International Journal for Research in Applied Science & Engineering Technology (IJRASET)

A Survey on Classification Methodologies of Encryption Methods in Cloud

G.Priyanga[1], S.Benila[2]
[1]PG Scholar, [2]Assistant Professor, Dept. of C.S.E
Valliammai Engineering College, Chennai, India.

Abstract*: Cloud computing is a model for emerging convenient, on-demand access to shared pool of configurable computing resources. Cloud computing is modify the way of organizations manage their data. Privacy is main issues for storing and retrieving the data. To prevent data from unauthorized data by using various methods such as access control, attribute based encryption method, trusted third party, audit ability these methods are enabling to provide user for integrity and confidentiality. Here this paper explains the various issues related to privacy for user's data on cloud server to propose third party authentication system. To propose an access control scheme for secure data storage in cloud server. It support anonymous authentication. The task of allowing third party auditor to verify the integrity of the dynamic data stored in the cloud.

KeyWords*: Cloud computing, Access control, Attribute based encryption method, trusted third party, Audit-ability.

I. INTRODUCTION

Cloud computing is globally developed technology used in various industries such as medical, IT, Business, Institution, which provides many services like resources, network access resources as per user require. The end user can access the cloud storage in which the data is store in virtualized pools of storage that are given by the third party auditor. In cloud storage the user have some issues like privacy, security data integrity, and dynamic updates. At any time it is not possible. Cloud storage provides to retrieve data through computers, and internet devices. This problem is addressed and solves by various privacy methods. To ensure the data integrity by enabling public auditing services for cloud storage. So that the user may third party auditor by audit the user data. The TPA has all capabilities to check the correctness of data stored in cloud and maintain the integrity.

Enabling public auditing services will play the main role for data privacy and security also minimizing like from unauthorized user or hackers. TPA is the external party of cloud server it maintain the data and it does not provide the guaranteed of data privacy.

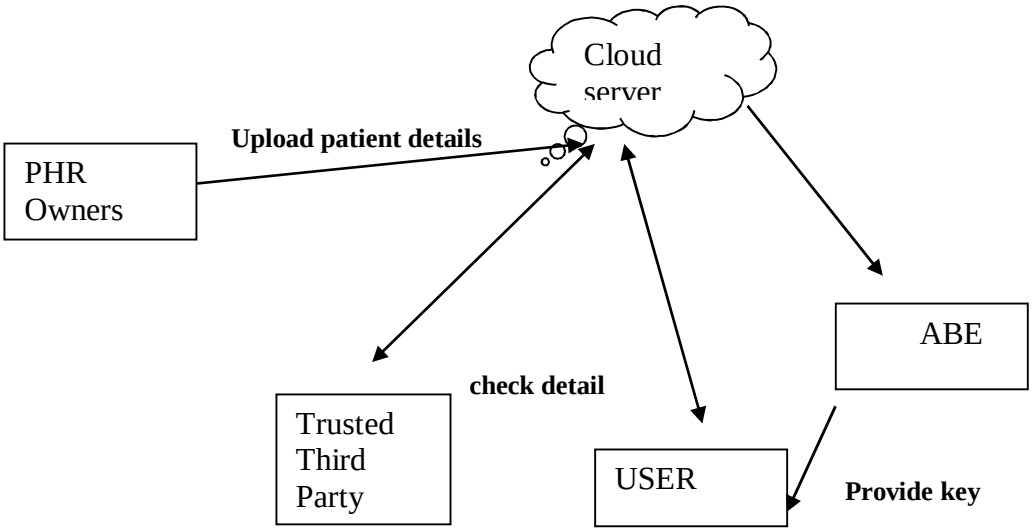

Fig. 1 Architecture

II. CLASSIFICATION OF ENCRYPTION METHOD

Cloud computing, there are different existing schemes that provide security, data confidentiality and access control. Users need to

share sensitive objects with others based on the recipient's ability to satisfy a policy in distributed systems. One of the encryption schemes is Attribute Based Encryption (ABE) which is a new paradigm where such policies are specified and cryptographically enforced in the encryption algorithm itself. Hence, the existing ABE schemes are of two types. They are Key- Policy ABE (KP-ABE) scheme and Ciphertext-Policy ABE (CP- ABE) scheme. Encryption techniques for personal health records in cloud computing literature review as follows.

