TRADITIONAL CLOUD DATA SECURITY MECHANISM FOR EFFICIENT PROCESSING IN CLOUD ENVIRONMENT

Sk. Ayisha Begum, *Asst. Prof., Department of MCA, QIS College of Engineering and Technology, Ongole*,
V. Prabhavathi, *Final Year Student of Master of Computer Applications, QIS College of Engineering and Technology, Ongole*

Abstract*—Public key encryption supporting equality test (referred to as PKE-ET) provides the capability of testing the equivalence between two messages encrypted under different public keys. Ciphertext-policy attribute-based encryption (CP-ABE) is a promising primitive to achieve versatile and secure data sharing in the cloud computing by providing flexible one-to-many encryption. In this paper, we first initialize the concept of CP-ABE with equality test (CP-ABE-ET) by combining the notions of PKE-ET and CP-ABE. Using ABE-ET primitive, the receiver can delegate a cloud server to perform an equivalence test between two messages, which are encrypted under different access policies. During the delegated equivalence test,the cloud server is unable to obtain any knowledge of the message encrypted under either access policy. We propose a concrete CP-ABE-ET scheme using bilinear pairing and ViJete'sformulas, and give the security proof of the proposed scheme formally in the standard model. Moreover, the theoretic analysis and experimental simulation reveal that the proposed scheme is efficient and practical.*

I. INTRODUCTION

The popularity and pervasiveness of cloud computing have brought a revolutionary innovation to data sharing . With cloud computing, cloud users can not only acquire useful data more effortlessly, but can offer noteworthy benefits to society as well by sharing their own data with other users or organizations. In this way, the cost for cloud users to share data can be saved signicantly. Taking the personal health record (PHR) system for example. Patients in PHR system can measure and gather their sensitive PHR information by using medical sensors. To share their PHR data with physicians in the hospital or other patients with similar symptoms, patients can upload their PHR data to a cloud server. Based on the collectedPHR data from various patients featured with similar

symptoms, one can evaluatehis/her own health status accurately. Moreover, the physicians can treat such kind of disease more precisely by analyzing the PHR data from a group of patients. No matter how favorable the cloud computing is, the unauthorized access of the sharing data should be prevented prior to the practical deployment of cloud computing to ensure the security of these data. When these data, such as e-mails, personal health records, financial transactions, are accessed by illegal entities including the cloud server itself, the data owner may suffer incalculable economic and reputational losses. Therefore, every data owner should take measures to ensure the efficient access control of their data before uploading them to clouds. Attribute-basedencryption (shorten as ABE) is commonly considered as a exile and versatile solution to enforce access control with ne-granularity over encrypted data in the cloud computing. So far, there are two types of ABE schemes, i.e., the cipher text-policy ABE (CP-ABE) and key-policy ABE (KP-ABE). In CP-ABE, any user is labeled with a set of attributes and can obtain a secret key according to these attributes. And the cipher text is generated under a given access policy. One secret key can be used to decipher a speciec cipher text only if the attributes related to this secret key satisfy the policy embedded into the cipher text. Different from CP-ABE, the access policy and the attributes are attached to secret keys and cipher texts of the user in a reverse order in KP-ABE. Apparently, the encrypt or in the KP-ABE is unable to decide who ought to or ought not to access the data and thus CP-ABE is more suitable for achieving exile access control over sharing data in the environment of cloud computing. So, in this paper, we only focus on CP-ABE. By leveraging CP-ABE, the _engrained access control for PHR system can be achieved as follows. Suppose one patient, say Alice, intends to share her PHR data m with medical researchers and attending physicians in the Massachusetts General Hospital.

To enforce access control over her PHR data, Alice species the access policy pol D f(``Massachusetts General Hospital'') AND (``Medical Researchers'' OR ``Attending Physicians'')g and generates the cipher text according to pol by using CP-ABE scheme. After uploading the cipher text to the cloud server, the secure and _exile data sharing can be realized such that only the specified users can access by using their own secret keys.However, the standard ABE alone may hinder search functionality over encrypted data outsourced in the cloud server. Suppose (Enc(m1; pol1), Enc(m2; pol2),

Enc(mn; poln)) is a set of encrypted medical data contributed by anonymous donators for research purpose.

