ISSN: 2277-9655
Impact Factor: 3.785

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

SECURE SHARING OF DATA IN CLOUD USING ATTRIBUTE BASED PROXY RE-ENCRYPTION

U.Aarthi*, Mr. N. Praveen

* PG Scholar, Department of Computer Science and Engineering,R.V.S Educational Trust's Group Of Institutions, Dindigul, Tamil Nadu

Assistant Professor, Department of Computer Science and Engineering, R.V.S Educational Trust's Group Of Institutions, Dindigul, Tamil Nadu

DOI: 10.5281/zenodo.51466

ABSTRACT

People rely more on networks where security is the major issue in cloud storage. The growth of electronic personal data leads to a trend that data owners prefer to remotely outsource data to cloud for high quality retrieval and storage without worrying burden of local data management and maintenance. However secure sharing of outsourced data is formidable task, which may easily incur leakage of sensitive personal information. The objective of this project is to provide security in Cloud storage by using Attribute based proxy re-encryption which can be applicable to many real world applications.

KEYWORDS: Searchable attribute-based proxy re-encryption, keyword update, encrypted data sharing.

INTRODUCTION

Cloud means the practice of using a network of remote servers hosted on the Internet to store, manage, and process data, rather than a local server or a personal computer. Data security is the major problem in cloud computing. For security, different attribute based encryption schemes are used for encryption before outsourcing data to cloud server. Bystepping into the era of big data, Internet users usually choose to upload their personal data remote cloud servers such that they can reduce the cost of local data to keep in good condition and succeed. In addition to individuals, many industries and research institutions also follow the trend to remotely store commercial and scientific data to clouds to enjoy high-speed data process and retrieval service. Cloud storage service, accordingly, reveals its infinite practical and commercial potential. However, it meanwhile unavoidably a meeting, especially one that happens by chance with many impredicible security and privacy challenges.

Motivation: We start with Attribute-Based Encryption(ABE) with a significant reason that it provides fine-grained expressiveness in data share and search. After storing data to a cloud server, the data owner usually needs two necessary operations: one is *data analysing*, and the other is *data sharing*.

In main action in traditional ABE technology to encrypt data that guarantees the confidentiality of the data, but within limits data sharing and ing. Suppose there is a set of genome encryption, *(Enc(g*1, *P*1*), ..., Enc(gn, Pn),)*, which are donated by anonymous volunteers for medical research purpose, where a data *gi* is encrypted under a policy *Pi* such that only a group of researchers matching the policy can acquire the data. The secret texts are stored in a remote server. To naively search a specific encrypted genomic data, a researcher, say Aniee, has to download all the secret texts related to her decryption policy *PA* from the server, and next to decrypt them to fulfill the search task locally. When sharing one of her accessible data with her colleagues, Aniee has to download the encrypted data, decrypt and further re-encrypt it under the decryption policy of the colleagues. Another interesting behavior, which might be done by Aniee, is the keyword update for the shared encrypted data. Consider an encrypted genomic data is with a keyword tag ("Materials at Lab A"). After its sharing to scientists in Lab B, Aniee may choose to change its tag as ("Shared to Lab B"). Since traditional ABE cannot support keyword update, Aniee has to modify the tags for all shared secrettexts on her own due to protecting the privacy of the keywords. However, the above naïve approaches do not scale well.

Because they bring additional decryption/encryption burden to Aniee who is required to be on-line all the time. The cost for the data owner will become more cumbersome,

when the number of searching and sharing is increasing. Besides, the size of download data yields a challenge for local data maintenance that definitely downgrades the advantage of remote data storage.

Alternatively, one may allow a (remote) third party to fulfill data search task, the re-encryption of data and keyword update on behalf of Aniee. Search keyword (i.e. what Aniee wants to search) and given the secret key of Aniee (i.e. knowing the underlying data). The escape of the above information seriously disgraces the privacy of anonymous donar because the chromosomal data may contain sensitive information, such as illness.

1.DIFFERENT ENCRPTION SCHEMES

Public key Encryption (PE): Public key Encryption is any system of encryption where in cryptographic keys are paired, such that an encryption performed with one key can be decrypted only by the other member of the pair, and possession of one key does not enable the practical computation of the other. The public key may be disseminated widely, while the other the private key is known only to the owner. Using the public key, any person can encrypt a message for the owner and leave it on a public server or transmit it on a public network, and such message can be decrypted only by the owner using the owner's private key.

2.Identity Based Encryption (IDE): It is an important primitive of ID-based cryptography. As such it is a type of public-key encryption in which the public key of a user is some unique information about the identity of the user (e.g. a user's email address).IDE[7] encryption scheme is a four steps scheme where the algorithms are,(1) Setup.(2) Private key Generation (3) Encryption (4) Decryption .In fuzzylogic identity based encryption view identities as a set of attributes. So in this scheme the fault problems related to identities in IBE is solved. Two sincere application of fuzzylogic IBE are(1) Identity based encryption system that uses software identities.(e.g. a user's email address)(2) It is used in AB encryption.

3. Attribute Based Encryption (ABE): Saghai and Wheters [8] first introduced the attribute based encryption (ABE) for enforced access control [5] through public key cryptography. The main aspects are to provide ability to easily changed, reliable and fine grained access control and safe. In ABE scheme both the user secret key and the secret text are associated with a set of attributes. Suppose the Attribute sets are Computer Science, Male and inner node consists of AND and OR gates and leaves consists of different attributes. Attribute sets that satisfy the tree can reconstruct the secret message and access it. In classic model, this can be targeted only when user and server are in a trusted domain. So different alternatives of AB Encryption are introduced.

4. Key Policy Attribute Based Encryption (KP-ABE): To enable more general access control, V. Goeyal, O. Panidey, A. Saghai, and B. Waters [8] proposed a key- policy attribute-based encryption (KP-ABE) scheme. It is the modified form of classical Model of ABE. . Attribute-based encryption (ABE) is a new cryptographic primitive which provides a promising tool for addressing the problem of secure and fine-grained data sharing and decentralized access control. Key-policy attribute-based encryption (KP-ABE) is an important type of ABE, which enables senders to encrypt messages under a set of attributes and private keys are associated with access structures that specify which ciphertexts the key holder will be allowed to decrypt. In most existing KP-ABE scheme, the secret text size grows linearly with the number of attributes embedded in ciphertext. In this paper, we propose a new KP-ABE construction with constant secret text size. In KP-ABE scheme, attribute policies are associated with keys and data is associated with attributes. In KP-ABE,a set of attributes is associated with secret text and the users Decryption Key is associated words uttered in a single tone access tree structure [5]. When the attributes associated with the secret text satisfy the access tree structure, then the user can decrypt the secret text. Limitations of KP-ABE are Encryptor cannot decide who can decrypt the encrypted data, it is not suitable for certain applications such as sophisticated broadcast encryption and it provide fine grained access but has no longer with flexibility and scalability.

5. Secret text Policy Attribute Based Encryption(SP-ABE): Saghai et al.[2] introduced the concept of another modified form of ABE called SP-ABE[2][4][1] that is Secret- text Policy Attribute Based Encryption. In SP-ABE scheme, attribute policies are associated with data and symbols are associated with keys and only those keys that the associated symbols to satisfy the power control associated with the data are able to decrypt the data. In a SP-ABE

scheme, a secret text is associated with a words uttered in single tone tree structure [4] National Journal of Computer Applications users decryption key is associated with set of symbols. Limitations of this scheme are: it cannot fulfill the enterprise requirements of access control which require considerable ability to be easily modified.

6. Tree Structure Attribute-Based Encryption (TABE): This scheme (TABE) proposed by Wheang et al [10].It is a combination of Tree Structure Identity Base Encryption and SP-ABE. It is access control, full assigned responsibility and high accomplishment. The TABE scheme consists of many attribute consist of many users. AB Encryption uses disjunctive normal form tactics. The same attribute may be determined by multiple domain according to specific tactics, which is most dangerous to implement in practice. TABE [10] model consists of a Root Expert (RE) and multiple domains. One domain consist of number of domain expert and number of users related to end users. It is main applicable to the environment of enterprise the sharing data in cloud computing. This technique has issues with multiple values assignments and practical implementation is occurring the fault because same attribute may be administered by different domain expert.

