International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-5, January 2020

Exploration of Attribute Based Encryption Schemes on Cloud Computing Storage

M. Vignesh, R. Naresh

Abstract: ***The storage of Electronic Health records on cloud storage has lead to the need for security and privacy concern. Different methods were proposed to prevent both internal and external threat in the healthcare framework. To guarantee security on health care records access control approach is required. In this paper different access control mechanisms used to provide security on Personal Health Records.***

Key words: Electronic Health Record, Cloud Storage, Access Control.

I. INTRODUCTION

The emergence of cloud has drawn large attention of healthcare industry to store patient information on cloud storage. Records in health industries are extremely sensitive; therefore require a level of security and privacy when stored on cloud storage and during sharing of those records. The security as well as the privacy of the sensitive health records is the major challenges that prevent the adoption of cloud storage in the health care industries. To prevent unauthorized Access to the health records the user will have to be authenticated to get access to the record.

Access control Mechanism prevents different users from getting access to the records in the cloud storage and provide access to only authorized users. Access control models differs in terms of type of authorization used, process in decision making, security and different other purpose of implementation. This paper study Attribute Based Encryption Schemes (ABE) used to address security and privacy issues in Health care cloud storage.

Challenges in adopting Cloud Storage by Health Industries

- The major concern of the health industries is the Privacy and Security of the sensitive patient information.
- Lack of mechanism provided on cloud for encryption may lead to access to the original patient data.
- The high risk of storing sensitive data on outsourced cloud storage.
- Traditional role based system failed to guarantee security to data on cloud.

Revised Manuscript Received on January 24, 2020.
* Correspondence Author
M. Vignesh*, Department of CSE, SRM Institute of Science and Technology, Chennai, Tamil Nadu, India.
Dr. R. Naresh, Department of CSE, SRM Institute of Science and Technology, Chennai, Tamil Nadu, India.

I. CLOUD COMPUTING ARCHITECTURE

Cloud architecture consists of front end and backend. The frontend are the client applications that are used to access the components of the backend. The backend consist of the servers, storage, networks that are provisioned to clients on demand to run their applications and store data.[15]

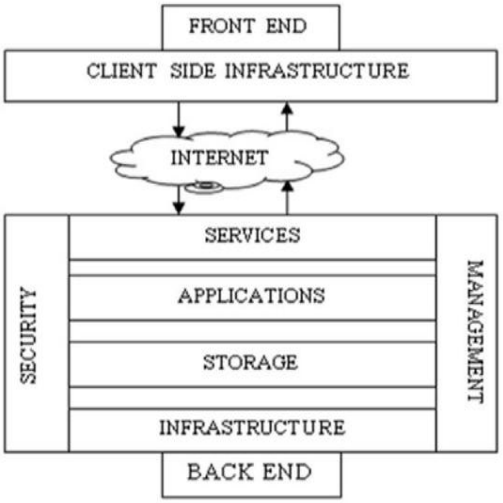


Figure 1: Cloud Architecture

II. ATTRIBUTE BASED ENCRYPTION

ABE is a public key (PK) encryption scheme in which the secret key (SK) of the file or data user and the cipher text (E) are dependent on the user attributes. Attribute based encryption is divided into Key Policy Attribute based encryption (KP ABE) and cipher text Attribute based Encryption (CP ABE.

In Attribute Based Encryption (ABE) Scheme both the SK of the user and the cipher text are associated with some attributes collection. User can only decrypt the cipher text if and only if at least a threshold number of attributes of the user overlap the cipher text and the SK of the user. ABE differs from the one-to-one encryption schemes like Identity based Encryption, where it is implemented for many users.

a. Key Policy ABE

In KP ABE data sender use a collection of attributes to labels cipher. A trusted authority issues private key of the user from an access structure that specifies the type of cipher text that can be decrypted. The KP ABE is suitable for organizations with hierarchies that specify which file is accessible by which user. The KP ABE consist of the following algorithms

Setup Algorithm: the setup algorithm receives as input a K and output the PK and MK, the sender use the public key to encrypt the message. Master Key generates a new user SK which is known to none except the authority.

