Impact Factor (SJIF): 4.542

International Journal of Advance Research in Engineering, Science & Technology

e-ISSN: 2393-9877, p-ISSN: 2394-2444

Volume 4, Issue 5, May-2017

Capability Of Certificateless Cryptography For Secure Data Sharing Over the Network

Gondake Pushpalata B[1], Khandagale Pallavi R[2],Tanpure Vidya S[3], Prof. S.K.Said.[4]

[1]*Final Year Student of Department of Computer engineering, Jaihind College of engineering, kuran*

[2]*Final Year Student of Department of Computer engineering, Jaihind College of engineering, kuran*

[3]*Final Year Student of Department of Computer engineering, Jaihind College of engineering, kuran*

[4]*Assistant Professor of Department of Computer engineering, Jaihind College of engineering, kuran*

***Abstract* —The mediated certificateless encryption scheme without pairing operations for the securely sharing sensitive information over the public clouds. Mediated certificateless public key encryption (mCL-PKE) solves problem of the key escrow in the identity based encryption and certificate revocation problem in public key of cryptography. mCL-PKE scheme does not utilize paring operations. Since most CL-PKC schemes are based on the bilinear pairing which are computationally expensive. The security mediator acts as a policy enforcement point as well supports instantaneous revocation of compromised or malicious users. It is more efficient than the pairing based scheme. By applying mCL-PKE scheme can construct the practical solution to the problem of sharing the sensitive information in the public network.The cloud is employed as a the secure storage as well as a key generation center. In our system, the data owner encrypts the sensitive data using the cloud generated by users' public keys based on its access control policies and uploads the encr ypted data to the cloud. Upon successful authorization, of public cloud partially decrypts the encrypted data for the users.**

Keywords-* *Cloud computing, certificateless cryptography, confidentiality, network access control.

I. INTRODUCTION

Because of the advantages of open distributed storage, associations have been receiving open cloud administrations such information. Be that as it may, for the across the board selection of distributed storage benefits, people in generaldistributed storage model ought to understand the basic issue of information classification.

The system does not know the keys used to encode the information, the secrecy of the information from the system is guaranteed. However a conventional open key cryptosystem requires a trusted Certificate Authority (CA) to issue advanced endorsements that quandary clients to their open keys. Since the CA needs to produce its own particular mark on every client's open key and deal with every client's testament, the general authentication administration is extremely costly and complex. To address such deficiency, Identity-Based Public Key Cryptosystem (IBPKC) was presented, yet it experiences the key escrow issue as the key era server takes in the private keys of all theusers Al-Riyami and Paterson presented another cryptosystem called Certificateless Public Key Cryptography (CL-PKC). At that point proposed the CL-PRE (Certificateless Proxy (Re-Encryption) plot for secure information partaking out in the open system situations.

In the conventional CLPKE scheme, user ' complete use the private key consists of a secret value chosen by the user and the partial private key is generated by the KGC. Unlike the CLPKE scheme, the partial private key is securely given to the SEM, i.e security mediator and the user keeps only a secret value as its own private key in the mCLPKE scheme it is important to see that if one directly applies our basic mCLPKE scheme to the cloud computing and if many users are authorized to the access the same data then the encryption costs of the data owner can become quite high so it expensive to buy.

II. LITERATURE REVIEW

1. An efficient certificateless encryption for secure data sharing in public clouds .

Author: M.Nabeel and X.Ding

exposure. Literature survey is the most important thing in software development process. The existing Attribute-Based Encryption (ABE), which is one effective and promising technique. The technique is used to provide fine-grained access control to data in the Cloud environment. Attribute-Based Encryption is an access control mechanism where a User to encrypt each data item based upon their access control policy. Access to data in the Cloud was provided through Access Control Lists (ACLs), so this was not scalable and only provided coarse -grained access to data 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.

2. Searchable Encryption Revisited.

Author*:* M.Abdalla, M.Bellare, D.Catelano.

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.

3. Certificateless public key cryptography .

Author *: S.S.Al-Riyami* and K.G.paterson

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.

4. Enhancing Cloud Computing Security using AES Algorithm .

Author*:* A.Sachdev and M.Bhansali.

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.

5. Relations among notions of security for public-key encryption schemes

Author: *A .Desa i* D. Pointcheval and P.Rogaway

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.

III. PROPOSED SYSTEM

AES

Rijndael was Proposed the AES algorithm with the larger size and columns**.**AES is based on a design principle known as a Substitution permutation network. It is fast in both software and hardware. AES does not use a Feistel network. AES has a fixed block size of 128 bits and a key size of 128, 192, or 256 bits. AES works on a 4×4 array of bytes, termed as the state .

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

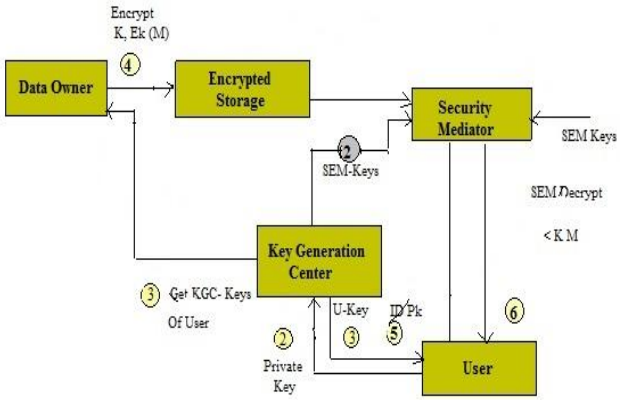

Fig 2. System Architecture

1. Data Owner-Data owner encrypt the sensitive data using public key and upload it on network.
2. User-User encrypt and decrypt the data over a network. After successful authorization, network partially decrypt the encrypted data and user can get the fully decrypted using their private keys.
3. Encrypted storage-Upload the data at encrypted storage that is on a network.
4. Key generation centre-Generated the key for getting the data.
5. Security Mediator

V. ALGORITHM

Algorithm implemented:

1. AES

AES Advance encryption algorithm is used to provide security of the public network because AES is considered as the secure. Encryption and decryption time taken by AES is minimum as compared to the others algorthim . 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 text.
2. Initialize the state array with the block data (plaintext).
3. Add the initial round key to the starting state of the array.
4. Perform nine rounds of the state manipulation.
5. Perform the ten and final round of state manipulation.
6. Copy the final state array out as the encrypted data (ciphertext).

Proposed Key Generation Steps:
1. Select the private key of Size 256 X 2 bits or 64 charac ters.
2. Size of the selected key will be vary from 128 bits to 256 bits or 10,12,14 round.
3. We can choose any character from 0 to 255 ASCII code.
4. Use of 64 * 8 key that means 512 bits in length.
5. Divide 64 bytes into 4 blocks of 16 bytes likes Key_Block1, Key_Block2, Key_Block3, and Key_Block4.
6. Apply XOR operation between Block1 and Block3. Results will store in new Key_Block13.
7. Apply XOR operation between Block2 and Block13. Results will store in new Key_Block213.
8. Apply XOR operation between Key_Block213 and Key_Block4. Results will store in new Key_Block4213.
9. Repeat Step 7, 8, 9 till (random number / 4).
10. end

Steps of proposed Algorithm:
1. Initially select plain text of 16 bytes
2. Initially insert key of the size 16 byte
3. Apply XOR operation between key and plain text block Result will store in Cipher Block1.
4. Use right circular shift with 3 values. Result will store in new Cipher Block2.
5. Apply XOR operation between Cipher block2 and Key block2. Result will store in new Cipher Block3.
6. Apply XOR operation between Cipher Block3 and Key Block4. Result will store in Cipher Block4.
7. Cipher Block4 is the input of the next round as a plane text block.
8. Repeat step 1 to 7 till
9. end.

MATHEMATICAL MODEL

Module 1:- User Key Generated and Encrypted
Let S1 be a set of parameters for generating key and cypher text
S1= {key}
Generating key:- R=((N-NP) S/L)/N=S/L
where, R is Binary data rate, N is Size of key, NP is size of key which carries the parameters, S is Small positive integer and L is size of binary data in key data.
Where,
File_Size = Actual size of key
key_Type = Type of key

COMPARISON RESULT

FOLLOWING FIG.DEMONSTRATES THE TIME NEEDEPERFORMTHE ENCRYPTION OPERATION IN THE MCL-PKE PLAN FOR DISTINCTIVE MESSAGE SIZES.

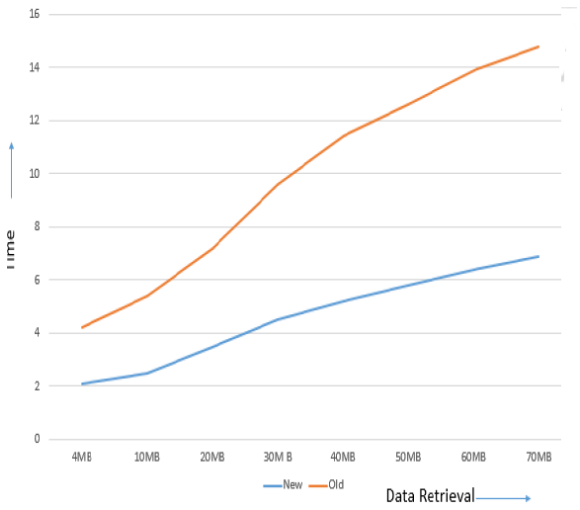

Fig 3: data Decryption

Following figure demonstrates that the exactness in MRSE plan is apparently influenced by the standard deviation of the arbitrary variable.

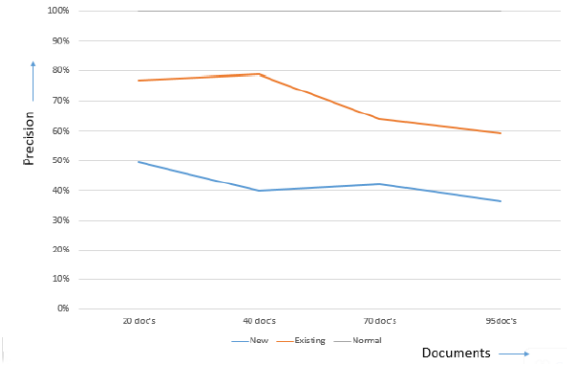

Fig 4: data Retrival

Fig shows that the comparison of Encryption for our schema and the mCl_PRE schema

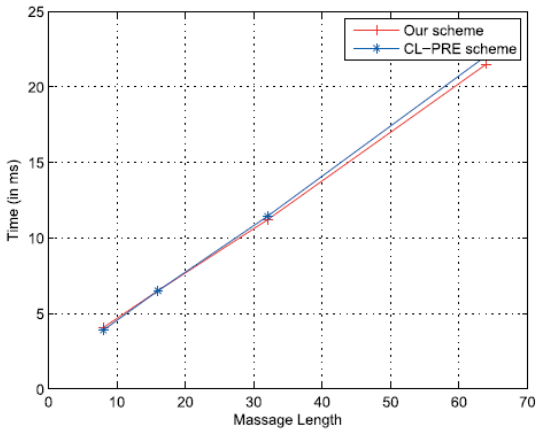

Figure 5: comparison of Encryption

Fig shows that the comparison of Decryption for our schema and the mCl_PRE schema

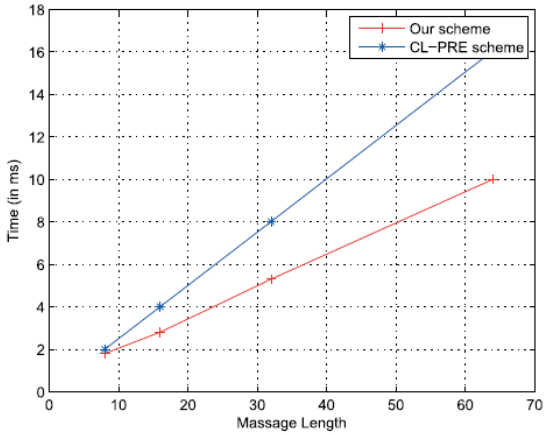

Figure 6: comparison of Decryption

IV. RESULT AND DISCUSSION

1.Result for the text file:

1. The original input file taken by this project is of .txt

Figure : original file before encryption

2.The cipher text file .txt file

Figure : Encrypted File

3.This file is output of encryption and input to decryption. The decrypted output file looks like original file. It is also .txt

Figure: Decrypted File after decryption

Same process for images and videos.

V. CONCLUSION

A conventional open key cryptosystem requires a trusted Certificate Authority (CA) to issue computerized endorsements that quandary clients to their open keys. Since the CA needs to create its own particular mark on every client s open key and deal with every client s testament, the general declaration administration is exceptionally costly and complex. To address such weakness, and to get high security to the cloud information over a system, and to enhance the proficiency of the encryption. We propose an augmentation to our approach. We propose our mCL-PKE plot, the general system based framework, assesses its security and execution. It will be significantly less costlier, less intricate and entirely secure security instrument to manage organize security issues. We proposed an enhanced way to deal with safely share delicate information in our database. Our approach bolsters prompt disavowal and guarantees the secrecy of the information put away in an untrusted database while implementing the get to control

ACKNOWLEDGMENT

Authors want to acknowledge Principal, Head of department and guide of their project for all the support and help rendered. To express profound feeling of appreciation to their regarded guardians for giving the motivation required to the finishing of paper.

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]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] Dan Boneh and Matt Franklin, "Identity-Based Encryption from the Weil Pairing," SIAM Journal on Computing, 32(3):586–615, 2003.