ISSN: 0975-766X
CODEN: IJPTFI
Available Online through *Research Article*
www.ijptonline.com

ATTRIBUTE BASED ENCRYPTION AND DECRYPTION OF MEDICAL RECORDS

Ankit Raj Saxena, SCOPE, VIT University
Dr.Swarnalatha P., Associate Professor, SCOPE, VIT University, Chennai.
Email: ankitrajsaxena@yahoo.com

Received on: 15.10.2016 *Accepted on: 12.11.2016*

Abstract

In hospitals, attributes such as patient Name, Address, Identification number describe patient's credentials and helps us to describe who can decrypt data from the server. Many researchers have been conducted in Personal Health as well as medical Records (PHR) to facilitate the mediation and direct connection of patient to different users (doctors with certain specialization, physicians, family members and clinic agents) through network. Attribute-based Encryption mechanism is used to determine the accessibility of this sensitive PHR documents. In this paper, with encrypted information and Constant Computation-Cost is used to describe patient's credentials, and a patient associate encrypted data with credentials that can determine which user can decrypt sensitive medical records from the server. Due to the large number involved in the access policy scheme this work is based on encryption and Constant Computation- cost.

Keywords: Attribute based Encryption(ABE), Decryption, Blowfish Algorithm, Personal Health Records (PHR), Cipher Text (CT), Secret key (MK).

1. Introduction:

In this decade of new technology, many people can access online data and it offers many advantages to patients because they can access their own electronic health records and have full control to them. A Personal Health Records In hospitals, attributes such as patient Name, Address, Identification number describe patient's credentials and helps us to describe who can decrypt data from the server. Many researchers have been conducted in Personal Health as well as medical Records (PHR) to facilitate the mediation and direct connection of patient to different users (doctors with certain specialization, physicians, family members and clinic agents) through network. Attribute-based Encryption mechanism is used to determine the accessibility of this sensitive PHR documents. In this paper, with encrypted information and Constant Computation-Cost is used to describe patient's credentials, and a patient associate encrypted data with

credentials that can determine which user can decrypt sensitive medical records from the server. Due to the large number involved in the access policy scheme this work is based on encryption and Constant Computation- cost.

Attribute-based encryption provides good solutions to the rectification of any anonymous access or breach control by defining access policies among private keys or over encrypted data and information. Usually, the users are identified by set of attributes such as gender, age, company, profession, experience etc. According to an Attribute Based Encrypted system by encrypting data can specify access to the data as function over a set of attributes specified. ABE is defined with two different complementary notions; one is Key- Policy Attribute Based Encryption, where a text when associated to a list of attributes, a secret key is associated to a policy for decryption, and the second is Policy of Attribute Based Encryption, where secret keys are associated to a list of attributes and given text is associated to certain amount of registered policies for decryption. Therefore, many applications found that Attribute Based Encryption is more useful and applicable than Attribute Based Encryption. In PHR each patient or a user in the system will be issued a private key from an authority that reflects their attributes. A user will be able to decrypt a text if the attributes associated with their private key satisfy the given registered access policy prescribed to the text. In Attribute Based Encryption, the size of a text depends on the number of attributes involved in the specific given method for that text.

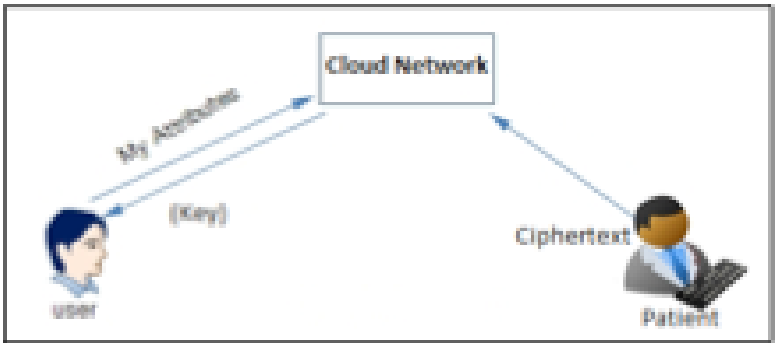

Figure1: Representation of three-level system of PHR document sharing.

2. Literature Review:

Previously there has been attribute based methods which encrypt and decrypt the information using r text policy. There various attributes like patient name, patient id, symptoms, age and date of birth. Using this system helps a lot as it can give the permissions to modify the sensible data and information. But there can be other factors like cost which can be considered as drawbacks. Our method has an effective way of dealing with the drawbacks as it is cost effective. There are some other methods which store the data and has a key supplied with it. This can be used to encrypt data and then

while decryption, the same key is used to decrypt the encrypted data to make it accessible. This method carries a public key which is quite insecure. There is also a concept of given key encryption method which has the given key safe and secured and data is sent to decryption by sending public key and it then receives an acknowledgement. Then the server sends the private key which is actually used for encryption. This way of encryption is secure as there can be the process of acknowledgement before sending the actual key to the client which requests the data from the server.