7.Hierarchical Attribute Set Based Encryption (HASBE):HASBE scheme is proposed and implemented by Zhiaguon Wheang etal [10].This scheme extended the ASBE scheme to handle the characteristics of a ranked order structure of the system. In this model trusted authorization is responsible for managing top level domain power. Each user in this system is assigned a key structure This scheme provide scalable, flexible and fine grained access control in cloud computing. Efficient user revocation can be done in this scheme due to attribute assigned multiple values.
8. Multi-Authority Attribute Base Encryption(MA-ABE): This scheme consists of many attribute authorities and many users.Attributes based key generation algorithm will run the authority and result will send to the user. In a multiple authority ABE scheme,multiple attribute-authorities overseeing different sets of attributes and main problem corresponding decryption keys to users, and encryptors can require that a user got keys for appropriate attributes from each authority before decrypting a message. Chase gave a multi authority ABE scheme which supports many different authorities operating synchronously, each handling out secret keys for a different set of attributes.

Our system has better efficiency regarding to keyword search and decryption phases when compared to existing systems which only support either data sharing or keyword search in the context of ABE. To achieve fine grained and scalable data access control for medical records stored in semi trusted servers, we leverage attribute based encryption (ABE) techniques to encrypt each patient's medical record file. In this paper, we describe a new approach which enables secure storage and controlled sharing of patient's health data. We explore key policy attribute based encryption and multi-authority attribute based encryption to enforce patient access control policy such that everyone can download the data ,but only authorize user can view the medical records. This project also supports multiple owner scenarios and divides the users in the system into multiple security domains that greatly reduce the key management complexity for owners and users. A high degree of patient privacy is guaranteed by exploiting multi-authority AB Encryption. In this paper we presents the detail design of modules and implementation Packages of the proposed framework. Our first system is proven selectively secure under a assumption that we call the decisional Parallel Bilinear Diffie-Hellman Exponent (PBDHE) assumption which can be viewed as a generalization of the BDHE assumption. Our next two constructions provide performance tradeoffs to achieve provable security respectively under the

EXISTING SYSTEM

Public Key Encryption With Keyword (PEKS):
Constructing a PEKS is related to Identity Based Encryption (IBE), though PEKS seems to be harder to construct. We showed that PEKS implies Identity Based Encryption, currently an open problem. Our constructions for PEKS are based on recent IBE constructions. We are able to prove security by exploiting extra properties of these schemes has lot of struggles in cloud.

Key-Policy Attribute-Based Encryption-(KP-ABE):
The key-policy attribute-based encryption (KP-ABE) was first introduced in 2006 by Goeyaln et al. In this cryptography system, secret text are labelled with sets of attributes. Private keys, on the other hand, are associated with access form .A private key can only decrypt a secret text whose symbol set is authorized set of the private key's access structure. KP-ABE is a cryptography system built upon bilinear map and Linear Secret Giving Schemes has

lot of data leakage While going for cloud computing storage, the data owner and cloud servers are in two different domains. On one hand, cloud servers are not entitled to access the contract out data content for data secrecy;on the other hand, the full resources are not physically under the full control of data owner Storing personal records on the cloud server leads to need of Encryption mechanism to protect the record, before outsourcing to the cloud. To deal with the potential risks of privacy exposure, instead of letting the service providers encrypt data and decrypt.Those techniques has leakage of data many disadvantages

PROPOSED SYSTEM

Proxy Re-Encrption:

The proxy encryption schemes are proposed by Mambo and Okamotoes and Blazene et al. Proxy re-encryption is a cryptographic primitive which translates secret texts from one encryption key and decryption key normally main purpose for It can be used to forward encrypted messages without having to expose the clear texts to the potential users. So new concept proxy re-encryption. The re-encryption protocol should be key independent to avoid compromising the private keys of the sender and the recipient. use proxy re-encryption , The primary advantage of this PRE scheme is that they are unidirectional (i.e., Aniee can delegate to John without John having to delegate to her) and do not require delegators to reveal their entire secret key to anyone.

Attribute Proxy Re-Encryption:

The concept of attribute based PRE was introduced by Saghai and Wheaters[7] . In attribute based proxy re-encryption scheme, a semi trusted proxy with some additional information can transform a secret text under a set of attributes into a new secret text under a set of attributes into a new secret text under another set of attributes on the same message. This encryption scheme, allows fine-grained access control on encrypted data. Attribute based encryption is a generalization of IBE. The data provider can express how he wants to share data in the encryption algorithm itself. Goeyaln et al.Introduced two variants of ABE namely CP-ABE and key policy attribute based encryption.

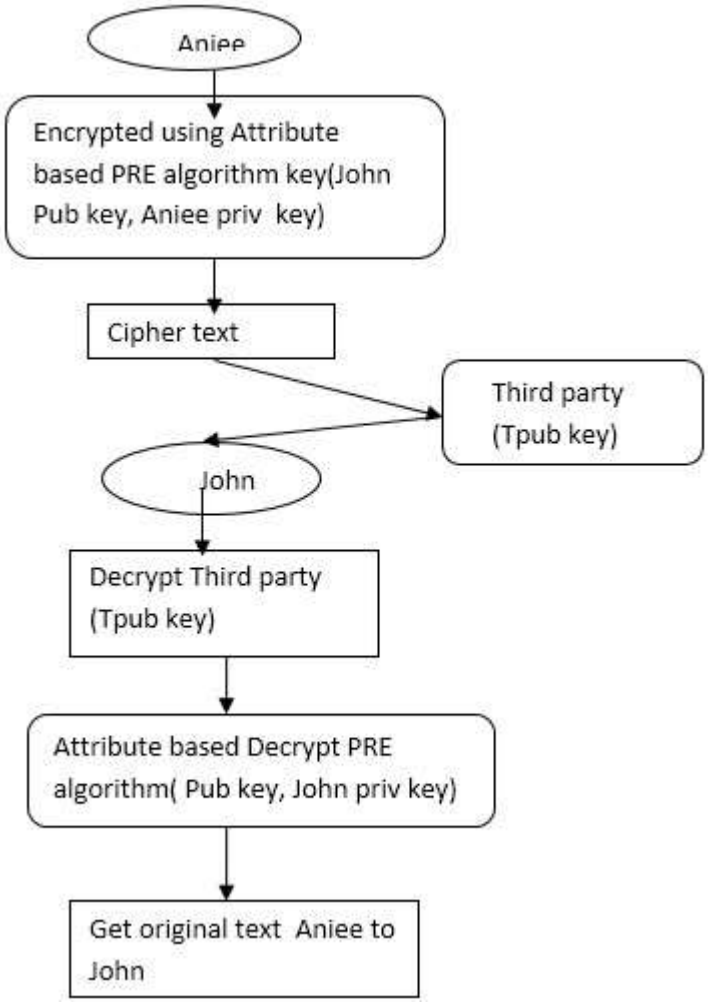
In a CP-ABE scheme, a user's private key is associated with a set of attributes and an encrypted secret text will specify an access policy over attributes. In KP-ABE scheme, each secret text is labeled by the encrypt or with a set of descriptive attributes. Each private key is associated with an access structure that specifies which type of secrettexts the key can decrypt .An important aspect of KP-PRE scheme deals with secure forensic analysis .In ABE technique, the data is stored on the storage server in an encrypted form while different users are still allowed to decrypt different pieces of data as per security tactics. This effectively remove the need to rely on the storage server for preventing unauthorized data access. Attribute Based PRE number of works used AB-Encryption to realize fine-grained access control for contract out data ,it is a semi trusted proxy with some extra information can transform a secret text under a set of attributes into a new secret text under a set of attributes into a new secret text under another set of attributes on the same message. This encryption scheme, allows fine-grained access control on encrypted data. In order to understand clearly about entire process personal health record as an application has developed

Our contributions are described as follows.We for the first time, introduce a novel and practical notion, searchable ABPRE. Our notion guarantees that the keyword search ability of a secrettext can be remained after the sharing of the secrettext. It is worth mentioning that all existing public key systems with keyword search fail to guarantee this property.

We design a concrete searchable Key-Policy (KP) ABPRE system satisfying the above notion. We also prove the scheme chosen secrettext secure in the Random Oracle Model (ROM). The scheme is the first of its type supporting the privacy of keyword search but also encrypted data sharing. As of independent interest, our protocol supports keyword update so that a secret text's keyword can be further updated before the secret text is shared with others. This property brings a convenience to data owner (who can gain access to the data) in the sense that the secret text keyword can be freely modified based on data share record.

ISSN: 2277-9655
Impact Factor: 3.785

Dataflow Diagram For Attribute Based Proxy Re-Encryption:



Attribute Based Proxy Re-Encryption Algorithm Step:

Proxy Re-Encryption Scheme

The re-encryption definitions and to introduce the concept of key privacy. We begin by specifying the input/output behave or of a proxy re-encryption scheme. For simplicity, we will only consider a definition for unidirectional, single-hop PREs. By single-hop, we mean that only original secrettexts (and not re-encrypted secrettexts) can be re-encrypted.

Proxy Re-Encryption Scheme is a tuple of algorithms = (Setup; KeyGen; ReKeyGen; Enc; ReEnc; Dec) for message space M:

Setup(1k)→PP. On input security parameter 1k, the setup algorithm outputs the public parameters PP.

KeyGen(PP) →(pk; sk). On input public parameters, the key generation algorithm KeyGen outputs a public key pk and a secret key sk.

ReKeyGen(PP; ski; pkj) → rki→j.Given a secret key ski and a public key pkj , where i ≠ j, this algorithm outputs a unidirectional re-encryption key rki→j . The restriction that i ≠ j is provided as re-encrypting a message to the original to recipient.

Enc(PP; pki;m) →Ci. On input a public key pki and a message m € M, the encryption algorithm outputs an original secrettext Ci.

A. System Definition

Definition 1*:* A Searchable Attribute-Based Proxy Re-Encryption with Keyword Update (S-ABPRE-KU) scheme consists of the following algorithms:

1) *(mpk, msk) ← Setup(1λ,U):* on input a security parameter λ and a universe of description *U*, output a master public key *mpk* and a master secret key *msk*. We will omit *mpk* in the expression of the following algorithms.

2) *skμ ← KeyGen(msk,μ):* on input *msk*, and a description $\mu \in \{0, 1\}*$, output a secret key *skμ*.

3) *CT ← Enc(m, v,KW):* on input a message $m \in \{0, 1\}\lambda$, a description $v \in \{0, 1\}*$ for the message and a keyword *KW*, output an original secrettext *CT* which can be further converted.

4) *τKW ← Trapdoor(msk, skμ,KW):* on input *msk*, *skμ* and *KW*, output a trapdoor token *τKW*, which is used to search encrypted data associated with *KW*.

5) 1/0← *Test (CT, τKW):* on input a secrettext *CT* under a keyword *KW_*, and a trapdoor token *τKW*, output 1 if *KW_* = *KW*, and 0 otherwise.

6) *rk ← RKGen(skμ, v,KW):* on input a *skμ*, a new description *v* and a new keyword *KW*, output a re-encryption key *rk*, where *μ* does not satisfy *v*. The *rk* is used to convert an original secrettext under *v_* and *KW_* to a re-encrypted secrettext of the same message under *v* and *KW*, where *μ* satisfies *v_*.

7) *CT/ ⊥← ReEnc(CT, rk):* on input an original secrettext *CT*, and a re-encryption key *rk*, output a re-encrypted secrettext *CT* or ⊥.

8) *m/ ⊥← Dec(skμ,CT):* on input *skμ*, and a secrettext *CT* under description *v*, output a message *m* if *μ* satisfies *v* or ⊥.

CONCLUSION AND FUTURE WORK

Thus a novel Attribute based proxy re-encryption algorithm is proposed for sharing of data and records in cloud storage. Instead of considering partially trustworthy cloud servers.User have complete control of their own privacy through encrypting their files to allow fine-grained access and this providing the data secure concept.This algorithm addresses the unique challenges brought by multiple owners and users, which greatly reduce the complexity of key management. It utilizes ABPRE to encrypt the data, so that data can allow access not only by personal users, but also various users from public domains with different professional roles, qualifications and affiliations. Furthermore, this project can be enhanced to various real world problems to provide better security in cloud on user demand. This encryption scheme, allows fine-grained access control on encrypted data. In order to understand clearly about entire process personal health record and other as an application has developed in future

REFERENCES

[1] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved proxyre-encryption schemes with applications to secure distributed storage,"*ACM Trans. Inf. Syst. Secur.*, vol. 9, no. 1, pp. 1–30, 2006.

[2] M. Bellare, A. Boldyreva, and A. O'Neill, "Deterministic and efficiently searchable encryption," in *Proc. 27th Annu. Int. Conf. Adv. Cryptol. (CRYPTO)*, vol. 4622. Santa Barbara, CA,

[3] S. Benabbas, R. Gennaro, and Y. Vahlis, "Verifiable delegation ofcomputation over large datasets," in *Proc. 31st Annu. Conf. Adv. Cryptol. (CRYPTO)*, vol. 6841. Santa Barbara, CA,

[4] M. Blaze, G. Bleumer, and M. Strauss, "Divertible protocols and atomic proxy cryptography," in *Advances in Cryptology*. Berlin, Germany: Springer-Verlag, 1998, pp. 127–144.

[5] D. Boneh, X. Boyen, and E.-J. Goh, "Hierarchical identity based encryption with constant size secrettext," in *Advances in Cryptology*

[6] D. Boneh and B. Waters, "Conjunctive, subset, and range queries on encrypted data," in *Proc. 4th Theory Cryptogr. Conf. (TCC)*, vol. 4392.
[7] Shagai and wheter ,R.Donald Security key search &update and PRE.
[8] R. Canetti and S. Hohenberger, "Chosen-secrettext secure proxy re-encryption," in *Process*
[9] N. Chandran, M. Chase, and TABE V. Vaikuntanathan, "Functional re-encryption and collusion-resistant obfuscation," in *Theory of Cryptography* (Lecture Notes in Computer Science), vol. 7194, R. Cramer, Ed. Berlin, Germany: Springer-Verlag, 2012, pp. 404–421.
[10] M. Chase and S. Kamara, "TABE Structured encryption and controlled disclosure," in *Proc. 16th Int. Conf. Theory Appl. Cryptol. Inf. Secur., Adv. Cryptol. (ASIACRYPT)*, vol. 6477. Singapore, Dec. 2010,pp. shagai and wheters proof of theory sharable data on AB encryption techniques.
[11] L. Cheung and C. Newport, "Provably secure secrettext policy ABE," in *Proc. 14th ACM Conf. Comput. Commun. Secur.*, 2007, pp. 456–465.
[12] R. Cramer and V. Shoup, "Design and analysis of practical public-key encryption schemes secure against adaptive chosen secrettext attack," *SIAM J. Comput.*, vol. 33, no. 1, pp. 167–226, Jan. 2004.
[13] L. Ducas, "Anonymity from asymmetry: New constructions for anonymous HIBE," in *Topics in Cryptology* (Lecture Notes in Computer Science), vol. 5985. Berlin, Germany: Springer-Verlag, 2010, pp. 148–164.
[14] P. Golle, J. Staddon, and B. Waters, "Secure conjunctive keyword search over encrypted data," in *Proc. 2nd Int. Conf. Appl. Cryptogr. Netw. Secur. (ACNS)*, vol. 3089. Huangshan, China, Jun. 2004, pp. 31–45.
[15] V. Goeyaln, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *Proc. 13th ACM Conf. Comput. Commun. Secur.*, 2006, pp. 89–98.
[16] S. Hohenberger and B. Waters, "Attribute-based encryption with fast decryption," in *Proc. 16th Int. Conf. Pract. Theory Public- Key Cryptogr. (PKC)*, vol. 7778. Nara, Japan, Feb./Mar. 2013, pp. 162–179.
[17] Y. H. Hwang and P. J. Lee, "Public key encryption with conjunctive keyword search and its extension to a multi-user system," in *Pairing-Based Cryptography—Pairing* (Lecture Notes in Computer Science), vol. 4575.
[18] R.meena nagarathinam et al.Attribute Based Encryption for Scalable and Secure Sharing of Medical Records in Cloud Computing Design and Implementation 2014
[19] VM.Prabhakara ram profs,S.Balasubramaniam Sequence Flow Modelling for Efficient[2014]sept,
[20] Protection of Personal Health Records (PHRs).