Capability of Certificate less Cryptography for Secure Data Sharing Over the Network

Pushpalata Gondake, Pallavi Khandagale, Vidya Tanpure, Prof S.K.Said

Abstract— A mediated certificateless encryption scheme without pairing operations for se-curely sharing sensitive information in public clouds. Mediated certificateless pub-lic key encryption (mCL-PKE) solves the key escrow problem in identity based encryption and certificate revocation problem in public key cryptography. How-ever, existing mCL-PKE schemes are either inefficient because of the use of ex-pensive pairing operations or vulnerable against partial decryption attacks. In or-der to address the performance and security issues, in this paper, we first propose a mCL-PKE scheme without using pairing operations .In our system, the data owner encrypts the sensitive data using the cloud generated users public keys based on its own access control policies and uploads this 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.

Index Terms— Certificateless, cryptography, public cloud, confidentiality, security.

I. INTRODUCTION

Cloud is not another innovation, but rather another conveyance technique in which administrations are facilitated on third gathering resources. Because of its disseminated engineering, security is one of the prime worry in distributed computing. There are different security models proposed and conveyed upto now, yet none of these is said to be full confirmation. So there are different research going ahead to make the cloud condition more proficient and secure .Distributed computing is generally utilized administration display for capacity i.e. Capacity as an administration that empowers client to share their information out in the open cloud . Open distributed storage model to settle the basic issue of information secrecy that information just got to by approved clients. Shared delicate information must be emphatically secured from unapproved access over the mists. With a specific end goal to guarantee privacy of touchy information put away out in the open mists, an ordinarily utilized approach is to scramble the information before transferring it to the cloud. Since cloud does not know the keys that we are utilized to encode the information, the secrecy of information from distributed storage is guaranteed. There are numerous security strategies officially existing to give the security. Security systems are utilized to give confirmation, secrecy and mix benefits in the cloud condition Main security mechanism comes under any of these two categories: Symmetric key mechanism and Asymmetric key mechanism. Fine grained encryption access control of the data is processed with the symmetric key based method. Symmetric key based mechanisms have various problems as handling uniqueness of keys, which in turn incurs high key management cost. To address certificate management issue new system as Identity Based Public Key cryptosystem (IB-PKC) was introduced but it had a key escrow problem which means the key generation server knows the private keys of a user. So this scheme not safe to assure users privacy.

Characteristic Based Encryption give the adaptability to the client to scramble each information thing based upon their get to control strategy. In any case, it likewise had the denial issue in light of the fact that the private key gave to the current clients must be refreshed at whatever point a client dynamic changes. Al-Riyami and Paterson built up another component called Certificateless Public Key Cryptography (CL-PKC). Next the Certificate less Proxy Re-Encryption system was presented for secure information partaking out in the open cloud. This instrument depends on CL-PKC to expel the key escrow issue and authentication administration issue in spite of the fact that utilizations blending operation. To address above issue the idea of interceded cryptography has been utilized which bolster prompt denial. System of intervened cryptography makes a handy and powerful utilization of security arbiter (SEM). Security middle person can control security capacities for each exchange. The client s interest in an exchange will ceased instantly, once the SEM is been advised that a client s open key ought to be renounced. A documentation of security intervened certificateless cryptography isacquainted with present a mCL-PKE which relies on the matching operations, the computational costs required for blending are still impressively high. In the event that client applies the fundamental mCL-PKE plan to the distributed computing condition or numerous clients get to similar information, the cost of encryption turns out to be high for information proprietor. In this circumstance information proprietor ought to encode the information content with a similar encryption key for various circumstances. To expel this trouble, the essential mCL-PKE plot with an expansion had been presented. The expanded plan makes the information proprietor to apply the information encryption key process just once not numerous circumstances such as past plan which in turns gives some additional dat data owner.

In this situation data owner should encrypt the data content with the same encryption key for multiple times. To remove this difficulty, the basic mCL-PKE scheme with an extension had been introduced. The extended scheme makes the data owner to apply the data encryption key process only once not multiple times like previous scheme which in turns provides some added information to the network. So with use of this additional information the authorized users can decrypt their content using the private keys. This scheme is similar to

that of the Proxy ReEncryption (PRE) in which the encryption key is encrypted using the data owner's public key and continue later to decrypt using different private keys. In this extension scheme, network does not perform any transformation it simply acts as the storage model. The security models of the existing schemes are insecure against partial decryption attack. So secure mediated CL-PKE without pairings is needed. The idea behind this scheme is that data owner encrypts the data and after encryption process sends the encrypted data over the network. Then the network partial decrypts the encrypted document and it to the requested users. The user, then fully decrypt the data content using their private keys. The extremely important thing is that, if more than one user are accepted and they want to get the access to same document then encryption rate will be enormously high for data owner since owner has to encrypt the same document several times for different users using the user's public key in previous mediated Certificateless public key encryption scheme. To overcome this difficulty the extended mCL-PKE system is, data owner encrypts the data only one time and sends the extra information to the network for certified users to decrypt the data. But in this proposed system there is no need of extra information for the user to decrypt the encrypted data.

II. Objectives

1. Sharing of data securely in database.
2. To show how the AES-128bit is different from AES-256bit.sy.
3. By removing Certificate authority we reduce the Cost.

III. Literature Review

An efficient certificateless encryption for secure data sharing in public clouds [1], We propose a mediated certificateless encryption scheme without pairing operations for securely sharing sensitive information in public clouds. Mediated certificateless 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.

Searchable Encryption Revisited [2], We identify and fill some gaps with regard to consistency (the extent to which false positives are produced) for public-key encryption with keyword search (PEKS). We define computational and statistical relaxations of the existing notion of perfect consistency, show that the scheme of Boneh et al. is computationally consistent, and provide a new scheme that is statistically consistent.

Certificateless public key cryptography [3], This paper introduces and makes concrete the concept of certificateless public key cryptography (CL-PKC), a model for the use of public key cryptography which avoids the inherent escrow of identitybased cryptography and yet which does not require certificates to guarantee the authenticity of public keys. The lack of certificates and the presence of an adversary who has access to a master key necessitates the careful development of a new security model. We focus on certificateless public key encryption (CL-PKE), showing that a concrete pairing-based CL-PKE scheme is secure provided that an underlying problem closely related to the Bilinear Diffie-Hellman Problem is hard.

Enhancing Cloud Computing Security using AES Algorithm [4] ,With the tremendous growth of sensitive information on cloud, cloud security is getting more important than even before. The cloud data and services reside in massively scalable data centers and can be accessed everywhere. The growth of the cloud users has unfortunately been accompanied with a growth in malicious activity in the cloud. More and more vulnerabilities are discovered, and nearly every day, new security advisories are published. Millions of users are surfing the Cloud for various purposes, therefore they need highly safe and persistent services.

Relations among notions of security for public-key encryption schemes [5], We compare the relative strengths of popular notions of security for public key encryption schemes. We consider the goals of privacy and non-malleability, each under chosen plaintext attack and two kinds of chosen ciphertext attack. For each of the resulting pairs of definitions we prove either an implication (every scheme meeting one notion must meet the other) or a separation (there is a scheme meeting one notion but not the other, assuming the first notion can be met at all). We similarly treat plaintext awareness, a notion of security in the random oracle model. An additional contribution of this paper is a new definition of non-malleability which we believe is simpler than the previous one.

Enhanced Key Expansion for AES-256 by Using Even-Odd Method [6], This study is conducted to determine an alternative, creative method for designing Key Expansion in AES-256 that is called Even-Odd (E-O) method. The proposed every day, new security advisories are published. Millions of users are surfing the Cloud for various purposes, therefore they need highly safe and persistent services.

Relations among notions of security for public-key encryption schemes [5],We compare the relative strengths of popular notions of security for public key encryption schemes. We consider the goals of privacy and non-malleability, each under chosen plaintext attack and two kinds of chosen ciphertext attack. For each of the resulting pairs of definitions we prove either an implication (every scheme meeting one notion must meet the other) or a separation (there is a scheme meeting one notion but not the other, assuming the first notion can be met at all). We similarly treat plaintext awareness, a notion of security in the random oracle model. An additional contribution of this paper is a new definition of non-malleability which we believe is simpler than the previous one.

IV. Problem Statement

In our system, the data owner encrypts the sensitive data using the database generated users public keys based on its access control policies and uploads the encrypted data to the database. Upon successful authorization, the database 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 database, because the database cannot fully decrypt the information. We also propose an extension to the above approach to improve the efficiency of encryption at the data owner.

V. Proposed Work

In order to reduce the overhead of key management, an alternative is to use a public key cryptosystem. However a traditional public key cryptosystem require a trusted Certificate Authority to intiate digital certificates likes that bind to share public keys. Because the CA has to generate its own signature on each users public key and manage each users certificate, the overall certificate management is very expensive and complex. To address such shortcoming, the Based public key cryptosystem (mCL-PKC) was introduced, but it arrives from the key encrypt problems on that key generation server learns the private keys of all users.

In order to address the key encrypt problem in IB-PKC, Al-Riyami and Paterson introduces a new cryptosystem called Certificateless Public Key Cryptography (CL-PKC). The Certificate less Proxy Re-Encryption mechanism was introduced for secure data sharing in public network. This mechanism is based on CL-PKC to remove the key escrow problem and certificate management issue although uses pairing operation. To address above problem the concept of mediated cryptography has been used which support immediate revocation.

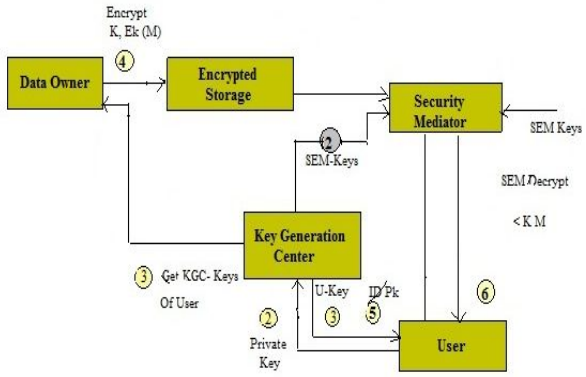

Fig 1. System Architecture

In proposed system each user first generates its own private and public key pair, called PK and PubK, using the SetPrivateKey and SetPublicKey operations respectively using our mCLPKEscheme. The user then sends its public keys and its identity (ID) to the KGC in the network. The KGC generates two keys for the user. One key, referred to as SEM-key, is stored at the SEM in the network. The other key, referred to as Userkey, is given to the user. The data owner obtains the KGC-keys of users from the KGC in the network. The data owner then encrypts each data item for which the same access control policy applies using a key K and then the data owner encrypts K using the KGC-keys of users. The encrypted data is uploaded to the network. When a user wants to read some data, it sends a request to the SEM to obtain the partially decrypted data. The SEM first checks if the user is in the access control list and if yes then users KGC-key encrypted content is available in the network storage. If the verification is successful, the SEM retrieves the encrypted content from the network and partially decrypts the content using the SEM-key for the user. The partial decryption at the SEM reduces the load on users. The user uses its SK and U-key to fully decrypt the data.

VI. Algorithm Implementation

AES encryption algorithm is used to provide security in public network because AES is considered secure. Encryption and decryption time taken by AES is minimum as compared to others. So it is fastest block cipher algorithm amongst all analyzed cipher algorithms such as blowfish, DES, triple DES.

Advanced Encryption Standard i.e. AES 128 bit block consist of following steps:

1. Derive the set of round keys from the cipher key.
2. Initialize the state array with the block data (plaintext).
3. Add the initial round key to the starting state array.
4. Perform nine rounds of state manipulation.
5. Perform the tenth and final round of state manipulation.
6. Copy the final state array out as the encrypted data (ciphertext).

Working Of AES:

Following steps gives detail working of AES algorithm over a network.

A. Key Expansion

Round keys are derived from the cipher key using Rijndael's key schedule. AES requires a separate128-bit round key block for each round plus one more.

B. Initial Round

Add Round Key- each byte of the state is combined with a block of the round key using bitwise XOR.

C. Rounds

a. SubBytes- non-linear substitution step where each byte is replaced with another.

b. ShiftRows - A transposition step where the last three rows of the state are shifted cyclically a certain number of steps.

c. MixColumnn - A mixing operation which operates on the columns of the state, combining the four bytes in each column.

d. AddRoundKey

D. Final Round (n+o Mix Columns)

a. SubBytes
b. ShiftRows
c. AddRoundKey.

VII. RESULT

Fig 2. Partial Decrypt

Fig 3. Admin Key Accept

Fig 4. Complete Decrypt

Fig 5. Send Data

CONCLUSION

A traditional public key cryptosystem requires a trusted Certificate Authority (CA) to issue digital certificates that bind users to their public keys. Because the CA has to generate its own signature on each user's public key and manage each user's certificate, the overall certificate management is very expensive & complex. To address such shortcoming, and to obtain high security to the cloud data over a network, and to improve the efficiency of the encryption. We propose an extension to our approach. We propose our mCL-PKE scheme, the overall network based system, evaluates its security and performance. It will be much less costlier, less complex and strictly secure security mechanism to deal with network security issues. We proposed an improved approach to securely share sensitive data in our database. Our approach supports immediate revocation and assures the confidentiality of the data stored in an untrusted database while enforcing the access control policies of the data owner.

ACKNOWLEDGMENT

Authors thanks project guide Prof. S. K. Said who always being with presence & constant, constructive criticism to made this paper. We would also like to thank all the staff of computer department for their valuable guidance, suggestion and support through the paper work, who has given co-operation for the project with personal attention. Above all we express our deepest gratitude to all of them for their kind-hearted support which helped us a lot during paper work. At the last we thankful to our friends, colleagues for the inspirational help provided to us through a paper work.

REFERENCES

[1] S.-H. Seo, M. Nabeel, X. Ding, and E. Bertino, "An efficient certificateless encryption for secure data sharing in public clouds," Knowledge and Data Engineering, IEEE Transactions on, vol. 26, no. 9, pp. 2107–2119, 2014.

[2] M. Abdalla, M. Bellare, D. Catalano, E. Kiltz, T. Kohno, T. Lange, J. MaloneLee, G. Neven, P. Paillier, and H. Shi, "Searchable encryption revisited: Consistency properties, relation to anonymous ibe, and extensions," in Advances in Cryptology–CRYPTO 2005, pp. 205–222, Springer, 2005.

[3] S. S. Al-Riyami and K. G. Paterson, "Certificateless public key cryptography," in Advances in Cryptology-ASIACRYPT 2003, pp. 452–473, Springer, 2003.

[4] A. Sachdev and M. Bhansali, "Enhancing cloud computing security using aes algorithm," International Journal of Computer Applications, vol. 67, no. 9, pp. 19–23, 2013.

[5] M. Bellare, A. Desai, D. Pointcheval, and P. Rogaway, "Relations among notions of security for public-key encryption schemes," in Advances in CryptologyCRYPTO'98, pp. 26–45, Springer, 1998.

[6] I. Saberi, B. Shojaie, and M. Salleh, "Enhanced key expansion for aes-256 by using even-odd method," in Research and Innovation in Information Systems (ICRIIS), 2011 International Conference on, pp. 1–5, IEEE, 2011.

[7] S. Heron, "Advanced encryption standard (aes)," Network Security, vol. 2009, no. 12, pp. 8–12, 2009.

[8] L. Xu, X. Wu, and X. Zhang, "Cl-pre: a certificateless proxy re-encryption scheme for secure data sharing with public cloud," in Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security, pp. 87–88, ACM, 2012.

[9] [1] Tu S, Niu S, Li H, Xiao-ming Y, Li M, "Fine-grained 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] [2] Dan Boneh and Matt Franklin, "Identity-Based Encryption from the Weil Pairing," SIAM Journal on Computing, 32(3):586–615, 2003.