Volume 2, Issue 4, April 2017 ISSN (online): 2456-0006
International Journal of Science Technology Management and Research
Available online at: www.ijstmr.com

An Efficient Certificateless Encryption for Secure Data Sharing in Public Clouds

Bhavana Rajendra Deshmukh[1]
Department of Computer Engg.,
Amrutvehini college of engineering
Nashik, India

Shaila Namdev Darade[2]
Department of Computer Engg,
Amrutvehini college of engineering
Nashik, India

Akanksha Anil Gaikwad[3]
Department of Computer Engg,
Amrutvehini college of engineering
Nashik, India

Abstract: ***Cloud computing is one of the emerging technology, as it provides huge storage of in- formation which is then requested by the end user. This pairing free system ensures security and integrity of the data which is stored on to the cloud. The susceptible in formation is rest encrypted and then uploaded on to the cloud and that information is half decrypted by the cloud and given to the requested end user for the full decryption process. In case of the data having same access control policy is requested by multiple users then our system generates a single encryption key whereas previous system was supporting single key for an individual whether they are requesting for the data having same access control policies. Therefore in our system, time for accessing same data by multiple requesters will reduce automatically and also key management will be easy. As only half decryption process is done on to the cloud, the confidentiality of the data is maintained over cloud. After uploading of data the authentication is maintained by encryption whereas the integrity is ensured by auditing technique. In the case of any changes done to the uploaded data, will generate an alert message for the data owner. If considered the properties of confidentiality and integrity with respect to cloud then definitely there will be take in its performance graph as compared to the existing system.***

Keywords: ***Authentication, Auditing technique, Access control policies.***

I. INTRODUCTION

Today on-demand computing is introduced as a remarkable succeeding expansion. Cloud can deliver computing resources and services in a pay-as-you-go mode, which is expected to become as appropriate to use similar to known daily routine utilities like ignition, water, gas, electricity and telephone in the coming duration because of resource virtu- alization. These computing services can be sort by type as Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS). Day by day the technology is becoming very popular for storing of huge data to access it from anywhere. But there is a fear about the privacy of stored data. As in for gaining the con dence over con dentiality of susceptible data which is kept in public clouds, generally preferred procedure is while uploading information to the cloud that data should be encrypted. There is an assurance about the data confidentiality over cloud because we are using CL-PKC scheme [1] which avoids the pairing operations and also solves built in key escrow issues, hence in the proposed system cloud also does not know about the private keys (Sk) of user which is later required for the decryption process. As now the data is not been decrypted over cloud the secrecy of data is truly ensured. In some cases data uploaded over cloud is shared by multiple users so for that existing scheme named broadcast group key management (BGKM) [2] was used, in which the ACPs in addition to adding and removing of user rights was managed. However, in many organizations it is necessary to compelne-grained access control [3] to the data

IJSTMR © 2017 | All Rights Reserved

this mechanism of encryption should also be capable of supporting ne-grained encryption based access 12 control. Another way is to use a public key cryptosystem, in consideration of reducing the overhead in administration of keys. However, there is a need of Certi cateless cryp- tography [4] ethnic public key cryptosystem to overcome the key escrow and revocation issues and ensures con dentiality over cloud. The next technique named Identity-Based Public Key Cryptosystem (IBPKC) [5] [6] was acquaint, again it is having the key es- crow problem because the SK of all the end users is discovered by the key generation server. Then one more scheme was proposed recently named Attribute Based Encryp- tion (ABE) [7] [8] that permits one to encrypt each piece of data accordingly the access control policy applicable to the data. Proposed system is to defeat the shortcomings of such previous approaches and proposed a novel system providing secure encryption and auditing of content on public cloud (PS-EA) which oppose to the operations of pairing.

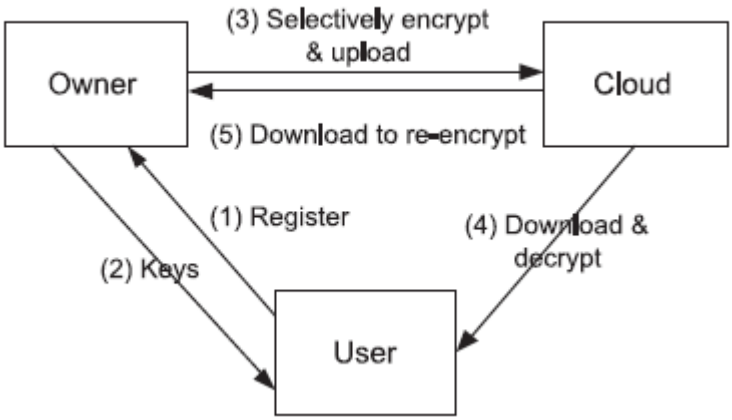

Fig-1.Sysmetric Key Based Fine Grained Encryption

II. RELATED WORK

We proposed a scheme named providing secure encryption and auditing of content on public cloud (PS-EA) against of pairing acts for securely sharing of hypersensitive in- formation in public clouds. Due to this system we can resolve the key escrow crunch of identity based encryption. Nevertheless, existing technologies used are either extrava- gant because of the utilization of very costly pairing act or susceptible against half-done decryption attacks. Here the cloud is protected storage as it decrypts only partial en- crypted content which is required by the user. This will reduce the load of decryption at user side. The data owner uploads the sensitive data using KGC generated public key whereas the user downloads the fully decrypted data by using its private key as well as KGC generated U key. As the cloud is partial decryptor hence security of data as well as the keys is maintained there.. 4 to intimate data owner about the fraud done with actual data. If any changes done to the originality of data it will give an alert message to the data owner for again sending the correct data. This will guarantee the integrity property over cloud. Mostly all of the CL-PKC schemes rely on computationally expensive bilinear pairings [9]. By using pairing-free approach, this guiding principle reduces the data processing overhead. As a partially trusted security mediator which moderately decrypts the en- crypted content before the users decrypt, therefore at user side the data processing cost for decryption are diminished. The security mediator is used for the acts like policy en- forcement point. This new means of arriving can e ectively handle keys and user ACPs. In the system of symmetric key, users are required to manage amount of keys equal to at least the logarithm of the amount of end users which was very hectic and opposite to that in our proposed work each user only required to preserve its public/private key pair. Due to the advantage of public cloud storage, industries have been accepting services related to public cloud such as Microsoft Skydrive [10] and Dropbox [11] to manage their data.

III. LITERATURE SURVEY

Our survey starts from certificateless public key cryptography [1], which consist of search for public key system that are against of utilization of certificateless and hence not having the built-in-key escrow aspect of ID-PKC, whereas consist of the shortcomings like public key cryptography is not needed in single-user environment. But public key cryptography for encryption is having some speed

issues and may be susceptible to imitation even if requester's private key is not available. In privacy conserving policy-based data sharing in public clouds [2], having a formalized innovative key administration scheme called broadcast group key management (BGKM) and system provides secure structure of a BGKM scheme entitled ACV-BGKM. Also provides an optimization to significantly improve performance of ACV-BGKM scheme. Professionally manages joining and departure of user with assured security. Also shows that users efficiently derive decryption keys and the data owner can manage efficiently bulk amount of users. It is unsuccessful in adding traitor tracing and also failed in privacy preserving querying potential. The Fine grained control of security capabilities [3], consist of certificate revocation and fine-grained control over security capabilities. Revocation is fast when its certificateless is revoked the client can no longer decrypt or sign messages. With binding signature semantics, there is no need to validate the certificateless as part of signature verification. Revocation technique is transparent to the peers since it uses standard RSA signals and 67 encryption formats. And drawback of the system is security mediator (SEM) architecture which is implemented for experimentation purpose. This is appropriate for only small-to medium-sized organization and is clearly not appropriate for the global internet or for educational campus like environments. The an efficient certificateless encryption for secure data sharing in public clouds"[4], provides SEM architecture. This ethnic public key cryptosystem to overcome the key escrow and revocation issues and ensures con_dentiality over cloud. But does not ensures the integrity.

IV. PRAPOSED SYSTEM

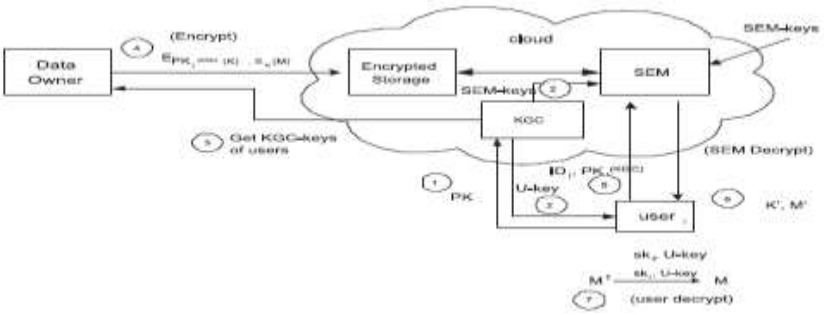

Fig. 2. Secure Cloud Storage

A. Secure Cloud Storage

In this section we provide a detailed description of our system for privacy preserving cloud storage using our mCL-PKE scheme.As shown in Fig. 2, our scheme consists of three entities: *data owner*, *cloud*, and *users*. The data owner possesses sensitive content that it wants to share with authorized users by storing it in the public cloud and requesting the cloud to partially decrypt the encrypted content when users request the data. The cloud consists of three main services: an encrypted content storage; a key generation center (KGC), which generates public/private key pairs for each user as explained in Section 2; and a security mediation server (SEM), which acts as a security mediator for each data request and partially decrypts encrypted data for authorized users. The cloud is trusted to perform the security mediation service and key generation correctly, but it is not trusted for the confidentiality of the content and key escrowing. Our approach allows one to have most of the key generation and management functionality deployed in the untrusted cloud as our mCL-PKE scheme does not have the problem of key escrowing and thus the KGC is unable to learn the full private keys of users. Our scheme consists of four phases: (1) Cloud set up; (2) User registration; (3) Data encryption and uploading and (4) Data decryption. Now we describe each of these phases in detail.

V. ALGORITHMIC STUDY

A) AES Algorithm:

Nowadays widely used encryption and decryption, symmetric key algorithm encountered is the Advanced Encryption Standard (AES). It is the fastest algorithm as compared to triple DES. We have chosen AES because it is a standardized cryptographic algorithm which provides us a huge security. It supports 128-bit block size with 128-bit keys. The features of AES are as follows:-

_ It is a parallel and symmetric structured algorithm therefore properly handles cryptanalysis bouts.17 18

_ This algorithm is amended for the current processor.

_ It is also suited for the smart cards. For encryption and decryption process AES algorithm is used. The basic ow of algo- rithm is as following.

1. User generates its Sk and Pk key pair.
2. User send its Pk to KGC.
3. KGC then generates two partial keys and one public key.
4. One partial key is known as SEM key which is given to the SEM. And another partial key is known as U key which is given to the user.
5. The KGC generated public key is known as KGC key which consists of user gen- erated public key (Pk) as well as KGC generated public key.
6. Then KGC key is given to the data owner. With the help of KGC key, the data owner will encrypt the data and upload that data on to the cloud.
7. User requests for the data by providing its ID to the SEM.
8. Accordingly request the SEM checks the access control list and if that user is authorized user then SEM will decrypt the data partially using its SEM key.
9. That partially decrypted data is then given to the authorized user for its full decryption using its U key and private key (Sk).

B) Hashing Algorithm:

Nearly all information security applications are enormously using Hash functions. A hash function is a scienti_c function that translates arithmetical input value to another compressed arithmetical value. The input to the hash function is always a message having arbitrary length but output is always a Hash value of fixed length.The value which we get as a final output is called as hash value because of hashing function applied over and sometimes it is also called as a message digest.

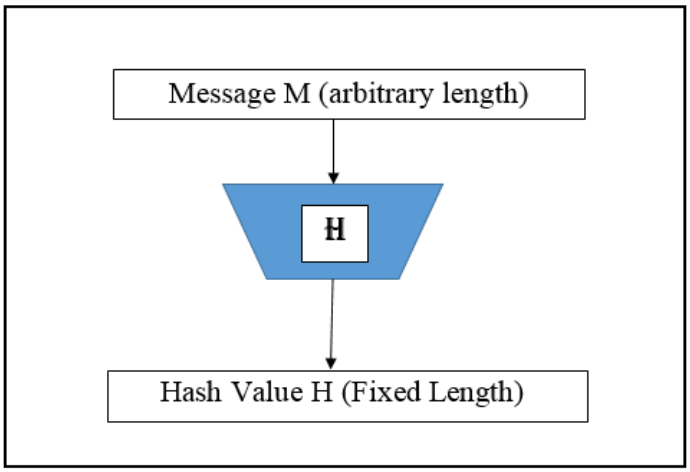

Fig. 3: Hash Value Architecture

For auditing, we are using SHA1 hashing technique as an elementary operation as it can be replaced easily with the other cryptographic hash function like SHA2. Hash key is generated before and after uploading of data on to the cloud. Whether there is an integrity in that uploaded data or not is confirmed by those hash Key values, if both are same then the data is in its consistent state else fraud is detected. In that case some alert messages will be generated to the data owner.

VI. EXPERIMENTAL RESULTS

In this section, we first present the experimental results for our mCL-PKE scheme. We then compare the basic approach with the improved approach. Finally we compare our approach with Lei *et al.*'s scheme[16]. The experiments were performed on a machine running 32 bits GNU Linux kernel version 3.2.0-30 with an Intel R _ Core TMi5-2430 CPU @ 2.40GHZ and 8 GBytes memory. Our prototype system is implemented in C/C++. We use V. Shoup's NTL library [24] version 5.5.2 for big number calculation and field arithmetic. The NTL library is compiled along with the GMP library [12] in order to improve the performance of computations involving large numbers. We construct the hash function required for the mCL-PKE scheme based on SHA1. For the hash functions, we use SHA1 as the elementary operation. However, SHA1 can easily be replaced with other cryptographic hash functions such as SHA2. The basic idea of the hash function construction is as follows.

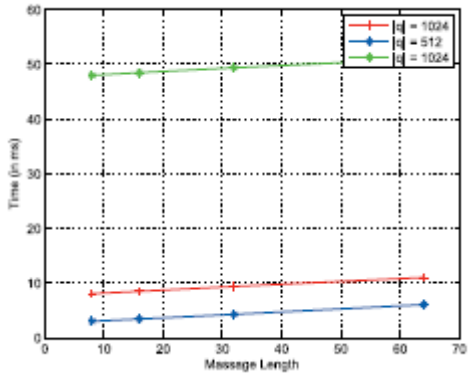

Fig. 4. Basic encryption.

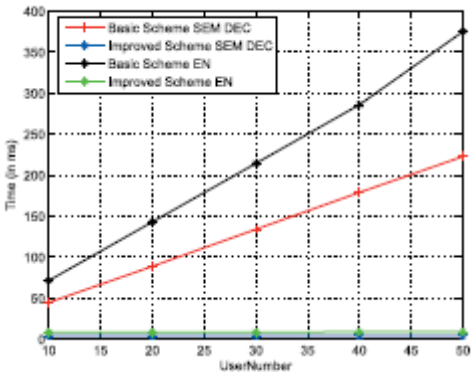

Fig. 5. Improved scheme

Based on the field of the hash function output, we break the input into multiple blocks, and the block number is dynamically adjusted. For each block, we execute SHA1, convert the output into decimal numbers, say $a1, a2, \ldots, an$. If the output field is $Z*q$, then we compute $(a1||a2||a3|| \cdots ||an) \bmod q$, where || denotes the concatenation operation, to get the final result of the hash function. This operation is very efficient even if other hash functions are used. According to our experimental results, it takes less than 1 ms to do this operation for a message of size 16KB. Fig. 4 shows the time required to perform the encryption operation in the mCL-PKE scheme for different message sizes. Since our scheme does not use pairing operations, it performs encryption efficiently. As can be seen from the graph, the encryption time increases linearly as the message size increases. As the bit length of q increases, the cost increases non-linearly since the encryption algorithm performs exponentiation operations. A similar observation applies to the the SEM decryption and user decryption. We also implemented the improved scheme where the data owner performs only one encryption per data item and creates a set of intermediate keys that allows authorized users to decrypt the data, In Fig. 5, we compare the time to perform encryption and decryption in the basic scheme and the improved scheme as the number of users who can access the same data increases from 10 to 50. We fixed the length of q to 1, 024 bits and the message size to 16KB. It is evident from the graph that as more users are allowed to access the same data item, the better the improved scheme performs compared to the basic scheme. The cost of the basic scheme is high since the encryption algorithm is executed for each user.

CONCLUSION AND FUTURE WORK

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 untrusted 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. S. Al-Riyami and K. Paterson, Certi_cateless public key cryptography, in Proc. ASIACRYPT, C.-S. Laih, Ed. Berlin, Germany:Springer, LNCS 2894, pp. 452-473, 2003.
2. N. Shang, M. Nabeel, F. Paci, and E. Bertino, A Privacy-Preserving Policy-Based Content Sharing in Public Clouds,Proc. IEEE VOL.25,NO. 11, November 2013.
3. D. Boneh, X. Ding, and G. Tsudik, Fine-grained control of security capabilities, ACM Trans. Internet Technol., vol. 4, no. 1,pp. 6082, Feb. 2004.
4. Seung-Hyun Seo, Xiaoyu Ding, "An E_cient Certi_cateless Encryption for Secure Data Sharing in Public Clouds" IEEE Transactions on Knowledge and Data Engi- neering, Volume 26, Number 9, September, pp. 2107-2119, 2014.
5. A. Sahai and B. Waters, Fuzzy identity-based encryption, LNCS3494 in Proc. EU- ROCRYPT, Aarhus, Denmark, pp. 457-473, 2005.
6. D. Boneh and M. K. Franklin. Identity based encryption from the Weil pair- ing.SIAM Journal on Computing, 32(3), 2003.
7. J. Bethencourt, A. Sahai, and B. Waters, Ciphertext-policy Attribute -based en- cryption, in Proc. IEEE Symp.SP,Taormina, Italy, pp. 321334, 2007.
8. S. Yu, C. Wang, K. Ren, and W. Lou,Attribute based data sharing with attribute revocation, in Proc. 5th ASIACCS, New York, NY,USA, pp. 261270, 2010.
9. J. Baek, R, Safavi-Nani and W. Susilo. Certi_cateless Public Key Encryption with- out Pairing. In Proc. ISC 2005, LNCS 3650, Berlin: Springer-Verlag,. pp.134-140, 2005. 8384
10. Microsoft Co. Ltd. Microsoft skydrive [online]. Available: https://skydrive.live.com/
11. I. Dropbox. Dropbox [online]. Available: https://www.dropbox.com/
12. V. Goyal, O. Pandey, A. Sahai, and B. Waters, Attribute-based encryption for _ne- grained access control of encrypted data,in Proc. 13th ACM Conf. CCS, New York, NY, USA,pp. 8998, 2006.
13. G. Miklau and D. Suciu, Controlling access to published data using cryptography, in Proc. 29th Int. Conf. VLDB, Berlin,Germany, pp. 898909, 2003.
14. 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, LNCS1462.
15. M. Abdalla et al., Searchable encryption revisited: Consistency Properties , relation to anonymousibe, and extensions, J. Cryptol.,vol. 21, no. 3, pp. 350391, Mar. 2008
16. N. Shang, M. Nabeel, F. Paci, and E. Bertino,A privacy preserving approach to policy-based content dissemination, in Proc. IEEE 26th ICDE, Long Beach, CA, USA, pp. 944955, 2010.
17. [17] J. Camenisch, M. Dubovitskaya, and G. Neven, Oblivious transfer with access con- trol, in Proc. 16th ACM Conf. CCS, New York,NY, USA, pp. 131140, 2009.
18. D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano. Public key encryption with keyword search. In EUROCRYPT 2004, LNCS 3027. Springer, 2004.
19. D. Boneh and B. Waters, Conjunctive, subset, and range queries on encrypted data, in Proc. 4th TCC, Amsterdam,The Netherlands, pp. 535554, 2007.
20. 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, pp. 501520, 2009.
21. Joonsang Baek and Yuliang Zheng. Identity-based Threshold Decryption. In Pub- lic Key Cryptography - PKC 2004, 7th International Workshop on Theory and Department of Computer Engineering (ME), SITRC,Nashik. 85 Practicein Public Key Cryptography, Singapore, March 1-4, 2004, volume 2947 of LNCS,pages 262276. Springer, 2004.
22. Boneh, D., Gentry, C., Hamburg, M.: Space-e_cient identity based encryption without pairings. In: FOCS, pp. 647657 (2007)
23. C. Yang, F. Wang, and X. Wang,E_cient mediated certi_cates public key encryp- tion scheme without pairings, in AINAW,Niagara Falls, ON, pp. 109112, May. 2007.
24. J. Bethencourt, A. Sahai, and B. Waters, Ciphertext-Policy Attribute-Based En- cryption, Proc. IEEE Symp. Security and Privacy(SP 07), pp. 321-334, 2007.
25. S. Goldwasser, S. Micali and R. Rivest, A digital signature scheme secure against adaptive chosen-message attack, In: Siam J. Computing,17(2), pp. 281-308, 1988.
26. H. S. Ju, D. Y. Kim, and D. H. Lee et al. E_cient Revocation of Security Capability in Certi_cateless Public Key Cryptography. In Proc. of KES 2005, LNAI 3682, Berlin: Springer-Verlag, pp. 453-459, 2005..
27. B.Libert and J. Quisquater. E_cient revocation and threshold pairing based cryp- tosystems. PODC 2003.Boston, Massachusetts. 2003. pp.163-171,2003.
28. Yinxia Sun and Futai Zhang,Secure Certi_cateless Public key Encryption without Redundancy, http://eprint.iacr.org.
29. E. Bertino and E. Ferrari. Secure and selective dissemination of XML documents, ACM TISSEC, vol. 5, no. 3, pp. 290331, 2002.
30. D. Pointcheval and J. Stern, Security arguments for digital signatures and blind signatures, J. Cryptology, vol. 13, no. 3,pp. 361396, 2000.
31. Krishna Kumar L and Deepa P Sivan, Preserving Public Auditing and Privacy Policy for shared data in the cloud,IJCSIT/VOL 6(2),pp.1092-1095,2015.

IJSTMR © 2017 | All Rights Reserved