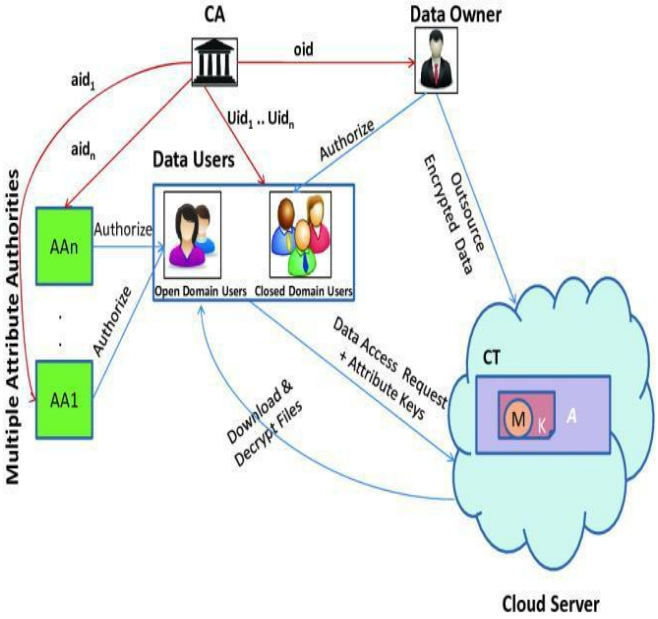


Fig: Ciphertext Searching with ABE-ET in cloud environment.

Here, each medical data mi is encrypted under the corresponding policy poli such that mi can only be accessed by cloud users who satisfy poli. To obtain intended information from this set of encryption, cloud user needs to download all cipher texts and then decrypt these cipher texts.It is easy to observe that this naive approach is inefficient and impractical. To solve this problem, the idea of ABE with keyword search (ABE-KS) was invented as the combination of ABE and public key encryption with keyword search (PKE-KS) . In ABE-KS scheme, a receiver can delegate the searching capability to the cloud server. With a trapdoor issued by the receiver, the cloud server is able to search the stored ABE-type cipher text once the attributes related to the trapdoor match the access structure of these cipher texts. Meanwhile, the cipher text is unable to be decrypted by the cloud server.who owns the trapdoor. Although ABE-KS seems to be a promising solution to provide search functionality in the ABE-based access control system, it is still far from satisfactory since the trapdoor can be used to search cipher texts only if the attributes of the trapdoor satisfy the policies of the cipher texts. For instance, if the attributes of Bob, match policies pol1 and pol2, then only the encryptions of (Enc(m1; pol1) and (Enc(m2; pol2) can be searched by the cloud server on behalf of Bob. To obtain more edibility about cipher text searching, a desirable solution is to allow the cloud server to perform search functionality on cipher texts associated with different access policies. This practical requirement naturally motivates us to design a novel attribute based encryption system with equality test (ABE-ET), which enables cloud user to search over the ABE-type cipher texts associated with different access policies.

II. RELATED WORK

Public key encryption with equality test (PKE-ET), initi-ated by Yang et al. [12], enables any entity to perform an equivalence test between two messages encrypted distinct public keys. This primitive can be used to achieve exible search functionality over ciphertexts under different public keys. To equip this primitive with authorization mechanism, a novel PKE-ET was suggested by Tang [13] to designate the entity who can carry out equality test. In [13], the autho-rization needs to be realized by performing an interactive protocol between the delegating users. It is easy to observe this authorization mechanism is not scalable since each user needs to interact with other users in the system to delegate the capability ofequivalence test power. Thus, the notion of PKE-ET scheme with delegated equality test (PKE-DET) was introduced by Tang [14] and Ma et al. [16] respectively in which each user can issue the delegation token indepen-dently to the cloud server. After that, Tang [15] formulated an enhanced PKE-ET scheme by allowing twoproxies jointly to execute the equality test and impede off-line message recovery attacks. Subsequently, Huang et al.[17] introduced a novel PKE with authorized equality test (PKE-AET) such that a user can authorize warrants on all ofhis/her ciphertexts or a speci ed ciphertext. To feature the authorization with more exibility. An efcient PKE-ET scheme was proposed by Ma et al. [18] in which four kinds of authorization are contained. As a special kind of PKE, identity-based encryp-tion (IBE) has attracted a huge amount of interest by simplifying public key certi cate management[19] [21]. Subsequently, an identity-based encryption scheme with outsourced equality test (IBE-ET) was formulated by Ma [22] by incorporating the concept of IBE and PKE-ET scheme. Following Ma's work [22], a semi-generic construction of IBE-ET scheme was introduced by Lee al et. [23] to strengthen the security requirement. Very recently, to improve the efciency of Ma's IBE-ET scheme, Wu et al. [24] pro-posed a novel IBE-ET scheme which is more tting for mobile cloud environment.PKE with keyword search (PKE-KS), rstly formulated in [9], achieves the functionality to perform an equivalence test between keywords embedded in a ciphertext or a tag. IBE with keyword search (IBE-KS), initially introduced in [25], is an extension of PKE-KS to enjoy the merits of IBE scheme andPKE-KS scheme. As an extension of IBE, ABE has also attracted a lot of concern since it can provide ne-grained access control [26][28].

Similarly, the attribute-based encryption with keyword search (ABE-KS) [7], [8] has been proposed as the best-of-two-worlds to enjoy the merits of ABE scheme and PKE-KS scheme. However, the above three primitives only allow performing an equiva-lence test on ciphertexts under a xed public key, a xed identity and a xed access policy. Recently, Zhu et al. pro-posed a KP-ABE with ET scheme [29] that allows testing whether the ciphertexts contain the same information under different attribute sets. However, it only supports monotonic access structure which limits the express of access policy. Besides, it only achieves one-way against

chosen-ciphertext attack (OW-CCA) in the random oracle model. As far as we know, CP-ABE with equality test has not been treated to support the functionality to perform an equivalence test on ciphertexts under different access policies in the literature so far.

III. EXISTING SYSTEM

So far, there are two types of ABE schemes, i.e., the ciphertext-policy ABE (CP-ABE) and key-policy ABE (KP-ABE). In CP-ABE, any user is labeled with a set of attributes and can obtain a secret key according to these attributes. And the ciphertext is generated under a given access policy. One secret key can be used to decipher a specific cipher text only if the attributes related to this secret key satisfy the policy embedded into the cipher text.

A) Disadvantages:

However, the standard ABE alone may hinder search functionality over encrypteddata outsourced in the cloud server. Suppose (Enc(m1; pol1), Enc(m2; pol2), : : :, Enc(mn; poln)) is a set of encrypted medical data contributed by anonymous donators for research purpose. Here, each medical data mi is encrypted under the corresponding policy poli such that mi can only be accessed by cloud users who satisfy poli. To obtain intended information from this set of encryption, cloud user needs to download all cipher texts and then decrypt these cipher texts.Although ABE-KS seems to be a promising solution to provide search functionality in the ABE-based access control system, it is still far from satisfactory since the trapdoor can be used to search cipher texts only if the attributes of the trapdoor satisfy the policies of the cipher texts.

IV. PROPOSED SYSTEM

We, for the First time, introduce the idea of PKE-ET into the CP-ABE-based setting to enjoy the best-of-thetwo- worlds. Specially, a semi-trusted entity (such as cloud server) in ABE-ET can be delegated to execute an equivalence test on CP-ABE-type cipher texts encrypted under different access policies. Meanwhile, this delegated entity cannot learn any information about the plaintext. Suppose the receiver (say Alice) intends to search the ABE-type cipher texts stored in the cloud server with another receiver (say Bob). It is desirable that the searching capability can be delegated to the cloud server by Alice. Inspired by the primitive of ABE-ET, Alice first delegates her trapdoor to the un trusted cloud server. After receiving the request of keyword searching from Alice, Bob then creates his trap door using his own secret key anddelivers his trapdoor to the cloud server. Equipped with the trapdoor of Alice, the cloud server could be authorized to perform search functionality on messages encrypted under different access policies. By using the ABE-ET primitive, the ABE-type cipher texts can be searched only if the attributes related to the trapdoor match the access structure of these cipher texts, whereas any useful information about the plaintext or secret keys of Alice or Bob can not obtained by the cloud server. Finally, Alice receives the returned searching result from the cloud server and then decrypts the cipher text with her own secret key. In this way, the overburden of cipher text searching could be offloaded to the cloud server with sufficient resources.

A) Advantages:

CP-ABE-ET cryptosystem named ciphertext-policy attribute based encryption with equality test is introduced to provide users with searching capability on cipher texts and fine-grained access control.With our proposed CP-ABE-ET scheme, each user featured with attributes delegates a cloud server to test the equivalence between two messages under different access policies.

V.METHODOLOGY

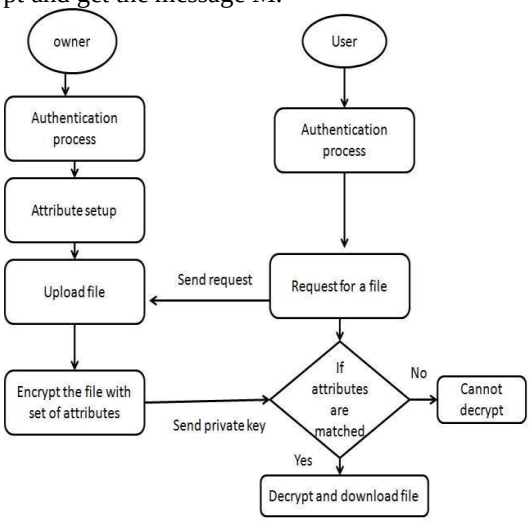
Attribute Based Encryption is specified by four algorithms namely Setup, Encrypt, key generation, and Decrypt.

