Volume 1, Issue 5 December 2015 ISSN NO: 2454 - 7514

North Asian International Research Journal Consortium

North Asian International Research Journal

Of

Science, Engineering and Information Technology

Welcome to NAIRJC

ISSN NO: 2454 -7514

North Asian International Research Journal of Science, Engineering & Information Technology is a research journal, published monthly in English, Hindi, Urdu all research papers submitted to the journal will be double-blind peer reviewed referred by members of the editorial board. Readers will include investigator in Universities, Research Institutes Government and Industry with research interest in the general subjects

Editorial Board

Address: - Dr. Ashak Hussain Malik House No. 221 Gangoo, Pulwama, Jammu and Kashmir, India - 192301, Cell: 09086405302, 09906662570, Ph. No: 01933-212815,
Email: nairjc5@gmail.com, nairjc@nairjc.com, info@nairjc.com Website: www.nairjc.com

NEW APPROACH FOR SECURE DATA SHARING IN PUBLIC CLOUDS WITH AN EFFICIENT CERTIFICATELES ENCRYPTION

PALLAVI GAWADE [1], PRANITA GENGAJE [2], NAMRATA UBALE [3], VARSHA HALWAR [4]
[1234]Department of Computer Engineering, Pune University, Pune, India

ABSTRACT:

We propose a mediated certificate less encryption scheme without pairing operations for securely sharing sensitive information in public clouds. Mediated certificate less public key encryption (mCL-PKE) solves the key escrow problem in identity based encryption and certificate revocation problem in public key cryptography. However, existing mCL-PKE schemes are either inefficient because of the use of expensive pairing operations or vulnerable against partial decryption attacks. In order to address the performance and security issues, in this paper, we first propose a mCL-PKE scheme without using pairing operations. We apply our mCL-PKE scheme to construct a practical solution to the problem of sharing sensitive information in public clouds. The cloud is employed as a secure storage as well as a key generation center. In our system, the data owner encrypts the sensitive data using the cloud generated users' public keys based on its access control policies and uploads the encrypted data to the cloud. Upon successful authorization, the cloud partially decrypts the encrypted data for the users. The users subsequently fully decrypt the partially decrypted data using their private keys. The confidentiality of the content and the keys is preserved with respect to the cloud, because the cloud cannot fully decrypt the information. We also propose an extension to the above approach to improve the efficiency of encryption at the data owner. We implement our mCL-PKE scheme and the overall cloud based system, and evaluates its security and performance. Our results show that our schemes are efficient and practical.

Keywords: ***Access Control, Cloud Computing, Public cloud, Certicateless Cryptography, Confidentiality, Encryption, Decryption.***

1. INTRODUCTION:

In a conventional CL-PKE scheme, user s complete private key consists of a secret value chosen by the user and a partial private key generated by the KGC. Unlike the CL- PKE scheme, the partial private key is securely given to the SEM, and the user keeps only the secret value as its own private key in the mCL-PKE scheme. So, each user s access request goes through the SEM which checks whether the user is revoked before it partially decrypts the encrypted data using the partial private key. It does not suffer from the key escrow problem, because the user s own private key is not revealed to any party. It should be noted that neither the KGC nor the SEM can decrypt the encrypted data for specific users. Moreover, since each access request is mediated through the SEM, our approach supports immediate revocation of compromised users. It is important to notice that if one directly applies our basic mCL-PKE scheme to cloud computing and if many users are authorized to access the same data, the encryption costs at the data owner can become quite high. In such case, the data owner has to encrypt the same data encryption key multiple times, once for each user, using the user public keys. To address this shortcoming,

we introduce an extension of the basic mCL-PKE scheme. Our extended mCL-PKE scheme requires the data owner to encrypt the data encryption key only once and to provide some additional information to the cloud so that authorized users can decrypt the content using their private keys. Fig. 3 gives a high-level view of the extension. The idea is similar to Proxy Re-Encryption (PRE) by which the data encryption key is encrypted using the data owner s public key and later can be decrypted by different private keys after some transformation by the cloud which acts as the proxy. However, in our extension, the cloud simply acts as storage and does not perform any transformation. Instead, the user is able to decrypt using its own private key and an intermediate key issued by the data owner.

2. SURVEY:

2.1CERTIFICATELESS PUBLIC KEY CRYPTOGRAPHY

This paper presents marks concrete the idea of certificateless open key cryptography (CL-PKC), a model for the utilization of open key cryptography which maintain sastrategic distance from the inalienable escrow of personality based cryptography but which not oblige testaments to ensure the validness of open keys. The absence of testaments and the vicinity of an enemy who has admittance to an expert key require the watchful improvement of another security model. We concentrate on certificateless open key encryption (CL-PKE), demonstrating that a solid matching based CL-PKE plan is secure given that a hidden issue firmly identified with the Bilinear Diffie-Hellman Problem is hard.

2.2 CIPHERTEXT-POLICYATTRIBUTE-BASEDENCRYPTION

In a few conveyed frameworks a client ought to just have the capacity to get to information if a client gangs a sure arrangement of certifications or properties. Right now, the main strategy for authorizing such strategies is to utilize a trusted server to store the information and intervene access control. On the other hand, if any server putting away the information is bargained, then the information's confidentiality will be traded off. In this paper we introduce a framework for acknowledging complex access control on encoded information that we call Cipher text-Policy Attribute-Based Encryption. By utilizing our procedures coded information can be kept confidential regardless of the possibility that the stockpiling server is untrusted; also, our techniques are secure against intrigue assaults. Past Attribute Based Encryption frameworks utilized credits to portray the scrambled information and incorporate arrangements with client's keys; while in our framework ascribes are utilized to depict a client's certifications, and a gathering encoding information decides an arrangement for who can decode. In this manner, our strategies are thoughtfully closer to customary access control strategies, for example, Role-Based Access Control (RBAC). Furthermore, we give a usage of our framework and give execution estimation.

2.3 CONJUNCTIVE, SUBSET, AND RANGE QUERIESON ENCRYPTED DATA

We build open key frameworks that bolster examination inquiries(x an) on encoded information and additionally more broad questions, for example, subset questions(x S). These frameworks support self-assertive conjunctive questions without spilling data on individual conjuncts. We exhibit a general structure for developing and

examining open key frameworks supporting in queries on scrambled information.

3. EXISTING SYSTEM

In existing system, symmetric keys are use for data encryption as well as data decryption. Existing mCL-PKE schemes are either inefficient. Because of the use of expensive pairing operations or vulnerable against partial decryption attacks. While sending data if certificate suffers any changes then whole data will be lost. Certificate management is very expensive.

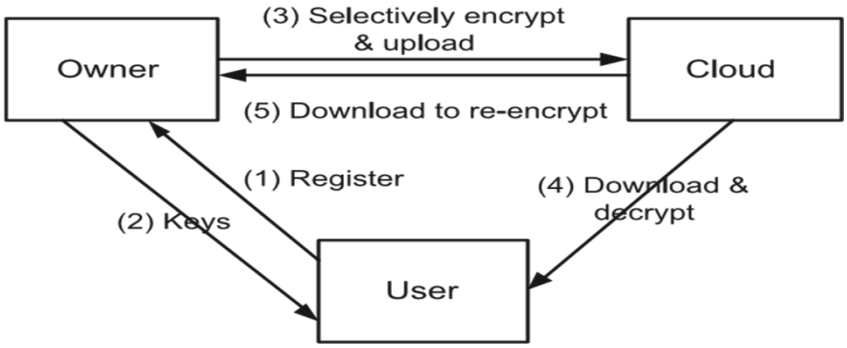

Fig. 1. Symmetric key based fine-grained encryption

4. PROPOSED SYSTEM

Approach is to supports immediate revocation and assures the confidentiality of the data stored. In an untrusted public cloud while enforcing the access control policies of the data owner. The efficiency of basic mCL-PKE scheme and improved approach for the public cloud. Performs only a single encryption of each data item and reduces the overall overhead at the data owner.

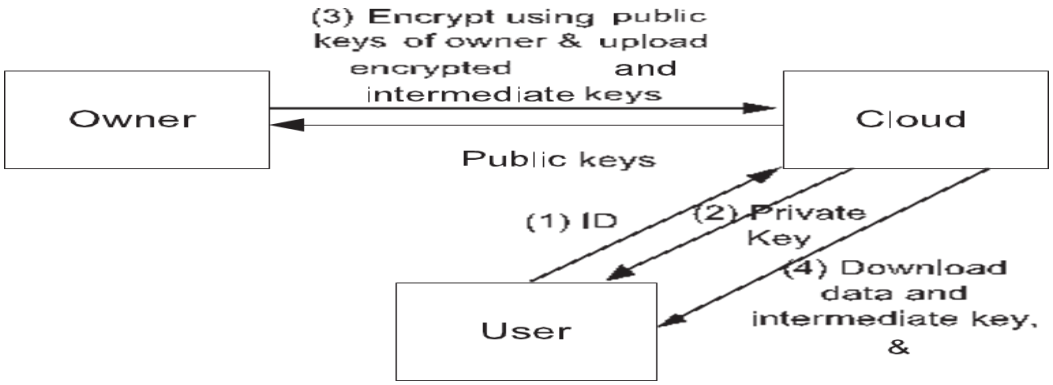

Fig. 2. CL-PKE with intermediate keys based fine-grained encryption

4.1 Implementation

Execution is the phase of the task when the hypothetical outline is transformed out into a working framework. Along these lines it can be thought to be the most basic stage in accomplishing a fruitful new framework and in giving the client, certainty that the new framework will work and be powerful. The execution stage includes watchful arranging, examination of the current framework and it's requirements on usage, planning of routines to accomplish changeover and assessment of changeover techniques.

4.2 Modules

The system is proposed to have the following modules along with functional requirements.

4.2.1 Identity token issuance

IdPs which are trusted by third parties that issue identity tokens to users based on their identity attributes. It should be noted that IdPs need not to be online after they issue identity tokens.

4.2.2Identity token registration

Users should register their token to obtain secrets in order to later decrypt the data they are allowed to access. Users should registration of their tokens are related to the attribute conditions in ACC with the Owner, and the rest of the identity tokens related to the attribute conditions in ACB/ACC with the Cloud. When Users register with the Owner, the Owner issues the two sets of secrets for the attribute conditions in ACC that are also present in the sub ACPs in ACPB Cloud. The Owner must keep one set and gives the other set to the Cloud. Two different sets are used in order to prevent the Cloud from decrypting the Owner encrypted data.

4.2.3Data encryption and uploading

The Owner first encrypts the data based on the Owner's sub ACPs should be in order to hide the content from the Cloud and then uploads them along with the public information generated by the AB-GKM :: Key Gen algorithm and the remaining sub ACPs to the Cloud. The Cloud in turn encrypts the data which based on the keys generated using its own AB-GKM :: Key Gen algorithm. Note that the AB-GKM :: Key Gen at the Cloud takes the secrets issued to Users and the sub ACPs given by the Owner into consideration to generate keys.

4.2.4 Data For downloading and Data Decryption

Users download encrypted data from the Cloud and decrypt twice to access the data .Firstly the Cloud generated public information tuple is used to derive the OLE key and then the Owner generated public information tuple is used to derive the ILE key which are using the AB-GKM::KeyDer algorithm. That the two keys allow a User to decrypt a data item which only for the User satisfy the original ACP applied to the data item.

4.2.5 Encryption Evolution Management

Over time, either ACPs or user credentials may change. Further, already encrypted data go through frequent updates. In such a situations, data must be already encrypted and re-encrypted with a new key. As the Cloud

performs the access control enforcing for encryption, it re-encrypts the affected data without the intervention of the Owner.

5. FLOW DIAGRAM

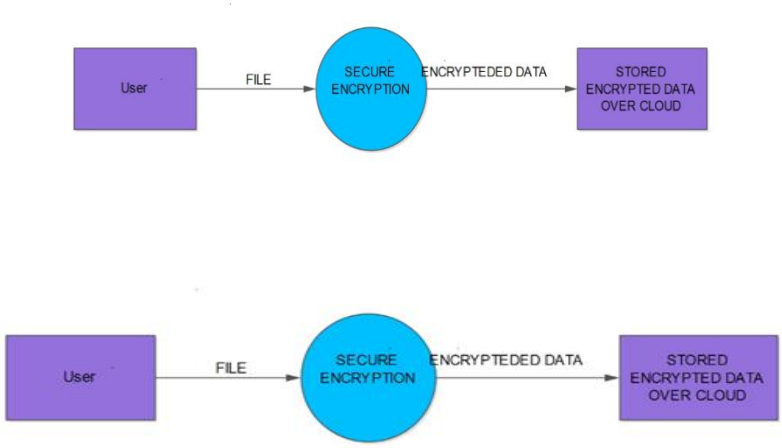

Fig.3 Data Flow Diagram Level 0

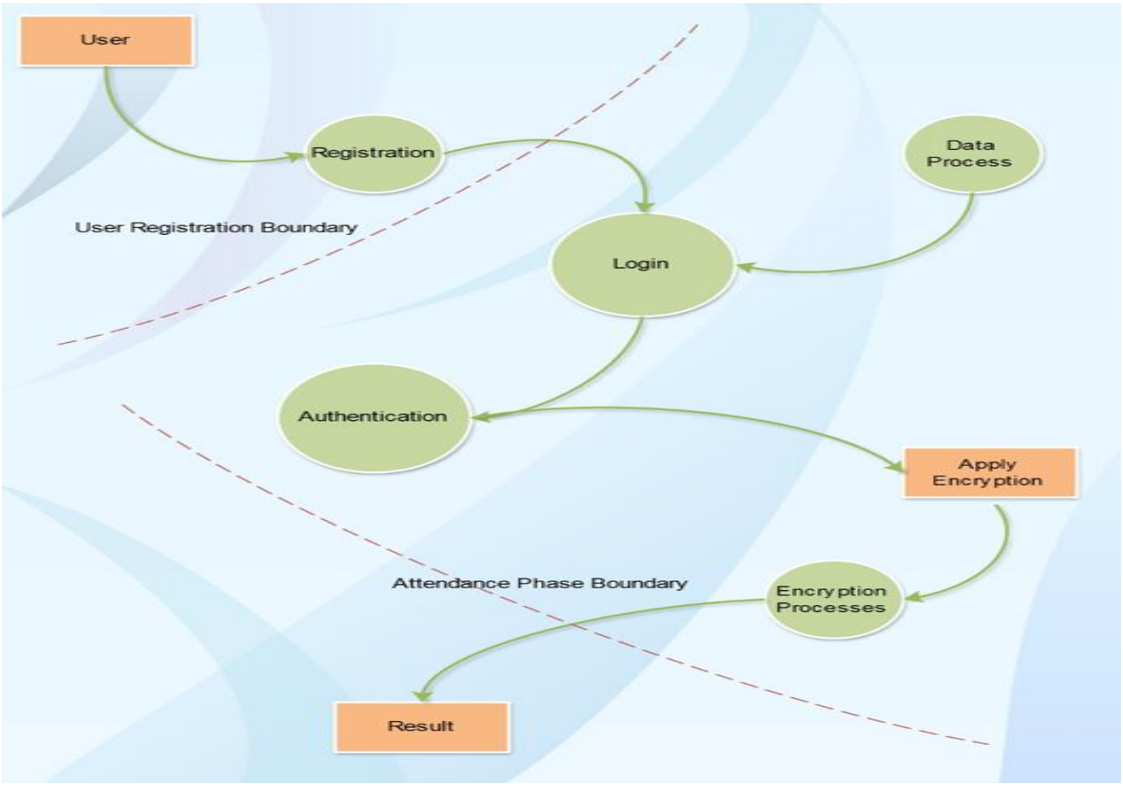

Fig.3 Data Flow Diagram Level 1

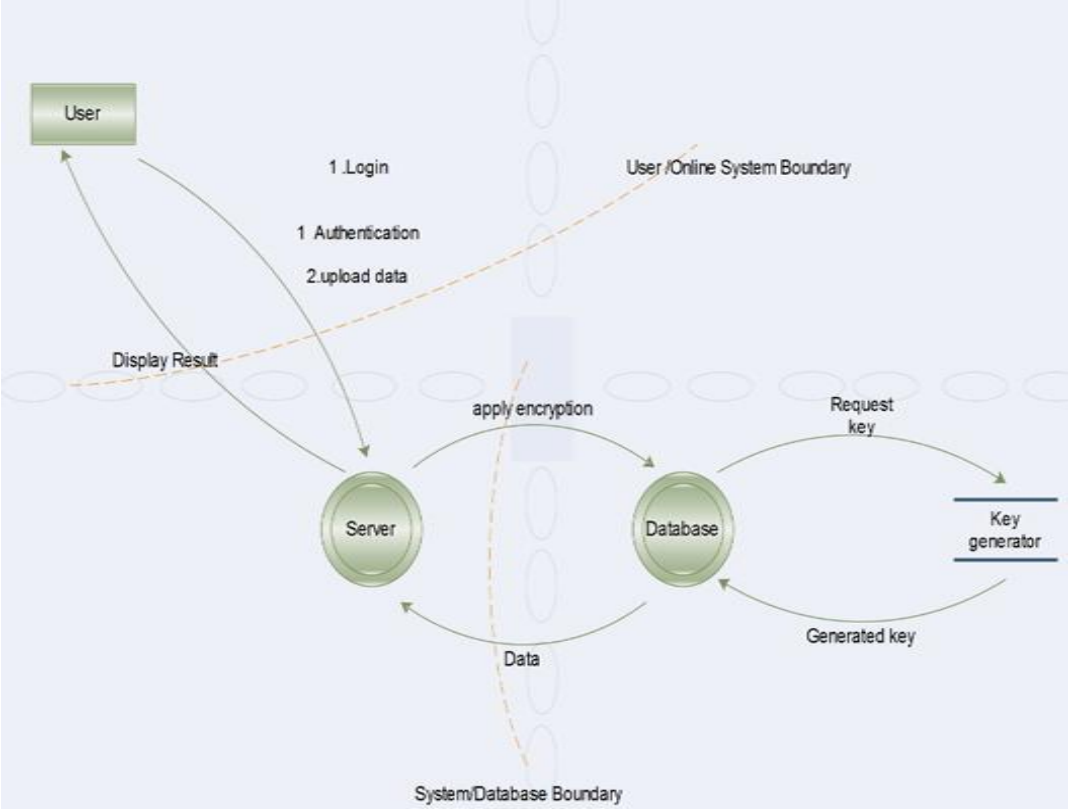

Fig.3 Data Flow Diagram Level 2

6. CONCLUSION AND FUTURE WORK:

In this paper we have proposed the rst 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 untrusted public cloud while enforcing the access controlpolicies 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.

ACKNOWLEDGEMENTS:

WE ARE THANKFUL TO OUR PROJECT GUIDE PROF. JAMEER KOTWAL FOR THEIR SUPPORT. ALSO ALL THE STAFF OF COMPUTER DEPARTMENT FOR COORDINATION.

REFERENCES:

[1] S. Al-Riyami and K. Paterson, Certificateless public key cryptography, in Proc. ASIACRYPT 2003, C.-S. Laih, Ed. Berlin, Germany: Springer, LNCS 2894, pp. 452473.Ding, W. and Marchionini, G. 1997 A Study on Video Browsing Strategies. Technical Report. University of Maryland at College Park.

[2] M. Bellare, A. Desai, D. Pointcheval, and P. Rogaway, Relations among notions of security for public-key encryption schemes, in Proc.Crypto 98, H.Krawczyk Ed. Springer-Verlag, LNCS 1462. Tavel, P. 2007 Modeling and Simulation Design. AK Peters Ltd.

[3] E.Bertino and E. Ferrari. Secure and selective dissemination of XML documents, ACM TISSEC, vol. 5, no. 3, pp. 290331, 2002. Forman, G. 2003. An extensive empirical study of feature selection metrics for text classification. J. Mach. Learn. Res. 3 (Mar. 2003), 1289-1305.

[4] D. Boneh and B. Waters, Conjunctive, subset, and range queries on encrypted data, in Proc. 4th TCC, Amsterdam, The Netherlands, 2007, pp. 535554.Y.T. Yu, M.F. Lau, "A comparison of MC/DC, MUMCUT and several other coverage criteria for logical decisions", Journal of Systems and Software, 2005, in press.

[5] J. Camenisch, M. Dubovitskaya, and G. Neven, Oblivious trans- fer with access control, in Proc. 16th ACM Conf. CCS, New York, NY, USA, 2009, pp. 131140.

[6] S. Yu, C. Wang, K. Ren, and W. Lou,“Attribute based data sharing with attribute revocation,” in Proc. 5th ASIACCS, New York, NY, USA, 2010, pp. 261–270

[7] Y. Sun, F. Zhang, and J. Baek, “Strongly secure certificateless pub- lic key encryption without pairing,” in Proc. 6th Int. Conf. CANS, Singapore, 2007, pp. 194–208

Publish Research Article

Dear Sir/Mam,

We invite unpublished Research Paper,Summary of Research Project,Theses,Books and Book Review for publication.

Address:- Dr. Ashak Hussain Malik House No-221, Gangoo Pulwama - 192301 Jammu & Kashmir, India
Cell: 09086405302, 09906662570,
Ph No: 01933212815
Email:- nairjc5@gmail.com, nairjc@nairjc.com , info@nairjc.com
Website: www.nairjc.com