3. Description of Proposed Framework:

Algorithmforblowfishencryption

1 Symmetric block cipher is considered.

2 Blocks are used which is in form of bits and here its 64-bit Block.

3 Variable-length key, from 32 bit (4 Bytes) to 448 bit (56 Bytes).

4 We have to run it

5 More suitable and effective for hardware implementation.

6 Patent is not required and no license is required

The algorithm has two parts in it. One is the key encryption part and the other is the extension part. Key expansion converts a key of at most 448 bits into 4168 bytes. There is a A-array and four 32-bit-S-boxes. The A-array contains 18 of 32-bit sub keys, while each S-box contains 256 entries. Data encryption occurs via a round network. Input data from the elements encryption may be illustrated as shown in Figure.

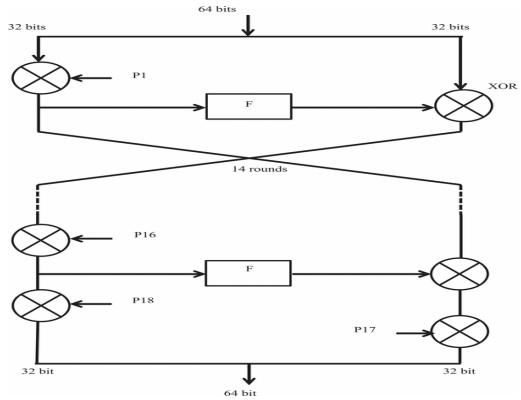

Figure 2: Data Encryption via round network.

How The Algorithm Works:

Start by making sub keys in this followed by attributes 0 through 255 of the first S box, then attributes 0 through 255 of the next S box all the way to attribute 255 of the next in sequence S box with the fractional part of Pi. The most

considerable bit of Pi becomes the most important bit of the first sub key. Consider the key, which may be of any size up to 72 bytes, and, make it to span the entire array of sub keys, XOR it with the sub key array members, Then the part of execution is made that is blowfish with an starting input. After each making, again place the part of the sub attributes or S boxes with the next outputs of Blowfish, in the order which is same as previous and make it key attributes and send it to make the blowfish algorithm work and it takes the box and S is taken from it. This algorithm is very effective to implement and gives a very significant results by implementing it to the above medical records to make encryption possible.

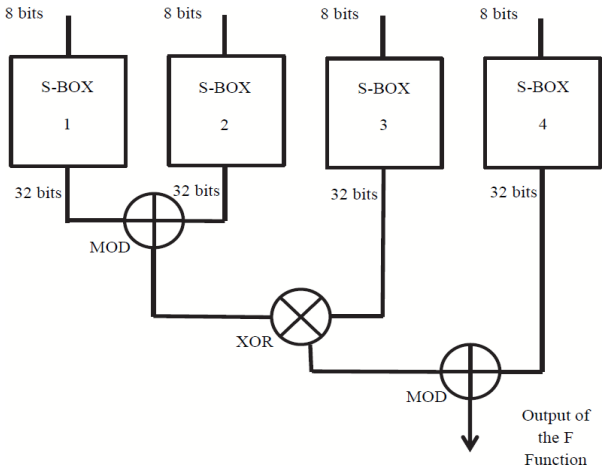

Figure 3: Set of attributes and a subset to represent different types of attributes.

In the above figure a set of attributes and a subset to represent different types such as profession, license status, medical specialty, and affiliation of the user in PHR system. The patient represents the PHR owner with complete authentication and users to represent friends, healthcare providers, family members, and pharmacies.

Let χrepresents a universe, $A_x$is a set of user's data attributes, $ is subset of attributes, P be an access to the given policy. MP and MK represent master key and public key, MK user's secret key. This work refers to the three extensions and bilinear group cited in the above paragraphs. The patient runs the set up algorithm of attribute Based System with constant text-size and computation costs to encrypt data with an access to the policy and will send the data to the registered authenticator and inform them to the trusted party (central server). The users get their secret keys that can be related to their attributes they possess from patient. The patient sends PHR documents to the registered central server and users can read or write when they fulfilled the conditions. Based on the access policy, the user must be responsible to generate secret keys associated with attributes. These secret keys are used to decrypt the plaintext message.

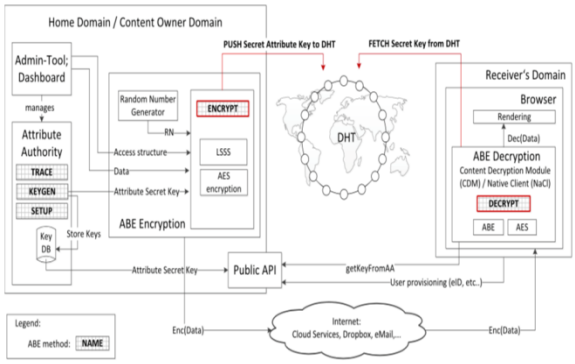

Figure 4: Encryption- Decryption Mechanism.

The user takes input the public parameter, the text CT and the secret key MK contain of user attribute set S. and run the message if attributes in MK satisfy the access policy of CT.

In CP-ABE with constant text-size and computation costs proposal, the size of text and the computation costs in encryption and decryption operations depend on the number of attributes involved in the access policy. This large number of attributes has a great impact on bandwidth in the network. The more the attributes, the slower the network is to access data on the server. Therefore, it is crucial to protect PHR when they are uploaded and stored on large network and to take care of the large number of users who will be connected to the network. This method can be done easily and has more efficiency compared to other methods and algorithms.

4. Application:

From the above data we encrypt the data using blowfish algorithm and then decrypt it to the client when requested.

P_ID	P_Name	P_DOB
1	RYAN	11/01/95
2	ABI	23/04/00
3	YASH	04/02/83
4	ROHAN	05/07/99
5	ANANYA	07/07/72
6	JANE	03/08/96
7	MARK	31/05/94
8	LOGAN	21/07/95
9	PARTH	21/12/95
10	VANSH	11/09/95

Figure 5: Data set for encryption and Decryption.

The result we obtain is what we gave the details in the database and then we use blowfish encryption technique to make it encrypted text. Hence, every value given like name, date of birth is encrypted so that it can be safe and secure which makes it less venerable to attacks like security threats andbreaching and thus makes the information retrieved secure.

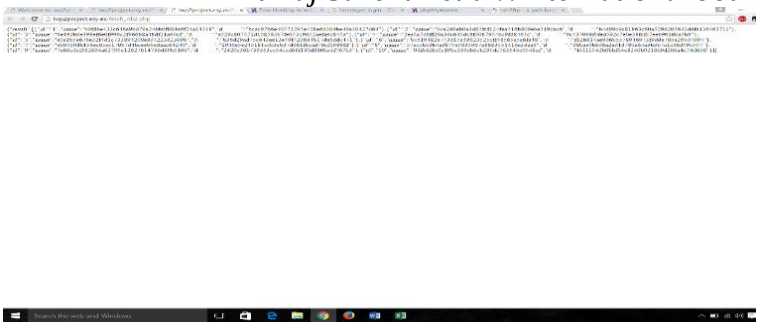

Figure 6: Encrypted data.

Thereafter, once decrypted we get the same data as previous and can retrieve the basic data allotted.

P_ID	P_Name	P_DOB
1	RYAN	11/01/95
2	ABI	23/04/00
3	YASH	04/02/83
4	ROHAN	05/07/99
5	ANANYA	07/07/72
6	JANE	03/08/96
7	MARK	31/05/94
8	LOGAN	21/07/95
9	PARTH	21/12/95
10	VANSH	11/09/95

Figure 7: Decrypted Data.

5. Conclusion:

Therefore, the proposed method has a seamless encryption and decryption between client and server or between two users in the real world environment. This method can be extended to many other industries also other than the discussed health records. It can be applied to automobile industry, automotive industry, petroleum industry and many other such industries. This can be a blow to the security issues as its highly secure. This breakout can be extended to prediction and optimization also using data mining. We can use orange tool to predict the data output from the input provided by users. There can also be machine learning that can be included within as machines on supervised learning predict data fasterwith more accuracy also. Overall view of attribute based encryption and decryption is very much helpful to pull out the drawbacks like cost and security and gives the advantage of seamless flow of data between the permitted users or within a network of users depending on the situation and privacy permissions.

The project also helps giving similar suggestions based on location and can guesstimate the disease taking the input symptoms.

References:

1. "National association of statutory health insurance funds (gkv- spitzenverband)," July 2015. [Online]. Available:https://www.gkv- pitzenverband.de/krankenversicherung/krankenversicherunggrundprinzipien/ allegesetzlichenkrankenkassen/allegesetzlichenkrankenkassen.jsp.
2. P.Dominiczak, "Nearly 1million patients could be having confidential data shared against their wishes," The Telegraph, June 2015. [Online]. Available: http://www.telegraph.co.uk/news/health/news/11655777/ Nearly-1million- patients- could- be- having- confidential- data- shared\
3. D.McCullagh, "Instagram says it now has the right to sell your photos," CNET, December 2012. [Online]. Available: http://www.cnet. com/news/instagram- says- it- now- has- the- right- to- sell- your- photos/
4. "German Federal Data Protection Act (BDSG)." [Online]. Available: http.//www.gesetze-im-internet.de/englisch bdsg/
5. "Basic Law for the Federal Republic of Germany." [Online]. Available: www.gesetze-im-internet.de/englisch gg/
6. A. Shamir, "How to Share a Secret," Commun. ACM, vol. 22, no. 11, pp. 612–613, Nov. 1979. [Online]. Available: http://doi.acm.org/10. 1145/359168.359176
7. G. R. Blakley, "Safeguarding Cryptographic Keys," in Proceedings of the 1979 AFIPS National Computer Conference, vol. 48, Jun. 1979, pp. 313–317.
8. C.Asmuth and J. Bloom, "A Modular Approach to Key Safeguarding,"
9. S. Mu ̈ller, S. Katzenbeisser, and C. Eckert, "Distributed Attribute-Based Encryption," in Information Security and Cryptology - ICISC 2008, ser. Lecture Notes in Computer Science, P. Lee and J. Cheon, Eds. Springer Berlin Heidelberg, 2009, vol. 5461, pp. 20–36. [Online]. Available: http://dx.doi.org/10.1007/978-3-642-00730-9 2
10. R.Petrlic, "Proxy Re-encryption in a Privacy-preserving Cloud Computing DRM Scheme," in Proceedings of the 4th International Conference on Cyberspace Safety and Security, ser. CSS'12. Berlin, Heidelberg: Springer-Verlag, 2012, pp. 194–211. [Online]. Available: http://dx.doi.org/10.1007/978- 3- 642- 35362- 8 16
11. R.Petrlic and C. Sorge, "Privacy-Preserving Digital Rights Management based on Attribute-based Encryption," in NewTechnologies, Mobility and Security (NTMS), 2014 6th International Conference on, March 2014, pp. 1–5.

12. P.Junod and A. Karlov, "An Efficient Public-key Attribute-based Broadcast Encryption Scheme Allowing Arbitrary Access Policies," in Proceedings of the Tenth Annual ACM Workshop on Digital Rights Management, ser. DRM '10. New York, NY, USA: ACM, 2010, pp. 13–24. [Online]. Available: http://dl.acm.org/citation.cfm?id=1866875
13. Q. Huang, Z. Ma, J. Fu, X. Niu, and Y. Yang, "Attribute Based DRM Scheme with Efficient Revocation in Cloud Computing," Journal of Computers, vol. 8, no. 11, pp. 2776–2781, Nov 2013.
14. R.Garg, R. S. Veerubhotla, and A. Saxena, "AtDRM: A DRM Architecture with Rights Transfer and Revocation Capability," in Proceedings of the 6th ACM India Computing Convention, ser. Compute '13. New York, NY, USA: ACM, 2013, pp. 2:1–2:6. [Online]. Available: http://doi.acm.org/10.1145/2522548.2522599
15. ISO, ISO/IEC 23001-7:2015: Information technology – MPEG systems technologies – Part 7: Common encryption in ISO base media file format files. Geneva, Switzerland: International Organization for Standardization, 2015.
16. ISO/IEC 23009-1:2014: Information technology – Dynamic adap- tive streaming over HTTP (DASH) – Part 1: Media presentation description and segment formats. Geneva, Switzerland: International Organization for Standardization, 2014.
17. Z. Liu and D. S. Wong, "Practical Attribute Based Encryption: Traitor Tracing, Revocation, and Large Universe," IACR Cryptology ePrint Archive, 2014, available at https://eprint.iacr.org/2014/616. [Online]. Available: https://eprint.iacr.org/2014/616
18. K. Yang, X. Jia, K. Ren, B. Zhang, and R. Xie, "DAC-MACS: Effective Data Access Control for Multiauthority Cloud Storage Systems," Infor- mation Forensics andSecurity, IEEE Transactions on, vol. 8, no. 11, pp. 1790–1801, Nov 2013.
19. K. Yang and X. Jia, "Expressive, Efficient, and Revocable Data Access Control for Multi-Authority Cloud Storage," Parallel and Distributed Systems, IEEE Transactions on, vol. 25, no. 7, pp. 1735–1744, July 2014.
20. Q. Huang, Z. Ma, Y. Yang, X. Niu, and J. Fu, "Attribute based DRM scheme with dynamic usage control in cloud computing.