Attribute based encryption for secure sharing of E-health data

IOP Conf. Series: Materials Science and Engineering **263** (2017) 042030 doi:10.1088/1757-899X/263/4/042030

Attribute based encryption for secure sharing of E-health data

Charanya R, Nithya S and Manikandan N
School of Information Technology and Engineering, VIT University, Vellore-632014, Tamil Nadu, India.

E-mail: charanyame@gmail.com[1]

Abstract Distributed computing is one of the developing innovations in IT part and information security assumes a real part. It includes sending gathering of remote server and programming that permit the unified information and online access to PC administrations. Distributed computing depends on offering of asset among different clients are additionally progressively reallocated on interest. Cloud computing is a revolutionary computing paradigm which enables flexible, on-demand and low-cost usage of computing resources.

The reasons for security and protection issues, which rise on the grounds that the health information possessed by distinctive clients are put away in some cloud servers rather than under their own particular control". To deal with security problems, various schemes based on the Attribute-Based Encryption have been proposed. In this paper, in order to make ehealth data's more secure we use multi party in cloud computing system. Where the health data is encrypted using attributes and key policy. And the user with a particular attribute and key policy alone will be able to decrypt the health data after it is verified by "key distribution centre" and the "secure data distributor". This technique can be used in medical field for secure storage of patient details and limiting to particular doctor access. To make data's scalable secure we need to encrypt the health data before outsourcing.

.

1. **Introduction**

Cloud computing gives various focal points to both end clients and business. "Security and protection is the significant issues in cloud. Distributed computing gives proficient utilization of information product house and availability of IT assets to diverse clients in view of their needs. To keep up information's and application cloud utilizes remote server and web. With no establishment distributed computing permits its clients to get to information. Cloud computing is becoming popular because network complexity is reduced and the users need not buy any licensed software and to access the ehealth data from cloud users do not require any applications or interface and also provides multi tenant sharing of services. Cloud computing innovation brings about enormous expense decrease to IT divisions yet information accessibility, information security, information security are the significant issues which is solved in this paper".

There are four models of cloud computing

- Infrastructure as a Service
- Platform as a Service

- Software as a Service
- Network as a Service

Cloud gives mechanized reinforcement instrument. Cloud is the major storage region for both open and private data's. "Since delicate and classified data's are put away in cloud server it is vital to give information privacy. The public key along with the attribute policy is distributed among the group members who join the system. Based on attribute encryption technique the user can decrypt the health data only if the identity is similar to the policy of the encrypter[15,16]. The user send his public key along with his identity to the key distribution centre to generate the private key based on attribute based encryption[7]. To make cloud health data more secure we have used multiparty (or) multi users. Secure authority is the second level where the user and the KDC send keys to secure authority and if only both the key matches the user is able to decrypt the data".

2. Problem Statement

"Besides the several benefits of cloud computing, there are lots of issues to the users. One of the most challenging issue in the cloud computing is the security between the provider and the users.

2.1. Location of Data

Various associations situated in better places have diverse needs and controls set on access. Since the health information is in the cloud, one may not understand that the health information must live in a physical area. The cloud supplier ought to give the level of security needed for diverse clients and their needs.

2.2. Access to data

Access control is a key concern, in light of the fact that insider attacks are a huge danger. A potential programmer is somebody who has been depended with affirmed access to the cloud. Anybody utilizing the cloud need to take a look at who is dealing with their information and what sorts of controls are connected to these people.

2.3. Service level agreement (SLA) terms

Organizations need to guarantee the security and trustworthiness of their information, notwithstanding when it is held by administration giving the cloud. They likewise need to demonstrate similarity with security models paying little heed to the areas of their information and applications.

2.4. Authentication and authorization

Every organization has its own way to manage authentication and authorization Security concerns based on delivery and deployment models are data integrity, data locality, data confidentiality, and data access. Some more security related concerns are Sign on process, Authentication & authorization, network security, identity management and especially multi-factor[13] authentication which considers multiple factors together for authenticating a user".

3. Existing System

In the IBE[7], "the sender of a message can indicate a identity such that just a recipient with coordinating personality can decrypt it. This is not the same as Public-key Encryption, in that the encrypter does not have to issue additional key to decode for every figure content. In the IBE, the

private key, which contains the identity of the holder, is distributed to each client just once when he joins the framework.

The information proprietor encodes the information's in cloud with specific encryption approach and stipend access to the clients with specific particular parts[17]. There are particular situated of parts and to which the clients are relegated and every part has set of assigned permission. Just the client with a specific part will have the capacity to unscramble the information's even the cloud supplier are denied to get to.

In attribute based technique [1,2,10,11] instead of encrypting to a single user and to provide advance data sharing attribute based encryption technique. The authority generates keys according to attributes; and these attributes of public key and master key, which are generated by the authority, should predefine (means that it will list attributes which will be used in the future)[3]. If any data user who wants to add to this system, and he owns to attributes don't include predefined attributes. The authority will re-define attributes and generate a public key and master key again. And data owner's role in this scheme is to encrypt data with a public key and a set of descriptive attributes. A data user's role is to decrypt encrypted data with his private key sent from the authority, and then he can obtain the needed data".

Data access control is an effective way to ensure data security in cloud [4]. The cloud server cannot be fully trusted to provide data access control service, which means existing server-based access control methods are no longer applicable to cloud storage systems. To achieve data access control on untrusted servers, traditional methods usually encrypt the data and only users holding valid keys are able to decrypt. Ciphertext-Policy Attribute-based Encryption (CP-ABE) is regarded as one of the most suitable technologies for data access control in cloud storage systems. In this technique each user will be issued a secret key according to its attributes. A user can decrypt the ciphertexts only when its attributes satisfy the access policies.

Health care services allows a patient to create, manage, and control their personal health data in one place through the web, which has made the storage, retrieval, and sharing of the medical information more efficient. Each patient has the full control of their own medical records and can share health data with a wide range of users[8,9], including healthcare providers, family members or friends". While it is exciting to have convenient PHR services for everyone, there are many security and privacy risks[8].

4 Design Goals

4.1 In Identity based encryption

The data's encrypted with identity policy can be decrypted only if the identity policy is satisfied. For example: "If Alice wants to send a message to bob he encrypts it with bobs mail id. When he receives the mail he himself authenticates his private key and decrypt the message. So when some hacker is using bobs mail id he will be able to decrypt data's easily. So this requires a secure channel between the sender and the receiver and IBE server for transmitting the private key.

4.2 Key-policy

Its used to achieve fine–grained access control. Health Data's are encrypted with dummy attribute which the cloud don't know. And the user with all such attribute will be able to decrypt the data. So encryptor cannot decide a particular decryptor who can decrypt the message.

4.3 In Ciphertext-policy

In Ciphertext-policy even if the storage server is untrusted data can be made confidential. Attribute determine user credentials and the owners determine who can decrypt the data. The user posses a set of attribute and get a secret from the authority only such user will be able to decrypt the data's. The advantage of this technique is the user can use all the possible attributes only once to decrypt the data with the generated secret key [12,14].

4.4 In Role-based attribute encryption

The user with a particular role will be able to access the health data even if the cloud provider deny their access. Drawback of this is an efficient cryptographic method is required for ordering the keys".

4.5 In Multi authority technique

Central authority and multi attribute authority is present which distributes the private attribute key. Since there are multi authority[5,6] each do not know who is issuing the key and there is a problem of collision. And CA will be able to decrypt the confidential health data.

5. Proposed Methodology

Security issues are all solved in the CP-ABE. "In the CP-ABE, ciphertext are created with an access structure, which specifies the encryption policy, and private keys are generated according to users' attributes and identity. A user can decrypt the ciphertext if only his attributes in the private key satisfy the access tree specified in the ciphertext. By doing so, the encrypter holds the ultimate authority about the encryption policy. Also, the already issued private keys will never be modified unless the whole system crashes. In this paper we have introduced a multi-authority system, where each user has an ID and they can interact with each key generator (authority) using different pseudonyms". In this multi authority technique cloud server does proxy re-encryption to enhance cloud security.

5.1 System Model

- *Data Owner*

The data owner encrypt the health data to the cloud along with the public key got from any of the authority and with some attribute policy (Figure 1).

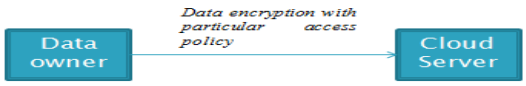

Figure 1: Encryption

- *Data Consumer*

Newly joined data consumer request for the public key and they do not know which attribute are controlled by which authority and same way the authorities do not know which Data Consumer is interacting with them.

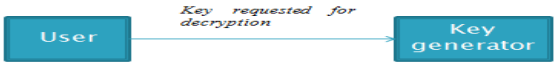

Figure 2: Decryption

- *Encryption*

Encryption process takes secret key (SK) as input, "a message and a set of privilege tree {TP}pϵ{0,....r-1}, where r is determined by the encryptor (Figure1). This will encrypt message M and return a cipher text (CT) and a verification set VR so that a user can execute specific operation if only the attribute satisfy the corresponding key policy.

For encryption we have also used SHA3 algorithm. A hash function is used to compress the data. The Init() function prepares the internal state for given hash size (n) and attribute (S).

The update function starts compression phase. In this phase the message text (M) is combined with internal state with (N) size bit. Final function starts the extraction or sqeeze phase(figure 3). The message from the initial state are extracted to form hash value". The first n bits are the hash value of the encrypted data and others are the error result.

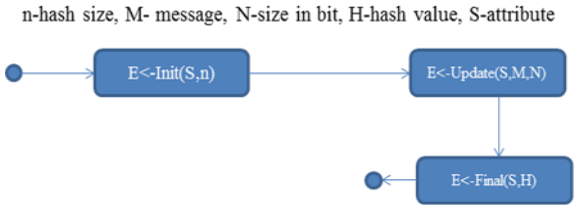

Figure 3: Encryption Process

- *Key Generator*

The Key Generation algorithm enables a user to interact with every attribute authority, and obtains a public key corresponding to the input attribute set Au and his global ID, Which is verified with the data owner and then generated in the form of OTP(Figure 4).

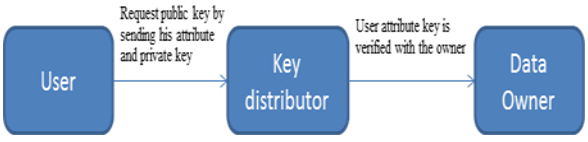

Figure 4:Key Generator

- *Proxy re-encryption*

The public key is used for all operations within the system, and the master keys are used by each attribute authority when he generates keys for Data Consumers. Once the user is authorized proxy re-

encryption server re-encrypt the encrypted data and sent it to secure data distributor. From where the user can decrypt the data by using the public key generated as the OTP.

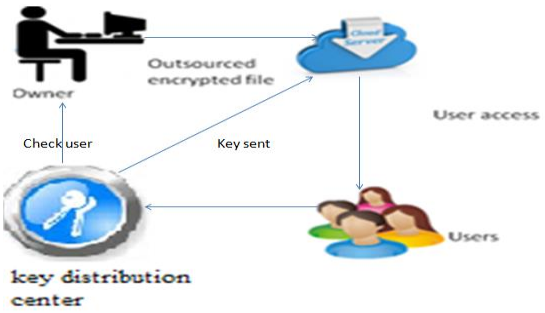

Figure 5 : System design

6. Comparison

The multi-authority cipher text strategy property based encryption plans are more expressive than the multi-authority key approach quality based encryption plans. "On the other hand, the usage unpredictability of multi ciphertext approach characteristic based plans are higher than the multi-authority key arrangement quality based plans. Little Universe MA-ABE plans: MA-ABE plans use polynomial size property universe in the security parameter. Expansive Universe MA-ABE plans: MA-ABE plans use exponential size quality universe in the security parameter. Expressiveness of the MA-ABE plans can be expanded by the system for vast universe development and the other way around. Productivity of the MA-ABE plans diminishes extensively with the utilization of huge universe development and the other way around. Substantial universe MA-ABE plans can be developed from little universe ones with the utilization of a hash function".

Table 1: Comparision between CP-ABE and KP-ABE

	MA-ABE Techniques/ Parameters	*Adaptively Secure*	*Standard Model*	*Prevent Decryption by Individual Authorities*	*Support Large Attribute Universe*	*Expressiveness*
Key policy attribute based encryption schemes	Multi-authority Attribute Based Encryption	No	Yes	No	Yes	Limited
	CA-less multi-authority anonymous ABE	No	Yes	Yes	Yes	Limited
Ciphertext policy attribute based encryption schemes	Distributed Attribute Based Encryption	No	Yes	No	Yes	Expressive
	Decentralized Attribute Based Encryption	Yes	No	Partially	No	Expressive

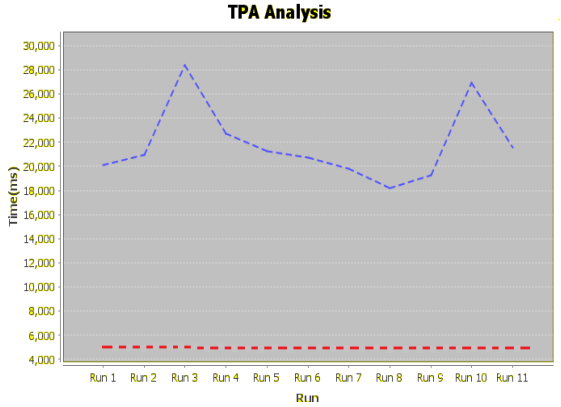

Figure 6: Comparision

7. Conclusion

We have proposed a multi party attribute based encryption technique to overcome the security issues. We first have designed CP-ABE technique to store data in cloud, but it has not fully satisfied the security issues so we have made a proxy re-encryption technique to make data more secure and difficult for unauthorised users to access data. By using multi party technique first attribute and key is passed to get the secret key and re-encryption is done with the public key, So the data can be decrypted with the OTP pin generated. The analysis shows that our work is more secure, scalable and efficient.

References

[1] Yang Ming, Liu Fan and Han Jing-Li 2011 An Efficient Attribute based Encryption Scheme with Revocation for Outsourced Data Sharing Control , *IEEE International Conference on Computer Comunication and Control* 978-0-7695-4519-6/11 *516- 520.*

[2] Kan Yang and Xiaohua Jia 2012 Attribute-based Access Control for Multi-Authority System in Colud Storage, *32nd IEEE International Conference 536-545.*

[3] Xun Yi, Yuan Miao, Elisa Bertino and Jan Willemson 2013 Multiparty Privacy Protection for Electronic Health Records *IEEE*. 978-1-4799-1353-4/13 2730-2735.

[4] Vijaya Lekshmi and Revathi 2014 Implementing Secure Data Access Control For Multi Authority cloud storage system using ciphertext policy-Attribute based Encryption, o.978-1-4799-3834-6/14/ *IEEE, ICICE*

[5] Yun Wang, Dalei Zhang and Hong Zong 2014 Multi-authority Weighted Attribute Encryption Scheme in cloud Computing, *IEEE International Conference on Natural Computation*. 978-1-4799-5151-2/14 *1033-1038*

[6] Xing Rong, Yong Zhao and Rong Jianh 2014 MMACS: A Multi-Authority cloud access scheme with mixed access structure, ICC'14 - W5: Workshop on Secure Networking and Forensic Computing, 978-1-4799-4640-2/14 706-711.

[7] Manjusha and Ramachandran 2014 Comparative study of Attribute based Encryption Techniqur in Cloud Computing, *IEEE International conference on Embedded systems.* 978-1-4799-5026-3/14 *116-120*

[8] Chen Danwei, Linling, Fan Xiaowei, He Liwen, Pan Su and Hu Ruoxiang 2014 Security Patient-Centric Personal Health Records Sharing System in cloud Computing. *China Communications* **1** 121-127.

[9] Wenhai sun, Shucheng yu, Thomas Hou and Hui Li 2014 Protecting your Right: Attribute – based Keyword search with fine-grained owner-enforced search authentication in cloud, *IEEE conference on Computer Communication. 1187-1198*

[10] M Li, S Yu, Y Zheng, K Ren and W Lou 2013 Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption, *IEEE Transactions on Parallel and Distributed Systems* **24** 131–143.
[11] Junbeom Hur 2013 Improving security and efficiency in attribute-based data sharing, *IEEE Transactions on Knowledge and Data Engineering* **25** 2271-2282.
[12] Ximeng Liu, Jianfeng Ma, Jinbo Xiong, Qi Li and Tao Zhang 2013 Ciphertext- Policy Weighted Attribute Based Encryption Scheme, *Journal of Xi'an Jiaotong University* **47** 44-48.
[13] Jung T, Mao X, Li X, Tang S, Gong S and Zhang L 2013 Privacy preserving data aggregation without secure channel: multivariate polynomial evaluation, in *IEEE INFOCOM*.
[14] C Wang, X Liu, and W Li 2013 Design and implementation of a secure cloud-based personal health record system using ciphertext-policy attribute-based encryption, *International Journal of Intelligent Information and Database Systems* **7** 389–399.
[15] Charanya R, Aramudhan M, Mohan K and Nithya S 2013 Levels of Security Issues in Cloud Computing, *International Journal of Engineering and Technology* **5(2)** 1912- 1920.
[16] Charanya R, Aramudhan M and Saravananguru Ra K 2016 A Review on Access Control Issues in Ehealth Application in Cloud Computing, *Indian Journal of Science and Technology* **9(42)** 1-5.
[17] Charanya R and Aramudhan M 2016 Survey on Access Control Issue in Cloud Computing, *IEEE International Conference*, 978-1-4673-6725-7/16 237 -240.