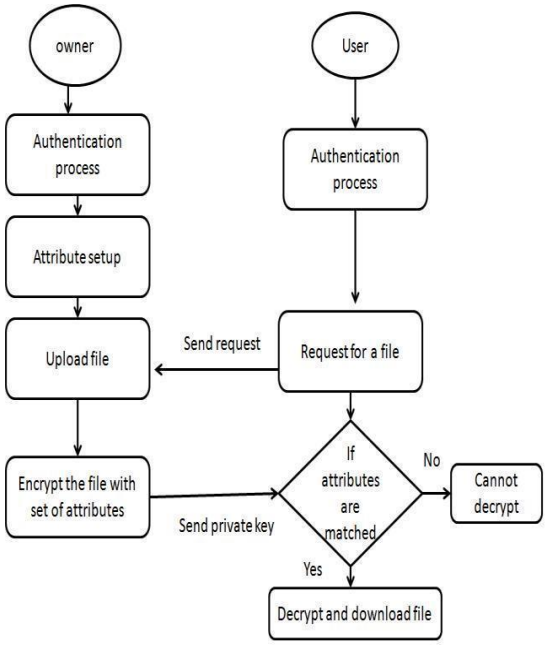
1) Setup: This step takes no input but considers implicit parameters and produces public key PK and master key MK.

2) Encrypt(PK,M,A): For encryption it uses public key PK , message M and access structure A for set of attributes.
Produces the cipher text CT. User whose attributes match with the policy only can access the information.

3) Key Generation(MK,A[ ]): this step takes master key and array of attributes as input and generates private key SK.

4)Decrypt(PK,CT,SK):It takes public key, ciphertext which includes policy and private key for array of attributes and if the array of attributes satisfies the policy only then he can decrypt and get the message M.





In order to encourage users to use the advisor and continue to

Here owner is going to upload file. While uploading owner selects certain set of attributes or credentials which describes user. Using those credentials access tree structure is formed called policy. To encrypt the data along with public and private keys, policy is also used. This provides fine grained access control and security for the data.

An Elliptic Curve is curve of the form:

$y^2 = x^3 + ax + b$ (1.2)

where a, b, c and x, y are elements of some Field. A finite field is a field where the set ishaving a finite number of elements. The algorithms based on elliptic curve uses smaller key size compared to other algorithms". This is the main advantage of elliptic curve cryptography. In this paper "fine grained access control of data is provided by using Ciphertext Policy Attribute Based Encryption (CP-ABE)" . A. Fine grained access control

While uploading file owner will register himself first. Owner will select certain set of attributes related to user that means owner is restricting the access of information to specified user. Only those users who satisfy the policy can access the information. Restricting access of information possesses fine grained access control. During uploading owner will select the attributes. Those attribute sets are sent as parameter to encrypt the file that is called as policy. At the user end any user can send request to access the file. Owner may accept or reject the request. If at all owner accepts the request even though sometimes user cannot download the file. Because his credentials may not match with the policy. So even if it is an untrusted network also owner can upload the file without any tension.

VI. CONCLUSION

In our paper, a novel CP-ABE-ETcryptosystem named ciphertext-policy attribute based encryption with equality test is introduced to provide users with searching capability on ciphertexts and fine-grained access control. With our proposed CP-ABE-ET scheme, each user featured with attributes delegates a cloud server to test the equivalence between two messages under different access policies. Meanwhile, the cloud server cannot access the plaintextduring the delegated equivalence test. Finally, the rigorous security proof is givento show the IND-CPA security in the standard model under DLIN assumption. Additionally, we present performance and simulation comparisons of existing IBE-ET, ABE-KS and KP-ABE-ET with our CP-ABE-ET scheme to demonstrate that our scheme is practical. Future work contains seeking to build CP-ABE-ET scheme to achieve the security level of IND-CCA2 in standard model.

