Secure Certificateless Encryption and Auditing Of Data for Multiple Users on Public Cloud

Mr. A.R.Gadekar[1], Dr.M.V.Sarode[2], Dr. V.M.Thakare.[3],
Department of Computer Science & Engineering[1,2,3],SGB Amravati University[1,2,3]
amit.gadekar@sitrc.org[1],sarodemilind1@gmail.com[2],vilthakare@yahoo.co.in[3]

Abstract- Cloud computing introduces a new era in information technology as it can provide various accommodating and innovative IT services in a very quick fashion, where its users can diminish the huge capital investments in their own IT infrastructure using new approach secure certificateless encryption and auditing (SCL-EA) of data on public cloud for multiple users lacking pairing process for sharing securely susceptible information. The system SCL-EA for multiple users work out on to the issues of mediated certificateless public key encryption (mCL-PKE) which was designed for the single user only who is requesting for accessing data having same access control policies but our approach supports the same for multiple user also. Due to this, time taken to generate multiple keys will be reduced and also key cost will be diminish as single key will be used by multiple user in above case. However, the existing mediated certificateless public key encryption schemes are whether critical against partial decryption attacks or inefficient on account of the utilization of upscale operations of pairing. The SCL-EA scheme is advantageous while transmitting the delicate messages between multiple users in public clouds satisfying the same access control policies. The intimacy of the content and keys is maintained regarding the cloud, as cloud is unable to decrypt full information. The idea also contributes an enhancement to the traditional approaches to scale the effectiveness of encryption at the data owner as it provides auditing at data owner side.

Index Terms-Secure certificateless encryption and auditing, Mediated certificateless public key encryption, Identity based encryption formatting.

1. Introduction

The cloud computing is being desperately mentioned to as one of the highly succeeding growth in recent years. The cloud come across with the computing resources and benefits in a pay-as-you-go mode, which is expected to become as appropriate to use similar to known daily routine utilities. As in for gaining the confidence over confidentiality of sensitive data which is kept in public clouds, generally preferred procedure is while uploading data to the cloud that data should be encrypted. There is an assurance about the data confidentiality from the cloud because the keys which are required to decrypt the contents, for that the cloud is unaware. The Certificateless Public Key Cryptography [1] consist of public key schemes searching and like Identity based public key cryptography, CL-PKC is not having inbuilt key escrow feature but the problem with this method is that it is not needed in single-user environment also it is having speed issues. The privacy preserving policy based content sharing in public clouds [2] provides broadcast group key management (BGKM) which efficiently handles joining and leaving of users with guaranty and also guaranty in the security too. However, in many organizations it is necessary to compel fine-grained access control [5] over an information, this fine-grained encryption established access control should be supported by the mechanism of encryption. Another way is to adopt a public key cryptosystem, in consideration of reducing the overhead in administration of keys. To issue digital certificate, there is a requirement of trusted certificate authority (CA) [8] in ethnic public key cryptosystem which binds an individual to their public keys. As the CA has responsibility of generating his own signature on each users public key and administrating individuals certificate, this whole administration process of the certificates is very tangled as well as expensive also. To overwhelmed such draw- backs, technique named Identity-Based Public Key Cryptosystem (IBPKC) [13] was acquaint, again it is having the key escrow problem because the private keys of all the end users is discovered by the key generation server. Then one more scheme was proposed recently named Attribute Based Encryption (ABE) [4] is a scheme in which the information is first divided into the part and accordingly the access control policy applicable to that part of information in encrypted.

Our project is to defeat the disadvantages of such previous schemes and hence proposed a unique secure certificateless encryption and auditing (SCL-EA) of data on public cloud for multiple user, which oppose the operations of pairing. Mostly all of the CL-PKC schemes rely on computationally expensive bi-linear pairings. By using pairing-free approach, this course of action reduces the data processing overhead. Before the user fully decrypt the encrypted content, a partially-trustworthy security mediator first moderately decrypts the encrypted content before the users decrypt, therefore at user side the data processing cost for decryption are diminished. And for multi- ple users requesting the data which is having same access control policies can be accessed, for which the data owner does not need to generate keys each and every time the user requested.

