Tzu Chi Medical Journal 2023; 35 (2): 143-147

Review Article

Review of hierarchical database access control for E-medicine systems

Tian-Fu Lee[a], Jyun-Guo Wang[a], Yen-Chang Chen[b,c]*

[a]Department of Medical Informatics, Tzu Chi University, Hualien, Taiwan, [b]Department of Anatomical Pathology, Hualien Tzu Chi Hospital, Buddhist Tzu Chi Medical Foundation, Hualien, Taiwan, [c]Institute of Medical Sciences, Tzu Chi University, Hualien, Taiwan

Submission : 29-Apr-2022
Revision : 23-May-2022
Acceptance : 10-Jun-2022
Web Publication : 23-Aug-2022

Abstract

Key management schemes for hierarchical access control enable users who have hierarchical relationships with each other to manage their secret keys efficiently. In these schemes, the users are divided into several groups, and all groups have their own central authorities. Each central authority is responsible for setting parameters and generating user's secret keys in a hierarchical structure such that all users efficiently derive their secret keys and solve dynamic access control problems. Several key management schemes with Health Insurance Portability Accountability Act regulations were recently proposed for hierarchical access control in e-medicine systems. However, these schemes either are insecure or require a large amount of storage and heavy computations. Therefore, this study reviews and discusses hierarchical access control schemes with privacy/security regulations for medical record databases.

Keywords: *Access control, E-medicine systems, Hierarchical, Medical information security*

Introduction

Background

With the rapid development of the Internet, the medical records of various hospitals and medical organizations are also oriented toward electronic medical information. Electronic medical records have become an important research topic in the electronic medical system. To protect the security of medical record data and patient privacy, a secure access control mechanism is very important. Electronization of medical information can reduce the waste of administrative costs while increasing the quality and efficiency of medical care. The benefits brought about by the electronicization of medical information have caused governments around the world to invest a lot of resources to build relevant systems. Based on the characteristics of medical service provision, medical information collection, use, and electronic consent exercise do not actually have much choice. Therefore, patients' right to control their medical information is not as strong as that of general information, so it is necessary to maintain the subject's privacy through rigorous information consent and confidentiality mechanisms. However, the organizational structure of personnel in medical institutions is huge. If the organizational authority mechanism of management personnel is poorly designed, data will be stolen and leaked. The system will also suffer from poor load due to the huge amount of computing and storage space. The ultimate goal of electronic medical records is to allow the medical records scattered in various hospitals to be shared with different hospitals through the Internet, but the data sharing is also accompanied by the problem of being stolen or destroyed. The early data access control mechanism is to encrypt each file or service with a different key. When a user in the organization needs certain files or data, the key is allocated to the user. When a user has the right to access a large number of files, he/she will be assigned multiple different keys and need to maintain these keys. This mechanism is very inefficient and impractical in more complex and huge systems. It is also difficult to perform dynamic key management. Therefore, it is very important to establish an organizational structure that can protect data security and at the same time have good efficiency.

In August 1996, the United States passed an important Health Insurance Portability Accountability Act (HIPAA), which established information security specifications in medical care to improve the overall quality of medical care. In these regulations, patients' privacy rights expressly stipulate that patients must have more control over personal medical information, and the use and disclosure of medical information should be controlled [1,2]. To promote the popularization and application of electronic medical information, Taiwan has also strengthened the implementation of many preventive measures

**Address for correspondence:* Prof. Tian-Fu Lee, Department of Medical Informatics, Tzu Chi University, 701, Zhongyang Road, Section 3, Hualien, Taiwan.
E-mail: jackytflee@mail.tcu.edu.tw

Access this article online

Quick Response Code:

Website: www.tcmjmed.com

DOI: 10.4103/tcmj.tcmj_124_22

How to cite this article: Lee TF, Wang JG, Chen YC. Review of hierarchical database access control for E-medicine systems. Tzu Chi Med J 2023;35(2):143-7.

on medical information security, including the establishment of a medical electronic authentication mechanism based on the public key cryptography system by the department of health to ensure the safety of the electronic operation of medical information. The department of health has gradually completed the establishment of the "Healthcare Certification Authority," and has begun to investigate and use credential IC cards for medical institutions and medical personnel. Its main purpose is to ensure the leakage of private or sensitive information generated by people seeking medical treatment, and to cooperate with the completion of relevant laws and regulations, and to actively plan related medical information applications such as electronic medical records.

The structure of hierarchical database access control

The hierarchical access control divides users into many groups, and users are divided into different security class (SC) sets according to their permissions, where SC = (SC_1, SC_2,…, SC_N). The SCs in the hierarchy have a privilege order relationship. When $SC_j \leq SC_i$, the privileges of SC_i are greater than those of SC_j, and SC_i is called the ancestor of SC_j; SC_j is called the successor of SC_i. The relation is defined as (SC_i, SC_j) $\in R_{i,j}$. When $SC_j \leq SC_k \leq SC_i$, and SC_k does not exist, SC_i is called the immediate predecessor of SC_j; SC_j is called the immediate successor of SC_i. The certification center (CA) will generate a suitable key and public parameters for each SC. The user only needs to store one secret key. Then, the successor's key can be deduced using this secret key with the public parameters to access the files corresponding to its permissions. Thus, the problems of repeated key storage and key management difficulties can be overcome [3-5].

Figure 1 illustrates the structure diagram of hierarchical access control. SC is the security level, and CA will generate a key for each SC. SC_1 has the highest permission and can use its own key to derive the keys of other SCs through public parameters to access files; SC with lower permissions cannot derive the keys of SCs with higher permissions, so as to achieve the confidentiality property of data access. The hierarchical access control mechanism is divided into dependent key and independent key. In the process of calculating the key, the subordinate key needs to use the key and parameters to calculate all the keys in the SC interval (indirect key derivation); the independent key only needs to use the owned key and parameters to do one operation (direct key derivation). For example, in Figure 1, when SC_1 attempts to obtain the key of SC_5, it needs to calculate the key of SC_2 between SC_1 and SC_5 in the way of subordinate key, and then use the calculated key of SC_2 to calculate the key of SC_5 [3].

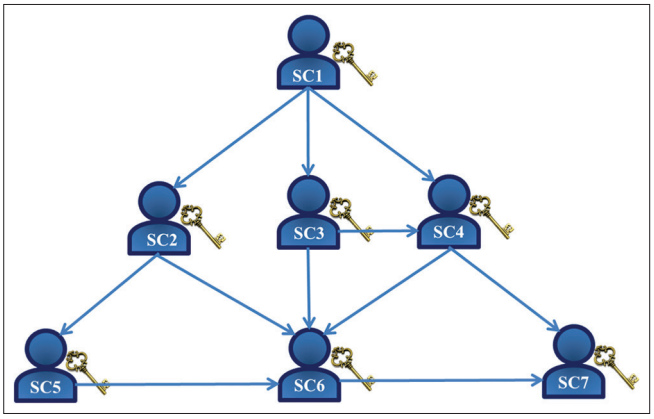

Figure 1: The structure of hierarchical access control [3]

The personnel organization structure in medical institutions is huge, and personnel in different departments can access different information. In general, a hospital organization has not many classes but has a lot of departments. Therefore, the management of the hospital organization with many departments focuses on

1. Using a small number of parameters to reduce the difficulty of management
2. The rapid generation and derivation of the key, and
3. Dynamic updating and management of keys.

The remainder of this investigation is organized as follows. Section 2 reviews the hierarchical access control schemes, which include access control schemes compliant with privacy/security regulations and hierarchical database access control schemes. Section 3 provides a performance comparison of related works. Section 4 describes the analysis and discussions. Finally, Section 5 draws conclusions and future works.

Reviews of hierarchical access control schemes compliant with privacy/security regulations

Access control schemes compliant with Health Insurance Portability Accountability Act privacy/security regulations

In 1996, the United States passed the HIPPA Act, so that the privacy of patients' personal medical records was protected by law. In recent years, many studies were presented on HIPAA-compliant access control research. For example, in 2008, Lee and Lee [6] proposed a HIPAA-compliant electronic medical information system. Lee and Lee proposed a health data card-based electronic health-care plan, in which patients use smart cards for secure storage and retrieval of PHI during treatment consultations. Symmetric encryption/decryption keys based on the health-care provider's session architecture are used for PHI data confidentiality. The mechanism weakness of Lee and Lee is that the smart card cannot be queried from a distance through the network, and multiple queries of the patient's PHI cannot be performed simultaneously. Subsequently, Hu *et al*. [7] in 2010 and Huang and Liu [8] in 2011 enhanced the scheme of Lee and Lee [6] and developed better solutions.

Hu *et al*. [7] in 2010 proposed an e-health system for HIPAA privacy and security regulations, which uses a hybrid security mechanism based on public key infrastructure (PKI) and Medicare smart cards, and provides access from PHI to Medical Center Server (MCS). Patient consent is not required during storage and retrieval, once the phase task is completed, the patient's PHI record is deleted, the patient cannot obtain a copy of his PHI for subsequent treatment sessions, and this mechanism does not take into account the legal requirements

for patient consent exceptions. Therefore, if an emergency occurs, it still cannot be handled correctly in accordance with HIPAA regulations.

In 2011, Huang and Liu [8] proposed an efficient key management scheme compliant with HIPAA regulations. Their scheme was based on elliptic-curve cryptography (ECC) and facilitates interoperability between the applied cryptographic mechanisms.

In 2014, Ray and Biswas [2] proposed a solution, which is similar to the scheme of Hu *et al*., [7] to comply with HIPAA privacy/security regulations. Their scheme was developed using a public key encryption-based e-health system architecture and using contracts and intelligence cards with RSA signature technology to protect user's PHI data. This scheme addresses emergency inquiries and data sharing with external medical centers, but does not provide user anonymity, prevent insider attacks, and safeguard data security.

In 2014, Lee *et al*., [9] proposed to use N-degree Lagrange interpolating polynomial to effectively solve the shortcomings of the scheme of Hu *et al*. [7] and the scheme of Huang and Liu [8] in the key authorization. The proposed scheme is to store the keys of patients and MCS in their own smart cards. When the key is generated, the patient's key and the master key generated by the linear equation are required. However, if the patient's smart card is obtained by an attacker, it may cause doubts about the security of the key and threaten the confidentiality of medical record information.

Hierarchical database access control schemes

The hierarchical database access control schemes are classified into PKI-based hierarchical database access control schemes and hierarchical database access control schemes without PKI. The former needs to use the public key cryptosystem in the process of key derivation, while the latter does not.

Public key infrastructure-based hierarchical database access control schemes

In 1983, AKL and Tylor [3] first proposed a key management scheme for hierarchical database access control. Later, many related schemes for hierarchical database access control were proposed one after another. These related schemes still require a large amount of computation and huge storage space. