Scientific Journal of Impact Factor (SJIF): 3.134

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 2, Issue 12, December -2015

SECURE DATA SHARING IN PUBLIC CLOUD

Vinayak Bhau Bharekar [1], Swapnil Ramdas Mahajan [2], Mahesh Madhav Kulkarni [3], Ajinkya Nanaso Dhurgude [4], Prof.Mrs.Sarika Pabalkar [5]

[1,2,3,4,5] *Department of Computer Engineering, Dr.D.Y.Patil Institute of Engineering and Technology,Pimpri,Pune.*

Abstract- *As the current world become digital, therefore large amount of digital data needs to handle. For handling large amount of data there is need of cloud, as cloud provides large amount of storage and computing capacity. Public cloud is very efficient but security is major problem. Security issue can be solved by using mediated certificateless public key encryption (mCL-PKE). Public cloud involves mainly Key escrow problem and certificate revocation problem, both problems are solved by the mCL-PKE plan. The mCL-PKE scheme can be use for secure data sharing and it does not use pairing operation. Current schemes are expensive due to pairing and require maintaining certificate, which requires more memory and there is chances of attacks. In the mCL-PKE cloud act as key generation centre, generates respective public keys. Data owner encrypts the data using cloud generated public key and cloud then partially decrypts data. Then user fully decrypts data. This scheme fully secures the data from third party as cloud also not able to reveal the information. In mCL-PKE scheme fine grained data access control achieved by addition of new thing. In this data owner divides user in the form of group and single key to each user group. This reduces number of keys required to maintain, produced as well as data confidentiality is achieved.*

Keywords- *Security mediator, access control, bilinear pairing, cloud computing, cloud security.*

I. INTRODUCTION

As in the current scenario the internet is key element of life, whole world become interconnected to each other. It produces large amount of digital and online data; for storing this data cloud is required. Cloud computing has transformed the way organizations approach IT, enabling them to become more agile, introduce new business models, provide more services, and reduce IT costs. Public cloud is more efficient and economical to use. The most prominent issue that affects cloud performance is security. With data ownership getting isolated with its storage, the control access and usage of shared data remains a point of concern [1]. Cloud has various issues like lack of user control, privacy, security and cloud trust issues [2]. Cryptography need to handle to deal with security issues of cloud. There are various cryptography techniques. As the people start using cloud to share information then the security needs to maintain to avoid any attack. The information is transferred in the form of plain text then any intruder is able to hack the information. Therefore cryptography techniques are used to transfer the plaintext information to ciphertext [3].

Various cryptography methods are not efficient; it has various drawbacks [4]. So new advanced methods can be used to efficiently handle security problems. Proxy re-encryption, certificateless encryption are new methods [5]. But mediated certificateless public key encryption is very useful than other method [6][7].

II. LITERATURE REVIEW

VARIOUS SECURE DATA SHARING TECHNIQUES IN PUBLIC CLOUD

There are various methods are used for sharing data based on the different cryptography techniques.

1. Fine-grained data access control

AUTHORS: Li J, Zhao G, Chen X, Xie D, Rong C, Li W, Tang L, Tang Y

The systems with user accountability in cloud computing based on attribute based encryption (ABE) mainly consist of Key policy ABE and Cipher text ABE. It also uses Access Control List. It is not scalable and access to data is limited. If the attribute are matched then only user can decrypt data. This scheme has various drawbacks like computational complexities and certificate management [8].

2. **Fine grained access control and revocation**

AUTHORS: Tu S, Niu S, Li H, Xiao-ming Y, Li M

It provides high adapatability.Secret key and access control policy are also used. It has revocation problem; when user is revoked all data in cloud encrypted using user's key become useless. It solves problems of cipher text attack. It has large computation overhead and whole load on cloud [9].

3. **Identity based encryption**

AUTHORS: Dan Boneh and Matt Franklin

The system consists of public key system and certificate to ensure the user identification. As the certificates are involved in the user identification lot's of memory is required. Certificates are needs to maintain for each user. Major issue is revocation problem. It also uses the pairing operation based on elliptic curve. This also has complexity of pairing operation. Identity strings contain short validity period can be use to solve revocation problem, but not implemented [10].

4. Certificateless proxy re-encryption scheme

AUTHORS: Lei Xu, Xiaoxin Wu and Xinwen Zhang

It solves key escrow problem. Key escrow is a problem in which third party gets access to the key. But the pairing operation cost is major issue. The plain text attack security was achieved but cipher text attack not solved. As cipher text attack is need to consider in data sharing. There is no need of certificate management. In this system data is re-encrypted cloud and new encryption key is derived by the user and data owner keys. Maximum resources are used to reduce the communication cost to ensure security in semi reliable cloud [7].

III. SURVEY OF PROPOSED SYSTEM

We will use the mediated certificateless public key encryption scheme. This scheme is without pairing and there is no any certificate involved. So no need of certificate management and memory requirement is also less. In the scheme the Key generation centre and security mediator are also introduced. Key escrow problem is solved by using security mediator and Key generation produces keys. Key generation centre present in the cloud; cloud act as key generation centre as well as storage. Cloud only half decrypts the data and receiver is only who can fully decrypt data [6].

We added new element to mCL-PKE in which data owner divide user in the form of group and single key for each user group for decryption. User is grouped based on the location, project, department. Each user shares part of key. Data can be only decrypted when threshold number of user are present. It ensures confidentiality of data as well as fine grained control to data.

IV. MATHEMATICAL MODEL

1.Let S be the system.
S={ }
2.Identify I as input
I={ A}
Where A=Request by user
S={I}
3.Identify P as process
P={J,K,L,M,N}
Where J=Cloud set up
K=User registration
L=Grouping of user.
M=Data encryption and uploading
N=Checking threshold
R= Data decryption
S={I,P}
4.Identify O as output
O={C,D}
Where C=Key from key generation center
D=Data from cloud
S={I,P,O}

5.Identify Q as case of success
Q={ E,F}
Where E=User gets partial decrypted data
F=User gets key
S={I,P,O,Q}
5.Identify T as case of failure
T={H,J}
Where H=Key is compromised
J=Threshold not matched.
S={I,P,O,Q,T}

V. SYSTEM ARCHITECTURE

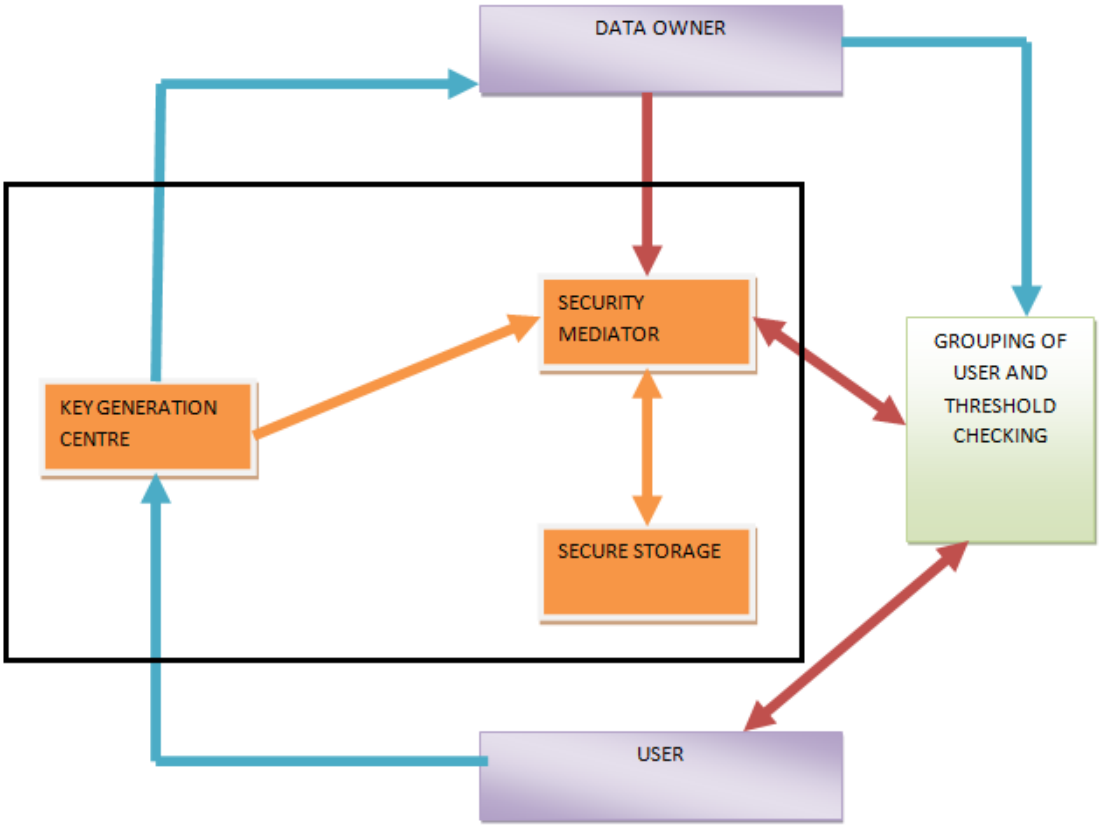

Figure 1.System Architecture

VI. CONCLUSION AND FUTURE WORK

The major advantage of approach is less computation overhead at the data owner side. It also takes care of the memory as size of certificate is less as compare to other. As the Key generation centre plays major role in this approach, key management is simple. The mediated CL-PKE uses the combination of private and public key and also introduced the concept of partial key. Further, the computation costs for decryption at the users are reduced as a semi-trusted security mediator partially decrypts the encrypted data before the users decrypt.

mCL-PKE approach can be used in any cloud system to ensure security of cloud. It will secure data of any user irrespective of the number of user. This mCL-PKE is added with grouping of user to provide data confidentiality. In future we can send data to user group securely and only certain number of user are there then only data is decrypted.

REFERENCES

[1] M. Jensen, J. Schwenk, N. Gruschka and L. L. Iacono, "Technical security issues in cloud computing", IEEE International Conference on Cloud Computing, 2010, p. 109.
[2] CSA, "Security Guidance for Critical Areas of Focus in Cloud Computing", 2009, Cloud Security Alliance.
[3] Kasundra Punit kumar R., Shikha J. Pachouly,"Data Security Policies in Cloud: A Survey",International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064 Impact Factor (2012): 3.358,Volume 3 Issue 12, December 2014.
[4] William Stallings "cryptography and network security principles and practice fifth edition" ISBN 13: 978-0-13-609704-4.
[5] Lei Xu, Xiaoxin Wu and Xinwen Zhang, "CL-PRE: a Certificateless Proxy Re-Encryption Scheme for Secure Data Sharing with Public Cloud," ASIACCS '12, May 2–4, 2012.
[6] Revathi. R.,"A Secure data sharing in cloud storage with Independent key generation centre and Certificate-less encryption",International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE),ISSN: 0976-1353 Volume 13 Issue 1 –MARCH 2015.
[7] S.Al-Riyami and K. Paterson, "Certificateless public key cryptography", in Proc. ASIACRYPT 2003, C.-S. Laih, Ed. Berlin, Germany:Springer, LNCS 2894, pp. 452–473.
[8] Li J, Zhao G, Chen X, Xie D, Rong C, Li W, Tang L, Tang Y, "Fine-grained data access control systems with user accountability in cloud computing," IEEE second international conference on cloud computing technology and science(CloudCom) 2010, pp 89–96.
[9] Tu S, Niu S, Li H, Xiao-ming Y, Li M, "Finegrained access control and revocation for sharing data on clouds," IEEE 26th international parallel and distributed processing symposium workshops and PhD forum (IPDPSW) 2012, pp 2146–2155.
[10] Dan Boneh and Matt Franklin, "Identity-Based Encryption from the Weil Pairing," SIAM Journal on Computing, 32(3):586–615, 2003.

AUTHORS

Vinayak Bhau Bharekar , pursuing the B.E degree in Computer Engineering at Dr.D.Y.Patil Institute of Engineering and Technology,Pimpri,Pune.

Swapnil Ramdas Mahajan , pursuing the B.E degree in Computer Engineering at Dr.D.Y.Patil Institute of Engineering and Technology,Pimpri,Pune.

Mahesh Madhav Kulkarni , pursuing the B.E degree in Computer Engineering at Dr.D.Y.Patil Institute of Engineering and Technology,Pimpri,Pune.

Ajinkya Nanaso Dhurgude , pursuing the B.E degree in Computer Engineering at Dr.D.Y.Patil Institute of Engineering and Technology,Pimpri,Pune.

Prof.Mrs.Sarika Pabalkar , Assistant Professor in Computer Engineering at Dr.D.Y.Patil Institute of Engineering and Technology,Pimpri,Pune.