The security mediator is for maintaining those access control policies. This new means of arriving can effectively handle keys and access control policies. Also at owner side auditing of data is done. Suppose after uploading the data on the cloud is changed then the alert message will be generated and given to the owner and in this manner the owner will come to know that his data is not in a consistent form. Users are enforced to take care of number of keys equal to slightly logarithm of bulk of end users which was very hectic in the symmetric key system and opposite to that in our approach, the pair of public/private key is only preserved by an individual user. Later, the revocation of users in symmetric key system needed continues update of private keys which is been provided to all the users in that group, opposite to that in our approach the user does not required to change the private keys means key update is not required. This project will also diminish the data owners overhead by providing an access to all those similar access control policies of content for multiple users, our system also improves the approach in more advantageous manner as on each data item we carry out single encryption only and hence minimizes the overall aloft at the side of data owner.

2. Related Work

Our scrutiny consists of the paper named “Certificateless Public Key Cryptography”[1], com- prise of public key schemes searching that are against of certificates and so far lack in built-in-key escrow feature of identity based public key cryptography (ID-PKC), whereas comprised of the weakness like public key cryptography does not required in single-user circumstances. Also public Key cryptography is having speed problem for encryption and may be susceptible to impersonation even though user private key are not ready for the use. In “Privacy Preserving Policy-Based content sharing in Public Clouds”[2] possess formalized a modern scheme of key management named broadcast group key management (BGKM) and also provide secure creation of system for BGKM scheme named ACV-BGKM. Efficiently handles the revoking of user immediately onto the cloud as they are revoked with guaranteed security. Also the users can conveniently acquire decryption keys and managing of huge number of users is done efficiently by the data owner. It lapse in comprising of adding traitor tracing and also the capabilities with respect to privacy preserving queries. In “Searchable encryption revisited: consistency properties, relation to anonymous identity based encryption and extensions”[3], which incorporate with the stronger consistency property for public key encryption with keyword search and trans- forms anonymous IBE (Identity Based Encryption) schemes to a secure PEKS scheme with consistency in it. Its drawback is anonymous IBE in the standard models and HIBE anonymous at level 2 or greater (even in random oracle model).

The “Cipher text policy attribute based encryption: an expression and provably secure realization” [4], comprise of accomplishing cipher text policy attribute encryption (CP-ABE) systems from general set of access structures in standard model under concrete and non-interactive assumptions; provides performance tradeoffs to achieve provable security. And receiver ambiguity is abandoned as the access structure of the cipher text declared the same where it lacks. The “Fine grained control of security capabilities”[5], consist of certificate revocation and fine-grained control over security capabilities. Revocation is fast when its certificate is revoked the client can no longer decrypt or sign messages. With binding signature semantics, there is no need to validate the signers certificate as part of signature verification. Revocation technique is transparent to the peers since it uses standard RSA signals and encryption formats. And shortcomings of this is, the security mediator (SEM) architecture which is implemented for experimentation purpose this is appropriate for only small to medium sized organization and is clearly not relevant for educational campus like environments or for the global internet. The “Conjunctive, subset and range queries on encrypted data”[6], which explored a general framework for analyzing security of searching on encrypted data systems and also then constructed systems for comparisons and subset queries as well as conjunctive versions of these predicate. And problems where it lacks are the best non-conjunctive comparison system they currently have, requires is cipher texts of size O (n) where n is the domain size. In principle it should be possible to improve this to log n, but this is wide open issue currently requiring creative ideas. Similarly in non-conjunctive sub-queries they have required cipher text of size O(n) which can be improved to O(log n). The “Oblivious transfer with hidden access control policies”[7], which provide the set of efficient protocols and thereby it is possible to build an access control system for a database with the maximal possible privacy for all involved parties and it has some shortcomings like keys to decrypt some media such as movies or a particular DNA-sequence of many people, then these protocol could be used in practice, such a system will result to less efficient protocol. The next survey consisting of “Security mediated certificateless cryptography”[8], which provide security mediated certificateless cryptography. It provides a generic construction with concrete encryption scheme. Supports distributed security mediator (SEMs). And it has some problems belonging to its basic form that it fails to reach Giraults level 3. This means that although there is less trust placed in authority than ID-based schemes, there is more trust placed in KGC than in traditional public key schemes.

The “Controlling access to an oblivious database using stateful anonymous credentials”[9], which involves efficient and flexible system that allows content providers to control access to their data, while simultaneously maintaining the privacy provided by the oblivious and anonymous protocols. Shortcoming of this paper is the flexibility. In “Attribute based encryption for fine grained access control of en-cryption data”[10], which consist of relevance of their construction to share the information of audit-log. Backing an approval of private keys which includes hierarchical identity-based encryption (HIBE), implemented fined grained access control. Current construction does not hide the set of attributes under which the data is encrypted. In this the open issue is regarding hiding the set of attributes. The next survey involves “Controlling access to published data using cryptography”[11], which is the method in which data sharing is done in a systematic manner also the system includes high-level access control policies, a powerful logical model for securing a document tree and encryption techniques to built an XML document which enforces policies. Framework can satisfy needs of emerging communities of users who want to share data in distributed environment but are tethered by trust and privacy constraints continued work is focused on proving formal security claims about data instances as well as improved query processing and update techniques are also lagging. The “Relations among notion of security for public key encryption schemes”[12], involves the non compliance and a refinement to the definition of the alertness among the plaintext. “Fuzzy Identity-Based Encryption”[13], presents two constructions of fuzzy IBE schemes, construction can be viewed as an Identity-Based encryption of a message under several attributes that compose an identity. Their IBE schemes are both error-tolerant and secure against an attack. It does not use random oracles method. To create a fuzzy IBE scheme where attributes come from multiple authorities is not present in it. An open issue with this is to build other fuzzy IBE schemes that use different distance metric between identities headings should be typeset in boldface with the words.

3. System Architecture

In the proposed system the shortcoming of the previous approaches is overcome by our novel Secure Certificateless Encryption and Auditing (SCL-EA) of data on public cloud for multiple users which is against of pairing operations. Our system provides multiple users access for the data which is having same access control policies, so the data owners work load is reduced because of our system. The data owner does not need to generate the separate key for that data which is having same access control policy. The system consists of three entities: data owner, users and cloud which is mentioned in fig. 1.

The data owner is having the sensitive for full decryption process. The user will decrypt fully by using their private keys.

There are three important services of cloud, an encrypted content storage, a security mediator which behaves like security advocate for each data request and a key generating server (KGC) which provides pair of public/private key for each user. The un-trusted cloud is deployed by the functionality of key management and also as our SCL-EA scheme is against of key escrow problem and hence users full private key is unable to get by the key generation server. Also auditing of data is done at owner side.

4. Methodology

The secure certificateless encryption and auditing scheme is 9-tuple SCL-EA which is described as:

- **Set Up**

For Set-Up the input is a security parameter k and returns system parameters para and a secret master key M_k. Assuming that para are publicly ready for use to each and every user. This security parameter k is used to derive values m and n where both are prime values such that m| n-1. Following steps are executed then.

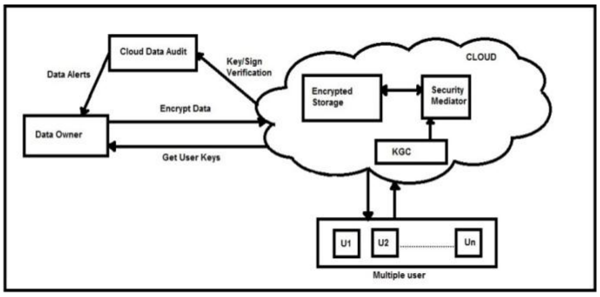

Fig. 1. System Architecture

1) Select a generator g of Z_m^* with order n.
2) Choose xϵZ_n^* uniformly at random and execute y = g x .
3) Use cryptographic hash functions.

