ATLANTIS PRESS

Advances in Computer Science Research, volume 86

International Symposium on Communication Engineering & Computer Science (CECS 2018)

Research on an Attribute Based Encryption Method Oriented IHE-XDS

Yanfeng Li [a], Runtong Zhang [b, *]

School of Economics and Management, Beijing Jiao Tong University, Beijing 100044, China.

[a]18811502035@163.com,*, [b]rtzhang@bjtu.edu.cn

Abstract. IHE-XDS (Integrating the Healthcare Cross-Enterprise Document Sharing) is an interagency, involving multiple medical institutions and users, for the integration of medical information sharing framework. The medical information shared by the medical institutions in this framework is mainly electronic medical reports, which is an important part of the patient's diagnosis and treatment record. It plays an important role in clinical diagnosis, scientific research and teaching, and to ensure its safety is the key issues. In the IHE-XDS specification, a role-based access control strategy is proposed to realize the secure access control of information. However, with the continuous development of the open network environment, the number of users is increasing, and the role-based access control is dynamically ex-tended and flexible. In order to achieve more flexible access control, this article presents a method of medical document information security protection oriented IHE-XDS, and designs an access control algorithm, based on cryptographic properties of multi access control algorithm, to allocate minimum privileges to users of different institutions in IHE-XDS, so that the medical information can be safe and flexible to be shared.

Keywords: IHE-XDS, Attribute-Based Encryption (ABE), Encryption algorithm, Privacy protection, Information security.

1. Introduction

Radiological Society of North America (RSNA) and Healthcare Information and Management Systems Society (HIMSS) developed the IHE [1] to build an integrated framework for implementing multiple standards in 1997. The IHE-XDS has been proposed especially for cross-institution medical document exchange. Under the IHE-XDS specification, the medical information of various medical institutions can be shared to the greatest degree, but the safety needs to be guaranteed. IHE-XDS white paper specification adopts role based access control strategy to protect patients' privacy and medical information security. But with the development of the isomer us and diversiform network environment, it is obvious that role-based access control strategy has deficiencies and constraints in dynamic propagation and flexible access [2]. Therefore, multi-access control attribute based encryption algorithm is proposed to achieve maximum security and flexible information sharing.

This article introduces the background of applying multi-access control attribute based encryption algorithm to IHE-XDS in the introduction. The first chapter reviews the literature of IHE-XDS and attribute-based encryption algorithm. The second chapter is the proposal and design of the multi access control attribute based encryption algorithm, and the third chapter carries on the simulation experiment to the algorithm and compares with the role-based access control strategy. The last chapter summarizes the whole paper.

2. Literature Review

IHE-XDS is mainly composed of two parts: actors and transaction. The role of the IHE-XDS is mainly used to identify the patient's id source, document source for XDS document, document repository for storing document information, document registration with index connection, and document user [3]. The role of XDS and its transactional relationship are shown in Figure 1. IHE-XDS mainly consists of a document registry and multiple independent document repositories, which are characterized by distributed information storage and centralized document indexing. The document users use the patient's ID information to request the relevant information from the

document registration, and obtain the inquired document from the corresponding document repository by using the returned information [4].

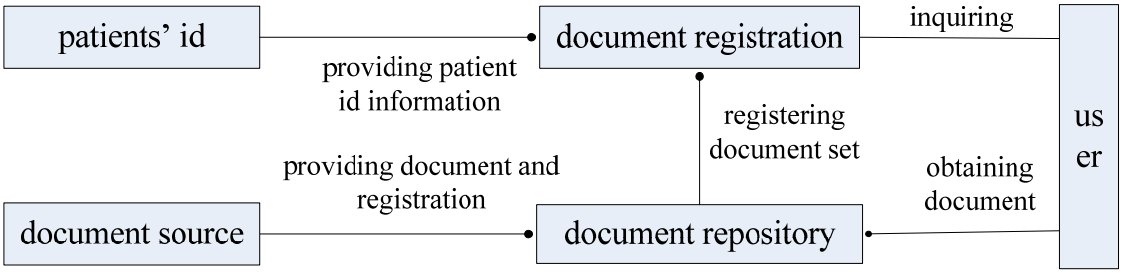

Figure 1. XDS Roles and Transaction Diagrams

In IHE-XDS white paper specification, it uses role based access control to ensure information security. In the role based access control strategy, the user access control authority and the role are associated with the role [5]. Role based access control solves the control problem of access rights in the process of information sharing among users to a certain extent. However, in the network environment with the characteristics of heterogeneity and diversity, the number of users in IHE is increasing and the expansion of large-scale user dynamic needs more flexibility, access control technologies need to be developed in a fine-grained direction, and role-based access control is more restrictive. Attribute based access control strategy can effectively solve fine-grained access control and large-scale user dynamic expansion problems in distributed network environments [6]. Therefore, it is very suitable to apply attribute-based access control policies to IHE-XDS.

Another way of information protection is to encrypt information, combine attribute encryption with attribute based access control strategy, and achieve maximum security in the process of information sharing [7]. Sahai and Waters proposed the concept of attribute encryption using bilinear pairing to associate keys with entity attribute [8]. Goyal divides the attribute encryption into two kinds: key policy attribute based encryption algorithm and cipher-text policy attribute based encryption algorithm [9]. It increases the operation of AND, OR, and Not operations for attributes which makes attribute encryption access control more flexible. Later, Bethencourt et al. proposed to use a tree-like access structure to achieve flexible access control, but its security is just based on the general group hypothesis [10]. In order to implement a policy-based attribute encryption strategy under the assumption of DBDH, Liang et al. proposed a bounded tree structure [11]. Ibraimi et al. removed the limitations of bounded conditions on the basis of Liang, making the access control strategy general [12].

In summary, there are limitations due to role-based access control, and the development and application of attribute encryption algorithms provide new ideas for IHE-XDS security sharing. This paper proposes multi-access control attribute based encryption algorithm. The users of different medical institutions are defined by attributes and associate their attributes with private keys. The encipherer encrypts the cipher-text through the access policy and only when the set of attributes possessed by the decrypted user satisfies the minimum number of access structure requirements can the plaintext be decrypted. So it can not only guarantee the minimization of access rights and improve the flexibility of system access control, but also guarantee the security of shared information through encryption.

3. Multi Access Control Attribute Based Encryption Algorithm

3.1 Preliminaries.

(1) Access Structure

The access structure refers to the access control strategy determined by an encrypted user. The following definition of the access structure is given:

$\{P_1,P_2,\ldots\ldots,P_n\}$ is a collection of all participants. The set $A\subseteq 2^{\{P_1,P_2,\ldots\ldots,P_n\}}$ is monotonous: For any x, if $B\in A$ and $B\subseteq C$, then $C\subseteq A$. Access structure A is a non-empty subset of $\{P_1,P_2,\ldots\ldots,P_n\}$ and the set of elements in A is called a set of authorized attributes, otherwise it is a collection of unauthorized attributes.

(2) Access Policy Tree

The access control strategy is a tree structure in which non-leaf nodes resemble a threshold structure and leaf nodes are defined with different attributes. The following definition of the access tree is given:

The access tree structure is represented by Γ, and the non-leaf node is defined by its children and threshold values. The total number of children with node x is num_x and k_x indicates threshold, so $0<k_x\le num_x$. If $k_x=1$, the gate is called or gate and if $k_x=num_x$, the gate is called and gate. The leaf node x in Γ is described by $k_x=1$ and an attribute. In order to better use Γ, some functions are defined. The parent node of the node x can be represented by the $parent(x)$. If x is a leaf node, it can be described by the function $att(x)$. Each node in the access tree Γ is marked with the index value from 1 to num_x, and the function $index(x)$ is associated with the node x. And for an established key index value, any node x in the Γ has only a unique assignment.

(3) Satisfy the Access Tree

Let Γ be an access tree rooted in r. The sub tree of Γ rooted x is represented by Γ_x, and Γ is the same as $\Gamma(r)$.It is assumed that the attribute set γ conforms to $\Gamma(x)$ and is represented as $\Gamma_x(\gamma)=1$. Calculate $\Gamma_x(\gamma)$ by Recursive Algorithm: x is a non-leaf node, and it calculates $\Gamma_{x'}(\gamma)$ for all children of x. $\Gamma_x(\gamma)$ returns 1 Only when at least k_x children return to 1. If x is a leaf node, only when $att(x)\in\gamma$, $\Gamma_x(\gamma)$ returns 1.

3.2 Algorithm Design.

The algorithm implementation in this paper also includes four stages: initialization system parameter stage, key generation stage, encryption stage and decryption stage. The specific implementation process is as follows:

Initialization stage: Generate the public key PK, the master key MK, and some other parameters. Select bilinear mapping G_0 with generator g and prime p. Select $\partial,\beta\ni Z_p$ randomly and generate public key PK and master key MK. The process of calculation is as follows:

$$PK=(G_0,g,h=g^{\beta},\ e(g,g)^{\partial}) \tag{1}$$

$$MK=(\beta,g^{\partial}) \tag{2}$$

Key generation stage: The input of the key generation algorithm is the S of the attribute set, and the output is the key marked by S.Select the random number $r\ni Z_p$, and then select the random number $r_j\ni Z_p$ for each $j\ni S$, and finally calculate the private key:

$$SK=\left(D=g^{(\partial+r)/\beta},\forall j\ni S: D_j=g^r.H(j)^{r_j},D_j'=g^{r_j}\right) \tag{3}$$

Encryption stage: The M (medical document) is encrypted to get CT and the access control tree Γ which is defined by the attributes defined in the system. It is known from the previous definition that CT contains Γ. Encryption begins with generating a polynomial q_x for non-leaf nodes and leaf nodes in Γ. Starting from the root node R of Γ, select q_x from root to leaf node. The degree d_x of q_x is 1 less than the threshold value k_x of x, that is $d_x=k_x-1$.

Select the random number $s \ni Z_p$ for the root node R, and satisfy the $q_R(0) = s$. The polynomial q_R is described by random selection of d_R points. For all non-root nodes x in Γ, define $q_x(0) = q_{parent(x)}(index(x))$, and continue to randomly select d_x points complete description polynomials. Using Y to define all leaf nodes in Γ, the algorithm formula of cipher-text is defined:

$$CT = \left(T, C^{'} = Me(g,g)^{\partial s}, C = h^s, \forall y \ni Y : C_y = g^{q_y(0)}, C_y^{'} = H\left(attr(y)\right)^{q_y(0)}\right) \tag{4}$$

Decryption stage: Use the concept of the recursive algorithm, from the leaf of Γ to the root R. For any node x of Γ, use the judgment rule to calculate F_x until finally s is completely obtained. The node function $DecryptNode(SK, CT, x)$ is used to express the access choice for each node in Γ and the user-supported attributes. There are $CT = \left(\Gamma, C^{'}, C, \forall y \ni Y : C_y, C_y^{'}\right)$ and SK is the private key of the user, and x is a node in the Γ.

If x is a leaf node, i is the attribute of node x, that is $i = attr(x)$. If $i \ni S$, there is:

$$\begin{aligned} DecryptNode(SK, CT, x) &= e(D_i, C_x) / e(D_i^{'}, C_x^{'}) \\ &= e(g,g)^{rq_x(0)} \end{aligned} \tag{5}$$

If x is a no-leaf node, call the function $DecryptNode(SK, CT, R)$. If the tree satisfies S then there is:

$$\begin{aligned} A &= DecryptNode(CT, SK, R) \\ &= e(g,g)^{rq_R(0)} \\ &= e(g,g)^{rs} \end{aligned} \tag{6}$$

The algorithm is decrypted by the following calculation:

$$\begin{aligned} M &= C^{'} / \left(e(C,D)/A\right) \\ &= C^{'} / \left(e\left(h^s, g^{(\partial + r)/\beta}\right) / e(g,g)^{rs}\right) \end{aligned} \tag{7}$$

3.3 Simulation Analysis.

For the proposed algorithm, the simulation tool *cpabe toolkit* can be used to complete the experiment [13]. The operating environment required by the algorithm is a Linux system. The program of the simulation tool is decomposed into *libbswabe* and *cpabe* packages. *cpabe toolkit* provides a four-phase command for the operation of the multi access control attribute-based encryption algorithm. It can implement all the operations using the algorithm commands of different stages.

(1). alization stage: Generate public parameter PK and master key MK, execute $cpabe - setup$ command, generate pub_key and $master\_key$ files, and record the time of algorithm initialization process, as shown in Figure 2.

Figure 2. System Parameter Generation

(2). eneration stage: the public parameter *PK* and the main key *MK* are read from the *pub_key* and *master_key* files, and the users *Sara* and *Kevin* generate the private files *sara_priv_key* and *kevin_priv_key* according to their own properties, and record the time of the key generation process, as shown in Figure 3.

Figure 3. Generation of Different User Private Keys

(3). ption stage: Read *PK* from *pub_key*, encrypt the file *security_report.pdf* through the corresponding access policy, generate the encrypted file *security_report.pdf.cpabe*, and record the time of the encryption process, as shown in Figure 4.

Figure 4. Document Encryption

(4). ption phase: If the users *Sara* and *Kevin* want to access the document *security_report.pdf.cpabe*, the attributes their owned can satisfy the control policy tree. Only when the number of attributes meets the required conditions, the document can be decrypted. The property set of *Kevin* does not satisfy the policy tree, so he does not have access to the document. The attribute set of *Sara* satisfies the policy tree, so he can access the document, get the decrypted document file *security_report.pdf*, and record the time of the decryption process, as shown in Figure 5.

Figure 5. Different Users Access the Document

4. Summary

How to limit the user's access rights to the minimum range is a key issue to ensure the security of medical information in IHE-XDS, and it is also the key to realize the user's flexible access control and secure sharing of medical information. The multi-access control attribute based encryption algorithm proposed in this paper can conveniently describe the attributes of users in different organizations in IHE-XDS. The medical document provider does not need to know the specific information of other users in the system, and only combining the attribute information that can be described with the access strategy can realize the access control. The multi-access control attribute based encryption algorithm can minimize the limits of users' rights in different institutions in IHE-XDS and make medical documents secure and flexible access to sharing.

Acknowledgements

This work is supported by National Natural Science Foundation of China (Grant number 71532002).

References

[1]. Peck D, D P, Peck D, et al. Digital Imaging and Communications in Medicine (DICOM): A Practical Introduction and Survival Guide [J]. The Journal of Nuclear Medicine, 2009, (8):1384.

[2]. WANG Y, YANG J, XU C, LING X, YANG Y. Survey on Access Control Technologies for Cloud Computing [J]. Journal of Computer Applications, 2015, (05):1129-1150.

[3]. SHANG W, WU H, ZHAO B. Design and implementation of integrated platform based on HL7 and IHE-XDS technology framework [J]. Journal of Guang Dong Medical College, 2012, (03):243-246.

[4]. LI Teng. A Research for the Heterogeneous Medical Information System Patient Identifier Cross-referencing [D]. Guang Dong: Southern Medical University, 2011.

[5]. LI Lianglei, SHAO Lisong, WANG Chuangyong, et al. Context-aware Access Control for Ubiquitous Network [J]. The Network Monitoring and Surveillance, 2017, 8(Z2):48-54.

[6]. WANG X, FU H, ZHANG L. Research Progress on Attribute-Based Access Control[J]. Acta Electronica Sinica, 2010, 07:1660-1667.

[7]. LIU Xiubin. Research on attribute encryption access control based on cloud computing [J]. Wireless Internet Technology, 2017(12):30-31.

[8]. Sahai A, Waters B. Fuzzy identity-based encryption [A]. Advances in the 24th Annual International Con-ference on the Theory and Applications of Cryptographic Techniques [C]. Aarhus, Denmark, 2005:457-473.

[9]. Vipul Goyal, Omkant Pandey, Amit Sahai, et al. Attribute-based encryption for fine-grained access control of encrypted data[C].Proc of Acmccs,2006:89-98.

[10]. BETHENCOURT J, SAHAI A, WATERS B. Ciphertext-policy attribute-based encryption [C]. Proc of IEEE Symposium on Security and Privacy. Washington DC: IEEE Computer Society, 2007:321-334.

[11]. Liang XH, Cao ZF, Lin H, et al. Provably secure and efficient bounded ciphertext policy attribute based encryption. In: Proc. of the ASIAN ACM Symp. On Information, Computer and Communications Security (ASIACCS 2009). New York: ACM Press, 2009. 343−352.

[12]. LBRAIMI L, TANG Q, HARTEL P, et al. Efficient and provable secure ciphertext-policy attribute-based encryption schemes[C]. Procof Information Security Practice and Experience. Berlin: Springer-Verlag, 2009: 1-12.

[13]. Jahid S, Mittal P, Borisov N. EASi ER: encryption-based access control in social networks with efficient revocation [C]. Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security, New York, NY, USA.2011:411-415.