our experimental results show the efficiency of basic mCL-PKE scheme and improved approach for the public cloud. Further, for multiple users satisfying the same access control policies, our improved approach performs only a single encryption of each data item and reduces the overall overhead at the data owner.

References

[1] M. Abdalla *et al.*, "Searchable encryption revisited: Consistency properties, relation to anonymousibe, and extensions," *J. Cryptol.*,vol. 21, no. 3, pp. 350–391, Mar. 2008.

[2] D. Boneh, X. Ding, and G. Tsudik, "Fine-grained control of security capabilities," *ACM Trans. Internet Technol.*, vol. 4, no. 1,pp. 60–82, Feb. 2004.

[3] D. Boneh and B. Waters, "Conjunctive, subset, and range queries on encrypted data," in *Proc. 4th TCC*,Amsterdam, The Netherlands, 2007, pp. 535–554.

[4] J. Camenisch, M. Dubovitskaya, and G. Neven, "Oblivious transfer with access control," in *Proc. 16th ACM Conf. CCS*, New York,NY, USA, 2009, pp. 131–140.

[5] S. S. M. Chow, C. Boyd, and J. M. G. Nieto, "Security mediated certificateless cryptography," in *Proc. 9th Int.Conf. Theory Practice PKC*, New York, NY,USA, 2006,pp. 508–524

[6] S. Coull, M. Green, and S. Hohenberger, "Controlling access to an oblivious database using stateful anonymous credentials," in *Irvine: Proc. 12th Int. Conf. Practice and Theory in PKC*, Chicago, IL, USA, 2009, pp. 501–520.

[7] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data,"in *Proc. 13th ACM Conf. CCS*, New York, NY, USA, 2006,pp. 89–98.

[8] C. Gu, Y. Zhu, and H. Pan, "Information security and cryptology," in *4th Int. Conf. Inscrypt*, Beijing, China, 2008, pp. 372–383.

[9] J. Katz, A. Sahai, and B. Waters, "Predicate encryption supporting disjunctions, polynomial equations, and innerproducts," in *Proc. EUROCRYPT*, Berlin, Germany, 2008.pp. 146–162.

[10] X. W. Lei Xu and X. Zhang, "CL-PKE: A certificateless proxy re encryption scheme for secure data sharing with public cloud," in *ACM Symp. Inform. Comput. Commun. Security*, 2012.

[11] B. Lynn. *Pairing-based cryptography* [Online]. Available:http://crypto.stanford.edu/pbc

[12] G. Miklau and D. Suciu, "Controlling access to published data using cryptography," in *Proc. 29th Int. Conf. VLDB*, Berlin, Germany, 2003, pp. 898–909.

[13] B. Chun and A.C. Bavier, "Decentralized Trust Management and Accountability in Federated Systems," Proc. Ann. Hawaii Int'l Conf. System Sciences (HICSS), 2004.

[14] **B**.Banu priya, V.Sobhana and Prof.Mishmala Sushith,"Concise Survey on Privacy Preserving Techniques in Cloud",in IARJSET Research Journal,2015