Encryption Algorithm*:* The encryption algorithm takes in as input a Plain Text M, PK, and attributes collection and output a cipher text E.

Key Generation Algorithm: The key generation step accept as input the structure T and MK and give as output a SK used to decrypt M encrypted based on the collection of attributes only if it matches the access structure T.

Decryption Algorithm*:* it receives SK of the user for access structure and E encrypted under collection of attributes and output the original message if and only if the set of attribute matches Structure T.

b. Cipher-Text Policy ABE

In CP ABE Scheme a data sender encrypt message using traditional encryption scheme. An access policy is specified in form of access structure over attributes in the cipher-text. The access structure specifies users that are capable of accessing the cipher-text. The users decrypt the cipher-text if only their attributes matches the access policy associated to the encrypted data. The following algorithms are included in CP ABE

Setup Algorithm: the setup algorithm receives in as input K and output the PK and MK, the sender use the public key to encrypt the message. Master Key generates the user SK which is known by the authority.

Algorithm for the Encryption: The encryption algorithm takes in as input, Plain Text M, PK, an access structure and output a cipher text E.

Key Generation Algorithm: the key generation algorithm receive in as input attribute of the user and the MSK and output a SK that can be used to obtain the message from the encrypted data based on the structure T used for access if and only if there is matching in the access structure T.

Decrypt Algorithm: The algorithm for the decryption of the encrypted data takes the cipher-text and a SK for the set of attributes and generate the actual data if and only if matching with the structure for access.

c. Cipher-text Policy Attribute-Set Based Encryption (CPASBE)

Decryption of cipher-text here depends on the user attribute which are logically organized as a single collection of attributes. Possible combinations of the attributes may be used by the user to satisfy the policy.

The CPASBE scheme was introduced to address the problem of CP-ABE. CP-ASBE extend the CP-ABE scheme by organizing the attributes as a repetitive collection of structure and allow the user to enforce some constraints on how the attribute set can be combined to satisfy the access structure.

d. Identity Based Encryption (IBE)

In IBE Scheme a message is encrypted using the identity of the user. The sender of the message who has access to the public parameters possessed by entire system encrypts the message using the identity attribute of the user as the key.

e. Hierarchical Identity Based Encryption (HIBE)

In HIDE the PKG which is the root allocate workload through assigning private key generation and authentication of the identities to the PKG at the lower level. The root PKG generates PK for the PKGs at the Domain Level only, which also in turn generates PK to users within domains at the subsequent level. Authentications as well as private key transmission are locally done.

f. Hierarchical Attribute-Base Encryption (HABE)

Hierarchical Encryption was designed to acquire a FGAC in cloud. This scheme combines the CP ABE and HIBE scheme [4].

g. Hierarchical Attribute Set Based Encryption (HASBE)

The issue of multiple keys assignment in HABE leads to the introduction of HASBE by *Zhiguo Wan*. in this scheme a delegation algorithm is applied to construct various hierarchical access structures for the owner's data during encryption. it functions as a repetitive set-based property to prevent the client data stored in the cloud. The owner of the stored data adds or removes user privileges from the set. The Domain Authority (DM) manages all users in this scheme [10]

Table 1: Overview of Various ABE Schemes

Encryption Scheme	Sub Encryption Schemes	Advantages of the Scheme	Disadvantages of the Scheme
Identity based encryption	Identity based encryption	- Easy to implement. - Less complexity in encryption and decryption. - Does not require certificates, user registration and key revocation - The key expires with time	- Require a centralized Private Key generator. - PK generator trust is needed. - All public and master keys are stored by the master - The entire system depends on the key generator. - Online centralized unit. - Does not resist collision - Lot of communication overhead.

Attribute based Encryption (ABE)	Attribute based Encryption	- More flexible and FGAC than ABE schemes. - It have a lesser over head due to communication when compared with other schemes that are not ABE - It has a mechanism for collision resistance	- at the time of decryption the system will need the entire public key in possession of the users authorized to gain access to the data - The system entirely depends on the key generator
KP ABE	KP ABE	- Fine-grained access control - Provide key revocation due to more control over users - Suitable when used for communications between on user at one end and many users at the other end.	- The greatest challenge in the scheme is the issue related to trust depending on the key allocator - Lack of control on who can decrypt cipher-text.
Ciphertext Policy Attribute-Based Encryption (CP-ABE)	Ciphertext-Policy Attribute-Based Encryption (CP-ABE)	- Overcomes the issue in KP ABE. - It operates in reverse order of KP-ABE. - An untrusted cloud storage is used to store the user records. - It is more suitable for use in actual Applications within the environments. - The model of access control here is based on RBAC and more complex. - It is capable of specifying the users that can decrypt the encrypted version of the file.	- Attributes can be combined to bypass the scheme. - CA has full authorities which can be misused.. - Lack of adaptability and proficiency. - The attributes required for decryption can be reshuffled by the users and may satisfy the access policy to retrieve the actual content.
	CP WABE	- It is more suitable for use in actual Applications within the environments - Fine-Grained Access Control. - All attributes involved are not treated in the same level. - Attributes Weight represent its significance within the system.	- High computation cost due to large size of cipher-ext. - No control over who can decrypt cipher-text. .
	CP- ASBE	- The structure used to access the decrypted file is based on a large and strong collection of attributes of the private key of the authorized Users - Attribute collision absent. - Additional attributes can be added to the encrypted file by the owner. - Access structure of the encrypted data is not monolithic.	- It is practically difficult to generate a composite attributes as user key - Collision is very difficult to prevent in this scheme - Useless attribute included and contained in the encrypted data. - excessive computation in encryption of record
H-ABE	H-ABE	- Proposed for enterprise environment. - Combines features of ABE and HIBE - Multiple Authorities are supported. - Provide FGAC and scalability. - Hierarchical structure is used in generation of key. - Short start-up time.	- Implementation is very difficult as entire attributes form a single clause.. - The system possesses multiple authorities which result in complexity in management. - the overhead due to excessive computation is directly proportional to variation in authorities - Confidentiality issue as CA Manages entire keys - Trust issue problem with system as CA has ability to decrypt all cipher-text.
	Hierarchical Attribute Set-Based Encryption (HASBE)	- Improved version of H-ABE. - HIBE and ASBE features are possessed by this scheme. - Access structure used has some hierarchy. - Attributes associated with user have repetitions - Attributes about the user can be multi value. - Domain Authority (DM) manages all users in the system.	- The structure used is complex - Query to verify the access policy leads to high time of execution. - Performance of the system is drastically reduced. - Absence of authority in the lower level leads to stoppage of the entire process for all attached authorities.

Table 2: Summarization of Various ABE Schemes and Parameters Used

Proposed Scheme	Method Used	Parameters	Future Work	Simulation Tools
Ciphertext-Policy Attribute-Based Encryption With Delegated Equality Test [12]	Bilinear pairing and ViJete's formulas and Concrete Construction	Access policies, cipher-text of equal size and cloud server for equality test, public parameter, secret key, list of attributes	To develop a CP ABE with a test for equality that will obtained a security level as in IND-CCA2 Model	CP ABE toolkit & (PBC) library

Ciphertext-PolicyWeighted Attribute Based Encryption for Fine-Grained Access Control [13]	Weighted Attribute	weighted access structure, user attributes, weights	To design a CP-WABE scheme that will efficiently revocation attributes in different weight	Not Specified
Conditional CPABE Encryption Scheme in Vehicular Cloud[11]	Conditional Ciphertext-Policy Attribute-Based Encryption	Additional Access Tree, Cipher-text, user attributes.	No future work	CPABE toolkit
Weighted attribute data Sharing in cloud computing[14]	Weighted Attribute Encryption	User space, user attributes, user key protocol	No future work	Not specified
An Efficient Key-Policy Fixed Cipher-text Size[10]	Key Policy Attribute Based Encryption	Access Policy, Cipher-text	to construct a KP-ABE scheme that will have cipher-text size as well as a constant private key size.	Not Specified
Data sharing strategy in cloud using ABE[9]	ABE	Unique Key	No future work	Real Cloud Environment
ABE for Securing PHR on Cloud[7]	Attribute Based Encryption Scheme	Unique Password, Cipher-text.	No future work	Real cloud environment
Secure of PHR shared in cloud using CP ABE[8]	AES and ABE	User attributes and AES key	To consider ABE systems with various expressibility	Real Cloud Environment

III. ABE METHODS FOR SECURING PERSONAL HEALTH RECORDS IN CLOUD

ABE for Securing Personal Health Record on Cloud: the system provides an interface for PHR, Doctor Database and other authorities' database. Based on requirement, the admin and central authority map patients to doctors. An auto generated password is sent to the mail of the doctor and the patient. The central admin approves access and the doctor access the patient records

IV. RESULTS AND DISCUSSION

Table 1: Comparison of Encryption Time

Number of Attributes	ABESPHR	Previous Method
10	8	10
20	16	20
30	24	30
40	32	40
50	38	50

Table 2: Comparison of Decryption Time

Number of Attributes	ABESPHR	Previous Method
10	0.05	0.08
20	0.11	0.16
30	0.18	0.24
40	0.25	0.32
50	0.3	0.4

Figure 1 shows the comparison of the encryption time of ABESPHR and the previous methods and figure 2 shows the comparison of the decryption time of ABESPHR and the previous methods.

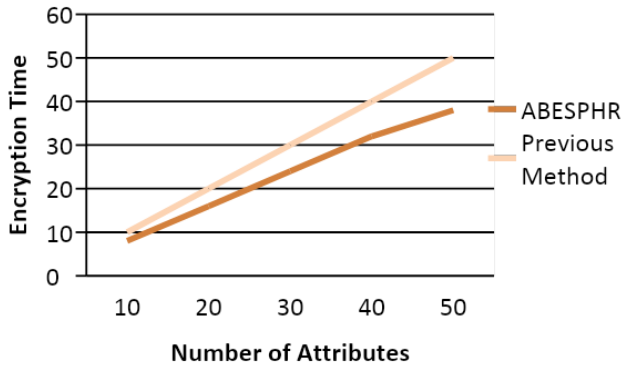
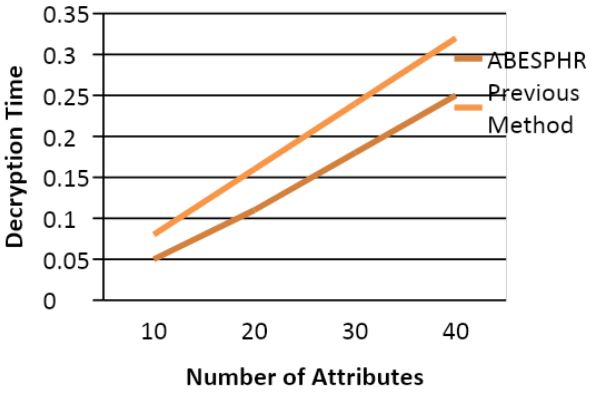


Figure 1: Comparison of Encryption Time



V. CONCLUSION

The security of the health care records is the major concern in health industries. In this paper we overviewed various attribute based encryption techniques that could be used to provide a secure and fine grain access control over health records in cloud storage.

REFERENCES

1. Wang, C., & Luo, J. (2013). An Efficient Key-Policy Attribute-Based Encryption Scheme with Constant Ciphertext Length. *Mathematical Problems in Engineering*, *2013*, 1–7. doi: 10.1155/2013/810969
2. Joshi, M., Joshi, K., & Finin, T. (2018). Attribute Based Encryption for Secure Access to Cloud Based EHR Systems. *2018 IEEE 11th International Conference on Cloud Computing (CLOUD)*. doi: 10.1109/cloud.2018.00139
3. Ravi Mitra Reddy. L & Harsha B. R. (2013) File Access Control through Access Tree and ABE in Cloud: A Survey. International Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181
4. Saravana Kumar N, Rajya Lakshmi G.V, & Balamurugan B (2014). Enhanced Attribute Based Encryption for Cloud Computing. Procedia Computer Science International Conference on Information and Communication Technologies (ICICT 2014)
5. Anup R. Nimje, V. T. Gaikwad, H. N. Datir.(2013) Attribute-Based Encryption Techniques in CloudComputing Security : An Overview. International Journal of Computer Trends and Technology- volume 4 Issue 3
6. Mhatre, S., Nimkar, A. V., & Dhage, S. N. (2017). Comparative study on attribute-based encryption for health records in cloud storage. *2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT)*. doi: 10.1109/rteict.2017.8256677
7. Gondkar, D. A., & Kadam, V. S. (2014). Attribute based encryption for securing personal health record on cloud. *2014 2nd International Conference on Devices, Circuits and Systems (ICDCS)*. doi: 10.1109/icdcsyst.2014.6926174
8. Benamara, M. A., & Li, H. (2015). Secure of personal health records shared in cloud computing using cipher-text attribute based encryption. *International Journal of Security and Networks*, *10*(3), 183. doi: 10.1504/ijsn.2015.071833
9. Deepanshu Mohan, Sayyed Wahid Rabbani & R. Mangalagowri (2018). Data Sharing Strategy in Cloud Computing Using Attribute Based Encryption. International Journal of Pure and Applied Mathematics ISSN: 1314-3395
10. Wang, C., & Luo, J. (2013). An Efficient Key-Policy Attribute-Based Encryption Scheme with Constant Ciphertext Length. *Mathematical Problems in Engineering*, *2013*, 1–7. doi: 10.1155/2013/810969
11. Guan, Z., Li, J., Zhang, Z., & Zhu, L. (2016). Conditional Ciphertext-Policy Attribute-Based Encryption Scheme in Vehicular Cloud Computing. *Mobile Information Systems*, *2016*, 1–10. doi: 10.1155/2016/1493290
12. Wang, Q., Peng, L., Xiong, H., Sun, J., & Qin, Z. (2018). Ciphertext-Policy Attribute-Based Encryption With Delegated Equality Test in Cloud Computing. *IEEE Access*, *6*, 760–771. doi: 10.1109/access.2017.2775741
13. Liu, X., Ma, J., Xiong, J., Li, Q., & Ma, J. (2013). Ciphertext-Policy Weighted Attribute Based Encryption for Fine-Grained Access Control. *2013 5th International Conference on Intelligent Networking and Collaborative Systems*. doi: 10.1109/incos.2013.18
14. T. Shashank & Vijay Kumar (2018). Weighted Attribute Data Sharing in Cloud Computing. International Journal of Pure and Applied Mathematics. ISSN: 1314-3395
15. Wadhonkar, A., & Theng, D. (2016). A survey on different scheduling algorithms in cloud computing. *2016 2nd International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics (AEEICB)*. doi: 10.1109/aeeicb.2016.7538374
16. Deepali A. Gondkar & V.S. Kadam (2014). *Attribute Based Encryption for Securing Personal Health Record on Cloud.* 2014 2nd International Conference on Devices, Circuits and Systems (ICDCS).

AUTHORS PROFILE

M. Vignesh pursuing M.Tech in Computer Science and Engineering, SRM Institute Of Science and Technology, Chennai, Tamil Nadu, India.

Dr. R. Naresh Associate professor, Department of Computer Science and Engineering, SRM Institute Of Science and Technology, Chennai, Tamil Nadu, India.