VII. REFERENCES

[1] *M. Armbrust et al., ``A view of cloud computing,"Commun. ACM, vol. 53, no. 4, pp. 50_58, 2010.*

[2] *S. Marston, Z. Li, S. Bandyopadhyay, J. Zhang, A. Ghalsasi, ``Cloud computing_The business perspective," Decision support Syst., vol. 51, no. 1, pp. 176_189, 2011.*

[3] *C. Pagliari, D. Detmer, and P. Singleton, ``Potential of electronic personal health records," Brit. Med. J., vol. 335, no. 7615, pp. 330_333, 2007.*

[4] *D. Kaelber et al., ``A research agenda for personal health records (PHRs)," J. Amer. Med. Informat. Assoc., vol. 15, no. 6, pp. 729_736, 2008.*

[5] *V. Goyal, O. Pandey, A. Sahai, and B.Waters, ``Attribute-based encryption for _ne-grained access control of encrypted data," in Proc. 13th ACMConf. Comput. Commun. Secur. (CCS), 2006, pp. 89_98.*

[6] *J. Bethencourt, A. Sahai, and B.Waters,``Ciphertext-policy attribute-based encryption," in Proc. IEEE Symp. Secur. Privacy (SP), 2007, pp. 321_334.*

[7] *K. Liang and W. Susilo, ``Searchable attribute-based mechanism with ef_cient data sharing for secure cloud storage," IEEE Trans. Inf. Forensics Security, vol. 10, no. 9, pp. 1981_1992, Sep. 2015.*

[8] *Q. Zheng, S. Xu, and G. Ateniese, ``VABKS: Veri_ableattributebased keyword search over outsourced encrypted data," inProc. 33rd Annu. IEEE Int. Conf. Comput. Commun. (INFOCOM), Apr./May 2014, pp. 522_530.*

[9] *D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, ``Public key encryption with keyword search," in Advances in Cryptology (Lecture Notes in Computer Science), vol. 3027, C. Cachin andJ. Camenisch, Eds. Berlin, Germany:Springer-Verlag, 2004, pp. 506_522.*

[10] *J. Baek, R. Safavi-Naini, and W. Susilo, ``Public key encryption with keyword search revisited," in Proc. Int.*

Conf. ICCSA, vol. 5072. Perugia, Italy, Jun./Jul. 2008, pp. 1249_1259.

[11]Y. H. Hwang and P. J. Lee, ``Public key encryption with conjunctive keyword search and its extension to a multi-user system,'' inPairing-Based Cryptography_Pairing (Lecture Notes in Computer Science), vol. 4575. Berlin, Germany: Springer, 2007, pp. 2_22.

[12]G. Yang, C. H. Tan, Q. Huang, and D. S. Wong, ``Probabilistic public key encryption with equality test,'' in Proc. Int. Conf. Topics Cryptol. (CT-RSA), vol. 5985. 2010, pp. 119_131.

[13]Q. Tang, ``Towards public key encryption scheme supporting equality test with _ne-grained authorization,'' in Proc. Austral. Conf. Inf. Secur.Privacy, vol. 6812. 2011, pp. 389_406.

[14]Q. Tang, ``Public key encryption supporting plaintext equality test and user-speci_ed authorization,''Secur. Commun. Netw., vol. 5, no. 12, pp. 1351_1362, 2012

[15]Q. Tang, ``Public key encryption schemes supporting equality test with authorisation of different granularity,'' Int. J. Appl. Cryptogr., vol. 2, no. 4, pp. 304_321, 2012.

[16]S. Ma, M. Zhang, Q. Huang, and B. Yang, ``Public key encryption with delegated equality test in a multi-user setting,''Comput. J., vol. 58, no. 4, pp. 986_1002, 2014.

[17]K. Huang, R. Tso, Y.-C. Chen, S. M. M. Rahman, A. Almogren, and A. Alamri, ``PKE-AET: Public key encryption with authorized equality test,''Comput. J., vol. 58, no. 10, pp. 2686_2697, 2015.

[18]S. Ma, Q. Huang, M. Zhang, and B. Yang, ``Ef_cient public key encryption withequality test supporting _exible authorization,'' IEEE Trans. Inf. Forensics Security, vol. 10, no. 3, pp. 458_470, Mar. 2015.

[19]D. Boneh and M. Franklin, ``Identity-based encryption from theWeil pairing,'' in Advances in Cryptology_CRYPTO. Berlin, Germany: Springer, 2001, pp. 213_229.

[20]C. Gentry and S. Halevi, ``Hierarchical identity based encryption with polynomially many levels,'' in Proc. Theory Cryptogr. Conf., 2009, pp. 437_456.

[21]S. Luo and Z. Chen, ``Hierarchical identity-based encryption without key delegation in decryption,'' Int. J. Grid Utility Comput., vol. 5, no. 2, pp. 71_79, 2014.