A. Attribute Based Encryption

Attribute-Based Encryption (ABE), a generalization of identity-based encryption that incorporates attributes as inputs to its cryptographic primitives. Data is encrypted using a set of attributes so that multiple users who possess proper can decrypt. Attribute-Based Encryption (ABE) not only offers fine-grained access control but also prevents against collusion. J. Benelux [2], has proposed a scheme in which a file can be uploaded without key distribution and it is highly efficient. But it is a single data owner scenario and thus it is not easy to add categories. C. Dong [5] has explored that the data encryption scheme does not require a trusted data server. The server can perform encrypted searches and updates on encrypted data without knowing the plaintext or the keys to decrypt. But in this scheme the server knows the access pattern of the users which allows it to infer some information about the queries. To realize fine grained access control, the traditional public key encryption based schemes and either incur high key management overhead, or require encrypting multiple copies of a file using different users keys. To improve upon the scalability of the above solutions, one-to-many encryption methods such as attribute based encryption (ABE) can be used. Sashay and Waters [7] first introduced the attribute based encryption (ABE) for enforced access control through public key cryptography. The main goal for these models is to provide security and access control. The main aspects are to provide flexibility, scalability and fine grained access control. In classical model, this system can be achieved only when user and server are in a trusted domain. So, the new access control scheme that is „Attribute Based Encryption (ABE)" scheme was introduced which consist of key policy attribute based encryption (KP-ABE). As compared with classical model, KP-ABE provided fine grained access control. However it fails with respect to flexibility and scalability when authorities at multiple levels are considered. In ABE scheme both the user secret key and the cipher text are associated with a set of attributes. ABE is implemented for one-to many encryption in which cipher-texts are not necessarily encrypted to one particular user, it may be for more than one number of users. Akinyele et al investigated using ABE to generate self-protecting EMRs, which can either be stored on cell phones or cloud servers so that EMR could be accessed when health provider is in offline also. Limitations of ABE: The use of a single trusted authority (TA) in the system. Single trusted authority (TA) not only creates a load bottleneck, but also have key escrow problem since the TA can access all the encrypted files. This opens the door for potential privacy exposure.

B. Key Policy Attribute Based Encryption

V. Goyal, O. Pandey, A. Sashay, and B. Waters [5] proposed a key-policy attribute-based encryption (KP-ABE) scheme. It is the modified form of the classical model of ABE. Exploring KP-ABE scheme, attribute policies are associated with keys and data is associated with attributes. The keys only associated with the policy that is to be satisfied by the attributes that are associating the data can decrypt the data. Key Policy Attribute Based Encryption (KP-ABE) scheme is a public key encryption technique that is designed for one-to-many communications. This scheme enables a data owner to reduce most of the computational Prof.Y.B.Gurav *et al*, International Journal of Computer Science and Mobile Computing, Vol.3 Issue.2, February- 2014, pg. 617-625 © ***2014, IJCSMC All Rights Reserved 622*** overhead to cloud servers. The use of this encryption scheme KP-ABE provides fine-grained access control. Each file or message is encrypted with a symmetric data encryption key (DEK), which is again encrypted by a public key corresponding to a set of attributes in KPABE, which is generated corresponding to an access structure. The data file that is encrypted is stored with the corresponding attributes and the encrypted DEK. Only if the corresponding attributes of a file or message stored in the cloud satisfy the access structure of a user's key, then the user is able to decrypt the encrypted DEK, which is used to decrypt the file or message. Limitations of KP- ABE: The main disadvantage in the scheme is that the data owner is also a Trusted Authority (TA) at the same time. If this scheme is applied to a PHR system with multiple data owners and users, it would be inefficient because then each user would receive many keys from multiple owners, even if the keys contain the same set of attributes.

C. Expressive Key Policy Attribute Based Encryption

Y. Zheng proposed Expressive Key-Policy ABE ,the encryption methods in clouds Attribute-based encryption (ABE), allows fine grained access control on encrypted data. In the key policy Attribute based encryption, the primitive enables senders to encrypt messages with a set of attributes and private keys are associated with access tree structure that specifies which all the cipher texts the key holder is allowed to decrypt. In most ABE systems, the cipher text size grows linearly with the number of cipher text attributes and the only known exceptions only support restricted forms of threshold access policies. This expressive key-policy attribute based encryption (KP-ABE) schemes allowing for non-monotonic access and with constant cipher text size. The private keys have quadratic size in the number of attributes. On the other hand, they reduce the number of pairing evaluation size to a constant, which appears to be a unique feature among expressive KP-ABE schemes. This is more efficient than KP-ABE. **cipher text policy attribute based encryption**

D. Cipher Policy Attribute Based Encryption

Sashay et al [7] introduced the concept of another modified form of ABE called CP-ABE that is Ciphertext Policy Attribute Based Encryption. In several distributed systems a user should only be able to access data if a user possesses a certain set of credentials or attributes. To store the data and mediate access control a trusted server is the only method for enforcing such policies The confidentiality of the data will be compromised, if any server storing the data is compromised. The storage server is untrusted if the data can be confidential by this technique. Previous Attribute-Based Encryption systems used to the outsourced data can be described and built policies into user's keys. While in this system attributes are used to describe a users credentials, and a party encrypting data determines a policy for decrypt. In cipher text-policy attribute-based encryption (CP-ABE), depends how attributes and policy are associated with cipher texts and users decryption keys. In a CP-ABE scheme, a cipher text is associated with a monotonic tree access structure and a user's decryption key is associated with set of attributes. In this scheme the cipher text is encrypted with a tree access policy chosen by an encrypt or, while the decryption key is generated with respect to a set of attributes. As long as the set of attributes should satisfy the tree access policy and it can be associated with a decryption key with a given cipher text, the key can be used to decrypt the cipher text. However, basic CP-ABE schemes are far from enough to support access control in modern enterprise environments, require considerable flexibility and efficiency in specifying policies and managing user attributes. Limitations of CP-ABE: Decryption keys only support user attributes that are organized logically as a single set, so users can only use all possible combinations of attributes in a single set issued in their keys to satisfy policies.

E. Cipher Text Policy Attribute Set Based Encryption

S. Jihad, P. Metal, and N. Borisov et al [6] applied CP- ASBE schemes with immediate attribute revocation capability, instead of periodical revocation. Cipher text Policy Attribute Set Based Encryption (CP-ASBE)- a new form of CP-ABE. It organizes user attributes into a recursive set based structure and allows users to impose dynamic constraints on how those attributes may be combined to satisfy a policy. In a CP-ABE scheme, decryption keys only support user attributes that are organized logically as a single set, so users can only use all possible combinations of attributes in a single set issued in their keys to satisfy policies. Prof.Y.B.Gurav *et al*, International Journal of Computer Science and Mobile Computing, Vol.3 Issue.2, February- 2014, pg. 617-625 © ***2014, IJCSMC All Rights Reserved 623*** To solve this problem, cipher text-policy attribute-set- based encryption is introduced. Thus, by grouping user attributes into sets such that those belonging to a single set have no restrictions on how they can be combined, CP-ASBE can support compound attributes without sacrificing the flexibility to easily specify policies involving the underlying singleton While restricting users to use attributes from a single set during decryption can be thought of as a regular CP-ABE scheme, the challenge in constructing a CP-ASBE scheme is in selectively allowing users to combine attributes from multiple sets within a given key while still preventing collusion. Limitations of CP-ASBE: Constructing a CP-ASBE scheme is in selectively allowing users to combine attributes from multiple the cloud providers. However HABE uses disjunctive normal form policy and assumes all attributes in one conjunctive clause are administrated by the same domain master by multiple domain masters. The same attribute may be administrated according to specific policies, which is difficult to implement in practice.

F. Identity Based Encryption (IBE) And Hierarchical Identity Based Encryption (HIBE)

M. Franklin, Debone [3] introduced an identity-based encryption scheme, data is encrypted using an arbitrary string as the key and for decryption; a decryption key is mapped to the arbitrary encryption key by a key authority. Hierarchical Identity Based

Encryption (HIBE) is the hierarchical form of a single IBE [3]. The concept of HIBE scheme can help to explain the definition of security. Ina regular IBE (1-HIBE) scheme, there is only one private key generator (PKG) that distributes private keys to each users, having public keys are their primitive ID (PID) arbitrary strings. A two-level HIBE (2-HIBE) scheme consists of a root PKG, domain PKGs and users, all of which are associated with PID‟s. A users public key consists of their PID and their domains. In a 2-HIBE, users retrieve their private key from their domain PKG. The private key PK is compute by Domain PKGs of any user in their domain, their domain secret key-SK can be provided and previously requested from the root PKG. Similarly, is for number of sub-domains. There also includes a trusted third party or root certificate authority that allows a hierarchy of certificate authorities: Root certificate authority issues certificates for other authorities or users in their respective domains. The original system does not allow for such structure. However, a hierarchy of PKG is reduces the workload on root server and allows key assignment at several levels. Limitations of IBE: The main disadvantage of this system is key management overhead. Letting each user obtain keys from every owner PHR wants to read would limit the accessibility.

G. Hierarchical Attribute-Base Encryption (HABE) And Hierarchical Attribute set Based Encryption (HASBE)

This scheme Hierarchical attribute-based encryption (HABE) is derived by Wang et al .It is designed to achieve fine-grained access control in cloud storage services. It is a combination of HIBE and CP-ABE. In the HABE scheme, there are multiple keys with different usages. Limitations of HASBE: Compared with ASBE, this scheme cannot support compound attributes efficiently and does not support multiple value assignments.

H. Distributed Attribute-Based Encryption

S. Run, A. Kayak, and I. Stojmenovic [9] introduced a concept of Distributed Attribute-Based Encryption (DABE). In DABE, there will be an arbitrary number of parties to maintain attributes and their corresponding secret keys. There are three different types of entities in a DABE scheme [9]:1. The master is responsible for the distribution of secret user keys. However, master is not involved in the creation of secret attribute keys.2. Attribute authorities are responsible to verify whether a user is eligible of a specific attribute; in this case they distribute a secret attribute key to the user. An attribute authority generates a public attribute key for each attribute it maintains; this public key will be available to all the users. Eligible users receive a personalized secret attribute key over an authenticated and trusted channel. 3. Users can encrypt and decrypt messages. To encrypt a message, user should formulate the access policy in Disjunctive Normal Form (DNF).To decrypt a cipher text, a user needs at least access to some set of attributes which satisfies the access policy. The main advantage of the solution is each user can obtain secret keys from any subset of the Trusted Authorities (TAs) in the system. Prof.Y.B.Gurav *et al*, International Journal of Computer Science and Mobile Computing, Vol.3 Issue.2, February- 2014, pg. 617-625 © ***2014, IJCSMC All Rights Reserved 624*** Limitations of DABE: It requires a data owner to transmit an updated cipher text component to every non-revoked user. While sharing the information the communication overhead of key revocation is still high.

I. Cipher text Policy Attribute Based Encryption

Recently Ibrahim et.al. applied cipher text policy ABE (CP-ABE) to manage the sharing of PHRs. However, they still assume a single public authority, while the challenging key-management issues remain largely unsolved. For the PUDs, our framework delegates the key management functions to multiple attribute authorities. In order to achieve stronger privacy guarantee for data owners, the Chase-Chow (CC) MA-ABE scheme is used, where each authority governs a disjoint set of attributes distributive.

J. Homographic Encryption

An encryption scheme has algorithm consists of three steps [2]. 1. Key Generation - creates two keys i.e. the privacy key park and the public key puck. 2. Encryption - encrypts the plaintext P with the public key puck to yield cipher text C. 3. Decryption - decrypts the cipher text C with the privacy key park to retrieve the plaintext P. 4. Evaluation - outputs a cipher text C of f(P) such that Decrypt (prk,P) = f(P). The scheme becomes homomorphism if f can be any arbitrary function, and the resulting ciphertext of Eval is compact. That means it does not grow too large regardless of the complexity of function f). The Eval algorithm in essence means that the scheme can evaluate its own decryption algorithm. Utilizing Homomorphic Authenticators[11] to significantly reduce the arbitrarily large communication Overhead for public auditability without introducing any online burden on the data owner, we resort to the homomorphic authenticator technique Homomorphic authenticators are unforgeable metadata generated from individual data blocks, which can be securely aggregated in such a way to assure a verifier that a linear combination of data blocks is correctly

computed by verifying only the aggregated authenticator.

III. CONCLUSION

This paper made a survey on the Improving the Security on Public Health Record System in Cloud Computing. And also made a detailed study about what are the techniques is needed for security the Health Record System. Attribute Based Encryption is the good technique to securing the Health records. It is efficient in the Conjunctive Property. But somewhat limitations on MA-ABE in real time with the property of Disjunctive as well as it had the little bit problem while revocation. Because it can be affect the non-revoked users. So move to the Attribute Based Broadcast Encryption. It satisfies the Disjunctive Property also and handles the revocation perfectly. Identity Based Encryption is the better way to provide the authentication for the Public Health Record System. homomorphic encryption with data auditing is used to verify the trustworthiness of third party auditor.

REFERENCES

[1] Sahai and B. Waters. “Fuzzy Identity Based Encryption.”, In Advances in Cryptology – Eurocrypt, volume 3494 of LNCS, pages 457–473. Springer, 2005.
[2] Li, M., Lou,W., Ren, K., “ Data security and privacy in wireless body area networks”, IEEE Wireless Communications Magazine (February 2010).
[3] M. Li, S. Yu, K. Ren, and W. Lou, “Securing Personal Health Records in Cloud Computing: Patient -Centric and Fine-Grained Data Access Control in Multi-Owner Settings”, Proc. Sixth Int˝l ICST Conf. Security and Privacy in Comm. Networks (SecureComm ˝10),pp. 89 -106, Sept. 2010. Prof.Y.B.Gurav et al, International Journal of Computer Science and Mobile Computing, Vol.3 Issue.2, February- 2014, pg. 617-625 © 2014, IJCSMC All Rights Reserved 625
[4] V. Goyal, O. Pandey, A. Sahai, and B. Waters, “Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data,”Proc. 13th ACM Conf. Computer and Comm. Security (CCS ˝06),pp. 89-98, 2006.
[5] Ming LiShucheng Yu, Yao Zheng,Kui Ren, and Wenjing Lou, “Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption”, IEEE transactions on parallel and distributed systems, vol. 24, no. 1, january 2013.
[6] L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker, “Ciphertext-Policy Attribute-Based Threshold Decryption with Flexible Delegation and Revocation of User Attributes”, 2009.
[7] L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker, “Ciphertext-Policy Attribute-Based Threshold Decryption with Flexible Delegation and Revocation of User Attributes”, 2009.
[8] S. Yu, C. Wang, K. Ren, and W. Lou, “Attribute Based Data Sharing with Attribute Revocation,” Proc. Fifth ACM Symp. Information, Computer and Comm. Security (ASIACCS ˝10), 2010.
[9] S. Narayan, M. Gagne´, and R. Safavi-Naini, “Privacy Preserving EHR System Using Attribute-Based Infrastructure”, Proc. ACM Cloud Computing Security Workshop (CCSW ˝10), pp. 47-52, 2010.
[10] J. Bethencourt, A. Sahai, and B. Waters, “Ciphertext-Policy Attribute-Based Encryption”, Proc. IEEE Symp. Security and Privacy (SP ˝07), pp. 321-334, 2007.
[11] Q.Wang et al.,“Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing,” Proc. ESORICS „09, Sept. 2009, pp. 355–70.