H_1:$\{0,1\}* \times Z_m^* \rightarrow Z_n^*$,
H_2:$\{0,1\}* \times Z_m^* \times Z_m^* \rightarrow Z_n^*$
H_3:$\{0,1\}* \rightarrow Z_n^*$
H_4: $Z_m^* \rightarrow \{0,1\}^{l+k0}$
H_5: $Z_m^* \rightarrow \{0,1\}^{l+k0}$ and
H_6: $Z_m^* \times \{0,1\}^{l+k0} \times Z_m^* \times \{0,1\}^{l+k0} \rightarrow Z_n^*$,
where l, k0 are the bit-length of a plaintext and a random bit string, respectively. The system parameters para are (m, n, l, k0, g, y, H_1, H_2, H_3,H_4, H_5, H_6). The master key of KGC is x. The plaintext space is M = $\{0,1\}^l$ and the ciphertext space is C = $Z_m^* \times \{0,1\}^{l+k0} \times Z_n^*$

- **Set-PrivateKey:**

For Set-PrivateKey inputs are para and ID whereas user secret value S_KID is the output. The algorithm executed by all the users. The entity E chooses $z_E \epsilon Z_n^*$ uniformly at random as the private key of E.

- **Set-PublicKey:**

For Set-PublicKey inputs are para and a user's secret value S_KID and the output is user's public key P_KID. The entity E computes $u_E = g^{ze}$.

- **SEM_KeyExtract:**

In KGC, every user enrolls its own individuality and public key. Then KGC checks for the verification by comparing private key with the public key, the input taken by the KGC is user identity ID, secret master key M k and para and produces the output of SEM_Key matching to the user identity which is required during decryption time by the security mediator. KGC selects s_0, $s_1 \epsilon Z_n^*$ and evaluate $w_0 = g^{s_0}$, $w_1 = g^{s_1}$, $d_0 = s_0 + xH_1(ID_E , w_0)$, $d_1 = s_1 + xH_2(ID_E , w_0, w_1)$. KGC sets d_0 as the SEM-key for E. After E certifies the knowledge of the secret value z_E as if $u_E = g^{ze}$, KGC sets as the E's public key.

(uE , $w0$, *datawhichheuploadsontothepubliccloud inanencryptedformatesoastosharehisinformationtothea uthen)*

- **Encryption:**

For encryption inputs are user's identity ID, para, a user's public key P_K ID and a message M_{sg} and produces the ciphertext C_T ID as ma successful result or a special symbol ⊥ meaning failure in encryption. This algorithm can be run by any entry.

- **SEM_Decryption:**

For SEM_Decryption the inputs are para, SEM_key and a ciphertext $C_T ID$ and then produces the successful output of partial decrypted message $C_T * ID$ which will be fully decrypted at user side or in case of failure produces a special symbol ⊥. This algorithm is run by only the SEM using SEM_key.

- **USER Decryption:**

In this input taken are para, a user's private key $S_k ID$, the output of SEM ($C_T * ID$) which is partially decrypted message and then produces the final output M_{sg} which is fully decrypted or in case of decryption failure produces a special symbol ⊥. The user can run this algorithm by using user's private key and the message which is partially decrypted by the SEM.

- **Data-Auditing:**

Verifying the data after uploading on to the cloud if done changes in that data then alert messages are generated for data owner

5. Mathematical Model

We used the set theory along with the functions and relationship for mathematical model. Our problem definition can be framed in the form of a set theory. Let S be a system, consisting of following:

1) ERP (user)
2) Cloud Middleware
3) Encryption
4) Uploading data
5) Downloading data
6) Shared authority

The system be described by S

S= {D, EU, CM, EN, SA, TP}

Where, S: is a system.

D: Set of training dataset. EU: ERP (user).

CM: Cloud Middleware. EN: Encryption.

SA: Upload Data. TP: Download Data.

Activity Relations

D $=\{d_1, d_2, \cdots\cdots, d_n\}$ //D is a given dataset.

E=$\{e_1, e_2, \cdots\cdots, e_n\}$ //E is associated to ERP (user).

C $=\{c1, c2, \cdots\cdots, cn\}$ //C is cloud middleware.

F $=\{f_1, f_2, \cdots\cdots, f_n\}$ //F is associated for encryption.

S $=\{s_1, s_2, \cdots\cdots, s_n\}$ //S is shared authority.

T $=\{t_1, t_2, \cdots\cdots, t_n\}$ //T is downloaded data.

Y={EU, CM, EN, SA, TP} //Y is a set of technique use for privacy preserving authentication protocol in cloud computing.

1) Let F_{n1} be the function in which ERP (user) is registered onto cloud middle- ware.
   $F_{n1}(\text{EU}):F_{n1}\{\text{CM}\}\rightarrow O_1$
   For Example:$F_{n1}(e_1):F_{n1}\{C1\}$ ϵ CM
2) Let F_{n2} be the function in which ERP (user) after registration will encrypt his data.
   $F_{n2}(D):F_{n2}\{\text{EN}\}\rightarrow O_2$
   For Example:$F_{n2}(d_2):F_{n2}\{f_1\}$ ϵ EN
3) Let F_{n2} be the function in which ERP (user) after registration will encrypt his data.
   $F_{n2}(D):F_{n2}\{\text{EN}\}\rightarrow O_2$
   For Example:$F_{n2}(d_2):F_{n2}\{f_1\}$ ϵ EN
4) Let F_{n3} be the function in which encrypted data is uploaded on cloud.
   $F_{n3}(EN):F_{n3}\{\text{SA}\}\rightarrow O_3$
   For Example:$F_{n3}(f_3):F_{n3}\{f_3\}$ ϵ SA
5) Let F_{n4} be the function in which uploaded data can be downloaded.
   $F_{n4}(SA):F_{n4}\{\text{TP}\}\rightarrow O_4$
   For Example:$F_{n4}(s_3):F_{n4}\{t_4\}$ ϵ TP

6. Conclusion

The system Secure certificateless encryption and auditing (SCL-EA) of data on public cloud for multiple users, is totally against of pairing procedures. This SCL-EA scheme solves the issues related to mCL-PKE scheme which was suitable for accessing of the data having same access control policies but for single user only whereas our system supports the same for multiple user using single key. The scheme provides confidentiality of the data which is uploaded onto cloud as it provides auditing at owner side. The expected result is to demonstrate the capability and performance of basic SCL-EA scheme and also to show the public cloud with progressive approach.

Acknowledgment

I would like to express my deepest appreciation to all those who provided me the possibility to complete this paper. A special gratitude to my guide, Prof. (Dr.) M. V. Sarode, whose contribution in stimulating suggestions and encouragement, helped me to coordinate my research paper in effective way.

REFERENCES

[1] S. Al-Riyami and K. Paterson, *Certificateless public key cryp- tography,* in Proc. ASIACRYPT 2003, C.-S. Laih, Ed. Berlin, Germany:Springer, LNCS 2894, pp. 452473.

[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] M.Abdalla et al.,*Searchable encryption revisited: Consistency Properties , relation to anonymousibe, and extensions,* J. Cryp- tol.,vol. 21, no. 3, pp. 350391, Mar. 2008.

[4] J.Bethencourt, A. Sahai, and B. Waters, *Ciphertext- policy Attribute -based encryption,* in Proc. 2007 IEEE Symp.SP,Taormina, Italy, pp. 321334.

[5] 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.

[6] D. Boneh and B. Waters,*Conjunctive, subset, and range queries on encrypted data,* in Proc. 4th TCC, Amsterdam,The Nether- lands, 2007, pp. 535554.

[7] J. Camenisch, M. Dubovitskaya, and G. Neven, *Oblivious transfer with access control,* in Proc. 16th ACM Conf. CCS, New York,NY, USA, 2009, pp. 131140.

[8] 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. 508524.

[9] 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, 2009, pp. 501520.

[10] V. Goyal, O. Pandey, A. Sahai, and B. Waters, *Attribute- based encryption for fine-grained access control of encrypted data,*in Proc. 13th ACM Conf. CCS, New York, NY, USA, 2006,pp. 8998.

[11] G. Miklau and D. Suciu,*Controlling access to published data using cryptography,"* in Proc. 29th Int. Conf. VLDB, Berlin,Germany, 2003, pp. 898909.

[12] M. Bellare, A. Desai, D. Pointcheval, and P. Rog- away,*Relations among notions of security for public-key encryp- tion schemes,*in Proc. Crypto 98, H. Krawczyk Ed. Springer- Verlag, LNCS1462.

[13] A. Sahai and B. Waters,*Fuzzy identity-based encryption,* LNCS3494 in Proc. EUROCRYPT, Aarhus, Denmark, 2005, pp. 457473.