Secure and Efficient Attribute-Based Access Control Optimization Scheme for EMR System

Mei-ping LIU¹, Cheng YANG¹ and Ya-na ZHANG¹

¹School of Information and Communication Engineering, Communication University of China, Beijing, China

*Corresponding author

Keywords: EMR System, ABAC, CP-ABE, Attribute value enabled.

Abstract. Electronic Medical Record (EMR) system based on the cloud has serious leaks of patient data and private information. Access control and privacy protection are considered to be the keys to ensuring the privacy of patients. Attribute-Based Access Control (ABAC) can realize fine-grained control of cloud medical data, but lacks the corresponding encryption mechanism. Moreover, as the scale of medical data grows, the number of entity attributes and policies required by ABAC is increasing, leading to performance degradation. Most of the existing research schemes focus on security but ignore efficiency, and the encryption scheme does not fit ABAC mechanism well. This paper proposed a retrieval method that enables attribute value, which filtered invalid policies, and improved Ciphertext-Policy Attribute-Based Encryption (CP-ABE), shared attribute set with ABAC to save attribute processing time, thus constructing a secure and efficient SE-ABAC solution in EMR system. Finally, through simulation experiment analysis, the optimizes solution is effective and more efficient than traditional ABAC.

Introduction

Electronic Medical Record (EMR) system records patient's medical information, including personal information, examination results, doctor's advice, nursing records, etc [1]. It not only saves time, but also improves the pass rate of medical records and the quality of medical work. In China's national informatization development strategy, it is clearly proposed to build an EMR system, and issued normative documents, laws and regulations to standardize the management of EMR [2]. But because of the concerns of cloud computing environment, all medical records are embedded in the medical information system based on LAN, which limits the sharing of medical information. At the same time, there are many problems of unauthorized access and privacy disclosure. Access control ensures that resources can be accessed by legitimate users through the identity information of the visitor and the system's security policies, while preventing theft by illegal users and unauthorized access by legitimate users [3].

Traditional access control models, such as Discretional Access Control (DAC)[4], Mandatory Access Control (MAC)[5], Role-Based Access Control (RBAC)[6] cannot meet the actual needs of complex EMR system, while Attribute-Based Access Control (ABAC)[7] is an ideal scheme, supported by extensible Access Control Markup Language (XACML) framework. There is no satisfactory solution to the efficiency problems in EMR, and the encryption mechanism is not suitable. Therefore, this paper proposed the ABAC method enabled attribute values, and used Attribute-Based Encryption (ABE) to store EMR information, constructing a secure and efficient EMR access control solution. The organizational structure of this paper is as follows: Section II gives an overview of the existing access control scheme of EMR system; Section III introduces the SE-ABAC solution; the simulation results is showed in section IV; finally, followed by the conclusion.
Related Work

Privacy protection in EMR system has become a focus of researchers. However, the research on the efficiency of personalized access is scarce. Maithilee et al [8] proposed an attribute-based field-level document encryption to manage EHR access and data security, and delegated the access rights of EHR to medical providers. Ming Li et al [9] divided the user into multiple security domains to reduce the complexity of key management. However, the authorization mechanism was completely left to the patient, which brought huge expense to the patient. Shantanu Pal et al [10] proposed an IoT access control, which simplifies policy management, but doesn't provide an effective encryption mechanism for patient health data. Premarathne et al [11] use encrypted RBAC to control the safe storage and access of EHR data, but complex EMR need more role assignment, which is difficult to manage. Kwangsoo et al [12] proposed XACML-based ABAC to provide fine-grained access control and use XML partial encryption and digital signature to protect patient privacy.

The above literature cannot give consideration to the fine-grained, efficiency and encryption that fits the access control mechanism. For this, this paper proposed an ABAC method enabled attribute value based on the XACML. Using the attribute values to implement permission grant quickly, and improved ABE to adapt the ABAC, a secure and efficient SE-ABAC solution is constructed to guarantee the efficiency of medical services and the security of patient privacy information.

Improved Algorithm and Optimization Scheme

ABAC Method Enabled Attribute Value

ABAC obtains three kinds of entity attribute information: subject, object and environment. According to the actual demand in EMR, this paper concretes object into resource and operation, use SA, RA, OA and EA to represent the set of subject attributes, resource attributes, operation attributes and environment attributes respectively. The attribute and their attribute value set involved in the policy description are shown in Table 1.

| Attribute Name | Attribute Value |
|----------------|-----------------|
| SA.Role        | Physician, Technician, Nurse |
| SA.Title       | Chief, Deputy chief, Attending, Resident, Assistant |
| SA.Department  | Emergency, Internal medicine, Surgery, Pharmacy, Inspection |
| RA.Type        | Medical order, Medical record, Nursing record, Test result |
| RA.Department  | Emergency, Internal medicine, Surgery, Pharmacy, Inspection |
| OA.Type        | Read, Write, Review |
| OA.Purpose     | Medical, Teaching, Research |
| EA.Current Time | 8:00-18:00, Otherwise |

XACML is widely used to formulate access control policies [13] in ABAC. The data flow model is shown in Figure 1. The Policy Information Point (PIP) collects SA, RA, OA and EA, and transmits the relevant information to the Policy Decision Point (PDP) through the context handler. PDP compares the attribute information with the policies obtained from the Policy Administration Point (PAP), and responds to the Policy Execution Point (PEP), which executes the corresponding decision results. XACML policy language model is expressed as the policy tree shown in Figure 2. In EMR system, when the medical staff wants to manipulate the patient's data, all relevant attributes will be parsed. According to XACML policy tree, from the policySet node to the rule effect node, the attribute-value pair (avp) contained in each node are matched layer by layer, and all policies are traversed in turn. When parsing a policy with many attributes, parsed to the last one and found that its value doesn't match the request. If there are many similar invalid policies, it will affect the efficiency.
ABAC attribute storage is in the form of avp, which is a two-tuple (att, value), i.e., att=value. Each attribute contains multiple attribute values, and the attribute values of different attributes are basically different. Based on this, in the process of policy matching, attribute values are more distinguishable than attribute names. Therefore, this paper considers changing the way of traditional XACML that matching attribute first and then matching attribute values, make full use of the advantages of attribute values in decision making, and use ABAC method enabled attribute value to quickly filter out the policies that meet the request, reduce PDP response time, and improve access control efficiency.

Some improvements have been made to XACML framework after enabling attribute values, as shown in Figure 3. Adding an attribute value array builder model in PIP. When access control is implemented, PIP obtains the attributes related to the request, and the attribute value array builder module extracts the attribute values of each attribute to generate a sequence, which is sent to PDP together with the attributes. PDP uses the attribute values one by one according to the received sequence, enables the next attribute value filtering in the former matching policies, filters the invalid policies step by step, omits the analysis of the remaining attribute values of the invalid policies, and realizes the efficient access control decision.
SE-ABAC Solution

The access control model itself lacks a certain encryption and decryption mechanism, the cloud medical service provider will obtain information as much as possible based on user input, and may collude with malicious users to illegally obtain confidential data, so the security of patient data is still a problem. Its ciphertext and key are associated with user attributes, and only users whose attributes meet the corresponding access control structure can decrypt ciphertext. It can support fine-grained control, but the basic ABE can only represent threshold policies, which can only be applied in scenarios with simple policy requirements. Some researchers put forward Ciphertext-Policy ABE (CP-ABE) and Key-Policy ABE (KP-ABE), both of which can support complex policies. Although they have similar structure, the algorithm flow and applicable scenario are totally different. Therefore, through comparative analysis, the encryption method suitable for access control in EMR system is pointed out.

In the KP-ABE mechanism, the user restricts the description of the received message, when access is allowed, a specific access structure is assigned to the user. This method is more suitable for query applications, such as network paid video, TV on demand system, etc. In EMR system, the patients want to set corresponding policies to determine which attributes the medical staff have can access their medical data. But the record data is not fixed, while the medical staff can be described by a series of attributes. These expressions are very consistent with CP-ABE, which the sender specifies the policies for ciphertext access. More importantly, the ciphertext can be decrypted if attribute set meets the access structure, which is very close to the ABAC permission granting. Therefore, CP-ABE is used to encrypt the patient's medical data to ensure the security in the above efficient access control solution.

The classic CP-ABE system is shown in Figure 4, where the attribute authorized agency AA Server stores user's attribute information and provides a set of attributes of the requesting user to the central authorized agency CA Server. CA Server generates public parameters required for encryption and private key for decryption. This paper not only introduces the idea of CP-ABE algorithm, but also considers its applicability in ABAC environment to improve the traditional model, which is more suitable for the EMR application scenario in this paper.

![Figure 4. Traditional ciphertext policy attribute encryption (CP-ABE) model.](image)

CP-ABE and ABAC both need to provide access control policies and collect attributes of the subject during the operation. Based on it, we present the CP-ABE model suitable for ABAC:

1. The CP-ABE attribute is represented by SA in ABAC, and is in the form of an attribute-value pair. In this way, CP-ABE can be described by the original ABAC attribute without re-establishing the relevant attribute, thus saving the storage space.

2. The access structure of CP-ABE represents the authorization set. It can be constructed by obtaining the avp of SA in ABAC policies and the users does not need to further develop the subject attribute authorization structure. At the same time, the encryption operation is implemented by the proxy module to reduce the patient's overhead.

Based on the analysis of encryption requirements in the EMR system above, a complete SE-ABAC solution was constructed by applying the CP-ABE improvement scheme in the ABAC environment, as shown in Figure 5:
Simulation Experiment and Analysis

Experimental Analysis

The experimental environment is as follows: Intel(R) Core (TM) 2 Quad CPU Q9550 @2.83GHz; (RAM) 4.00GB; Windows7 Ultimate, SP1; Java jre1.8.0. 300 policies are constructed according to XACML3.0 and actual EMR system, each one contains at least one rule, and different access requests are written according to different resources and environments. To test the efficiency of the SE-ABAC, the experiments of the traditional XACML model and attribute value-enabled scheme were performed.

The simulation experiment compared the time consumption of the two schemes when the number of policies increased. Figure 6 shows the trend of the policy resolution time of the two models as the number of policies increases. The policy resolution time refers to the time that PDP analyzes the attribute, attribute value and its data type in the policy step by step. It can be seen that as the number of policies increases, the efficiency advantage of the scheme in this paper becomes more and more obvious; Figure 7 shows the change of the policy evaluation time of the two models with the increase of the number of policies. The policy evaluation time refers to the total time of PDP from retrieving the policy to analyzing and giving the response result. It can be seen that the scheme proposed in this paper has obvious efficiency advantages, which is 2 to 3 times higher than the classic model, therefore the SE-ABAC solution has higher efficiency.
Security Analysis

In the security, the improved CP-ABE model uses SA in ABAC to indicate related attributes, and obtains the subject attribute-value pair in the ABAC policies to construct the required access control structure. However, its algorithm steps are basically the same as traditional CP-ABE, and the original random algorithm and security parameters have not changed. Therefore, it has no impact on security and can guarantee the data security in the EMR system.

For general users, if the attribute set does not conform to the access control policy, he does not have authority to the ciphertext, then, he cannot recover the plaintext because of the lack of corresponding bilinear mapping pair. For the semi-trusted cloud server, although it collects as much ciphertext data as possible, it cannot obtain the user's attribute information through the ciphertext, and does not have any public parameters and keys. Therefore, the cloud server cannot decrypt ciphertext. Therefore, the SE-ABAC solution can guarantee the confidentiality of the data in the EMR system, so it is secure.

Conclusion and Future Research

Modern medical EMR system contains more and more patient data, and the multidisciplinary interaction also makes the medical record data needed by medical staff to diagnose patients become complicated, so the access control policies are increasing, which affects the system performance. This paper builds a secure and efficient SE-ABAC solution. First, an ABAC method enabled attribute values is proposed to improve access control performance. Meanwhile, CP-ABE is improved to better integrate with ABAC to protect patient privacy and medical data. The security of SE-ABAC is theoretically demonstrated, which can guarantee data confidentiality indeed, and the high efficiency and good scalability of the scheme in policy decision are verified by simulation experiments.

The following work will focus on two aspects: first, in view of the policy disclosure in access control, consider the confidentiality of the policy to prevent malicious users from obtaining the attribute value information in the policy and divulging sensitive information; the second is to add attribute revocation function in the SE-ABAC to avoid the traditional duplicate authorization.

Acknowledgement

This research was financially supported by "High-Precision" Discipline Construction Project of Beijing Colleges (Internet Information Discipline of Communication University of China) (CUC190J054), Outstanding Ph.D Supervisor Team Project of Communication University of China (CUC2019A009) and Major Research Project of Communication University of China-AI News Production System and Key Technologies in Media Events (CUC19ZD003).
References

[1] https://www.sohu.com/a/124701829_252291
[2] Wang Ying, et al. A usage control model suitable for an electronic medical record system[J]. Computer Science, 2010(11):196-199.
[3] Shen Haibo, Hong Fan. Survey of Research on Access Control Model[J]. Application Research of Computers, 2005, 22(6):9-11.
[4] Lipton R J, Snyder L. A Linear Time Algorithm for Deciding Subject Security[J]. Journal of the ACM, 1977, 24(3):455-464. R.J. Ong, J.T. Dawley and P.G. Clem: submitted to Journal of Materials Research (2003)
[5] Upadhyaya S. Mandatory Access Control[M]//Encyclopedia of Cryptography and Security. Springer US, 2011.
[6] Komlenovic M, Tripunitara M, Zitouni T. An empirical assessment of approaches to distributed enforcement in role-based access control (RBAC)[C]//Acm Conference on Data & Application Security & Privacy. 2011.
[7] Xin J, Krishnan R, Sandhu R. A Unified Attribute-Based Access Control Model Covering DAC, MAC and RBAC[M]//Data and Applications Security and Privacy XXVI. 2012.
[8] Joshi M, Joshi K, Finin T. Attribute Based Encryption for Secure Access to Cloud Based EHR Systems[C]// 2018 IEEE 11th International Conference on Cloud Computing (CLOUD). IEEE, 2018.
[9] Li M, Yu S, Zheng Y, et al. Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption[J]. IEEE Transactions on Parallel and Distributed Systems, 2013, 24(1):131-143.
[10] Pal, Shantanu & Hitchens, Michael & Varadharajan, Vijay & Rabehaja, Tahiry. (2018). Policy-Based Access Control for Constrained Healthcare Resources. 588-599. 10.1109/WoWMoM. 2018.8449813.
[11] Premarathne U, Abuadbba A, Alabdulatif A, et al. Hybrid Cryptographic Access Control for Cloud-Based EHR Systems[J]. IEEE Cloud Computing, 2016, 3(4):58-64.
[12] Seol K, Kim Y G, Lee E, et al. Privacy-preserving Attribute-based Access Control Model for XML-based Electronic Health Record System[J]. IEEE Access, 2018, pp. (99):1-1.
[13] https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml