Scientific Journal Impact Factor (SJIF) : 3.518
International Journal of Modern Trends in Engineering and Research
ISSN (ONLINE) : 2349 - 9745 ISSN (PRINT) : 2393 - 8161

A Certificate less Encryption for Data Sharing Securely in Public Cloud

Prof P.V.Waje[1] ,Sonawane Shwetambari P.[2] ,Sawal Pranali P.[3], Shinde Priyanka P. [4] , Sangale Pallavi M.[5]

[1] *Assistant Professor,* [2,3,4,5]*B.E. Students,*

I.T. Dept., S.V.I.T. Nashik, India

Abstract- For securely sharing sensitive information in public clouds, we propose a mediated certificate less encryption scheme without pairing operations. The problem related to key escrow in IBE and certificate expiration problem in public key cryptography, mediated certificate less public key encryption solves. Due to the use of costly pairing operations or weakness against partial decryption attacks, however, existing mCL-PKE schemes are either inefficient. We first propose a mCL-PKE scheme without using pairing operations, in order to address the performance and security issues. Solution to the problem of sharing sensitive information in public clouds, we apply our mCL-PKE scheme to construct a practical. A secure storage as well as a key generation center, the cloud is employed. Public keys based on its access control policies and upload the encrypted data to the cloud; the data owner encrypts the sensitive data using the cloud generated users. The encrypted data for the users, upon successful authorization, the cloud partially decrypts. The partially decrypted data using their private keys, the users subsequently fully decrypt. Because the cloud cannot fully decrypt the information, the confidentiality of the content and the keys is preserved with respect to the cloud. To improve the efficiency of encryption at the data owner, we also propose an extension to the above approach. Evaluates its security and performance, we implement our mCL-PKE scheme and the overall cloud based system. Results show that schemes used are practical and efficient.

Key Words-- Access control, certificate less cryptography, cloud computing, confidentiality

I. Introduction

Now a days cloud computing has become the technology that has been used in every possible area. When using services offered by cloud, the organizations using such services should be aware of the threats posed by different cloud service providers and cloud users. To ensure confidentiality of data uploaded on cloud we use techniques like encryption. In this scheme we provide a technique of securing data with encryption uploaded on cloud. This scheme eliminates the failures of previous schemes.

In previous schemes approaches like IBE (Identity Based Encryption)[2], ABE(Attribute Based Encryption)[5],and many others were used. All these approaches proved to be inefficient because of their time consuming pairing operations. Also these schemes were certificate based that is user had a registration certificate of cloud services. These certificates had problem of revocation. Our scheme is certificate less and hence proves to be efficient as there is no issue of certificate revocation and we provide a pairing free approach. This scheme is efficient also because we provide access to multiple users at a time.

II. Literature survey

Existing System

A Certificateless Public Key Cryptography (CL-PKC) was introduced by Al-Riyami and Paterson in 2003. Since it removed the key escrow problem and certificate management problem but pairing of key was still the problem. Handling key was expensive and inefficient computation cost

required was high. CL-PKE without pairing operations was introduced to improve efficiency. But key revocation problem was still the issue.

In some cases security related to private key was comprised for this Boneh*et al.*proposed the concept of mediated cryptography with security mediator (SEM) which has control security capabilities. SEM can stop the user from accessing if found revoked.

Notion of security-mediated certificateless cryptography was introduced by Chow *et al.*itwas based on pairing operations. Mediated CLPKE without pairings was first proposed by Yang *et al.* but was insecure for partil decryption attacks. Our approach provides security against this attack.

III. Proposed System

- Better security proof and security model than existing system. A new mCL-PKE scheme. Since the pairing-based operations are eliminated, computational overhead is reduced. Moreover, to efficiently encrypt data for multiple users an extension is introduce of mCL-PKE scheme.
- KCG is semi-trusted. It can be placed in public cloud the reason is it does not have key escrow problem. This introduces to securely share data in a public cloud.
- Implemented mCL-PKE scheme and the extension to evaluate the performance. The experimental result shows that our mCL-PKE scheme can be realistically applied in a public cloud for secure data sharing.

A. Proposed System Architecture:

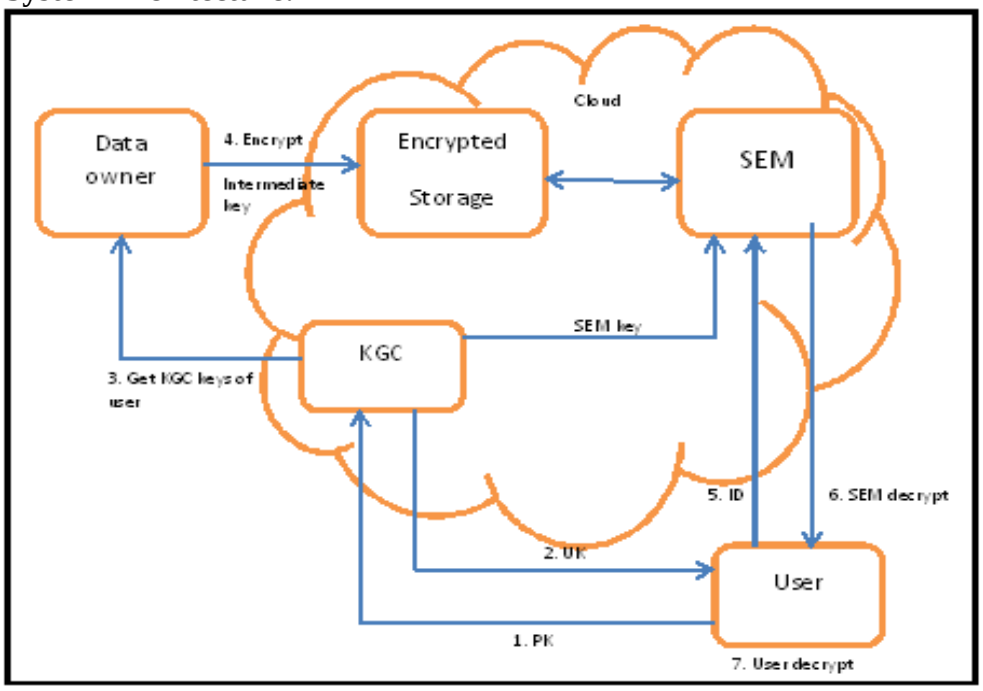


Figure 1: Proposed System Architecture.

B. Proposed System Algorithm

Blowfish algorithm

The data transformation process for Pocket Brief uses the Blowfish *Algorithm* for Encryption and Decryption, respectively. Blowfish Algorithms a **Feistel Network**, iterating a simple encryption function 16times. The size of block 64 bits, and the length of the key can be 448 bits.. Even if there is a difficult beginning phase required before any encryption can take place, the actual encryption of data is very efficient on large microprocessors.

Blowfish is a variable-length key block cipher. The applications in which the key remains same for a longer period of time, like a communications link or an automatic file encryptor, blowfish is suitable for all these. Its speed of execution is faster than most encryption algorithms when implemented on 32-bitmicroprocessors with number of data caches.

C. Algorithm Technique

A technique called Feistel network is a method which is usually used for converting any function (generally called an F function) into a permutation. It was invented by Horst Feistel and has been used in many block cipher designs. The way the technique works is given below:

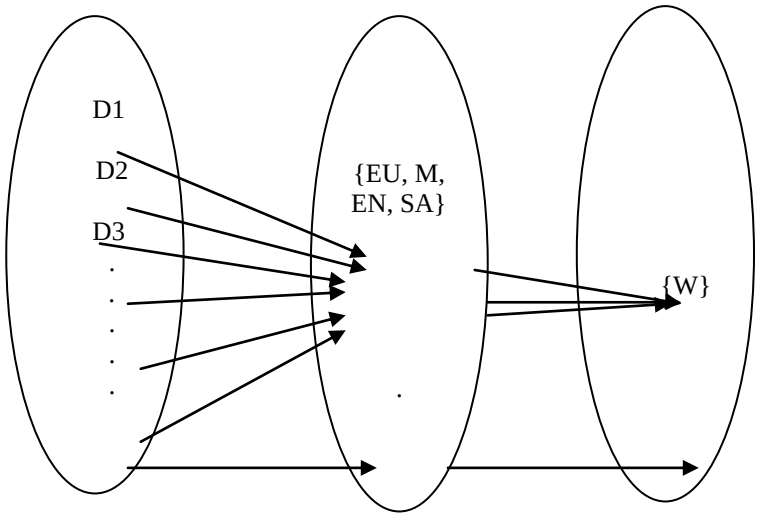
- Split each block into halves
- Right half becomes new left half
- New right half is the final result when the left half is XOR'd with the result of
- Applying *f* to the right half and the key.

Note that previous rounds can be obtained even if we are unable to invert function f

IV. Mathematical model

Mathematical model of Proposed System

Sr No.	Contents	UML Design Description
1.	**Problem Description** The system aims is Cloud computing is emerging as a prevalent data interactive paradigm to realize users' data remotely stored in an online Cloud server. 1) ERP (user). 2) Middleware 3) Encryption. 4) Upload / Download Data. 5) Combined Authority. Let the system be described by S, S={D, EU, CN, EN , SA,TP}	Where S: is a System. D: Set of training dataset EU: ERP (user). M: Middleware. EN: Encryption. SA: Upload Data. TP: Download Data.
2.	**Activity** A={a1,a2,…….an} B={b1, b2 ……., bn} C={c1, c2, ……., cn} V={v1, v2, ……., vn} K={k1, k2, ……., kn} W={w1, w2, ……., wn} Y={ EU, CN,EN , SA,TP}	A is a given dataset B is features associated ERP. C is Cloud Middleware. V is features associated for Encryption. K is Combined Authority. W is Download Data Y is a set of techniques use for Cloud Computing.

3.		D: Set of training dataset EU: ERP (user). M: Cloud Middleware. EN: Encryption. SA: Upload Data. W: Download Data.

Advantages/Applications of Proposed System

- It is a paring free approach
- Revocation problem of certificate is eliminated
- Multiple users can access the data at a time without any overhead
- Secure against partial decryption attack and chosen cipher text attack

V. Conclusion

In this paper we have proposed the first mCL-PKE scheme without pairing operations and provided its formal security.The key escrow problem and revocation problem are solved by using this mCL-PKE scheme. This mCL-PKE scheme works as a key building block, for an improved approach to securely share sensitive data in public clouds. Immediate revocation and confidentiality of the data are supported by our approach stored in an untrusted public cloud while enforcing the access control policies of the data owner. In this scheme experimental results show the efficiency of basic mCL-PKE a better approach for the public cloud. Further, for multiple users satisfying the same access control policies, our improved approach each data item is encrypted only once also reduces the overall overhead at the data owner.

VI. Acknowledgement

We take this opportunity to express hearty thanks to all those who helped us in the completion of the project on "An Efficient Certificateless Encryption for Secure Data Sharing in Public Cloud".We express deep sense of gratitude to our Project Guide Prof. P. V. Waje and H.O.D. Prof. P. V. Waje, Asst. Prof., Information Technology Department, Sir Visvesvaraya Institute of Technology, Chincholi for their guidance and continuous motivation. We gratefully acknowledge the help provided by our Project Guide Prof. P. V. Waje of Guide on many occasions, for improvement of this project with great interest.

We would like to extend our sincere thanks to our family members. It is our privilege to acknowledge their cooperation during the course of this Project. We express heartiest thanks to my known and unknown well-wishers for their unreserved cooperation, encouragement and suggestions during the course of this Project. Last but not the least, we would like to thanks to my all teachers, and all my friends who helped us with the ever daunting task of gathering information for the Project.

References

[1] M. Abdallaet al., "Searchable encryption revisited: Consistency properties, relation to anonymousibe, and extensions," J. Cryptol.,vol. 21, no. 3, pp. 350–391, Mar. 2008.
[2] S. Al-Riyami and K. Paterson, "Certificateless public key cryptography," inProc. ASIACRYPT 2003, C.-S. Laih, Ed. Berlin, Germany: Springer, LNCS 2894, pp. 452–473.
[3] 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.
[4] E. Bertino and E. Ferrari. "Secure and selective dissemination of XML documents," ACM TISSEC, vol. 5, no. 3, pp. 290–331, 2002.
[5] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext - policy attribute-based encryption," in Proc. 2007 IEEE Symp. SP, Taormina, Italy, pp. 321–334.
[6] 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.
[7] D. Boneh and B. Waters, "Conjunctive, subset, and rangequeries on encrypted data," in *Proc. 4th TCC*, Amsterdam, TheNetherlands, 2007, pp. 535–554.
[8] 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.
[9] 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.
[10] S. Coull, M. Green, and S. Hohenberger, "Controlling access toan oblivious database using stateful anonymous credentials," in *Irvine: Proc. 12th Int. Conf. Practice and Theory in PKC*, Chicago, IL,USA, 2009, pp. 501–520.

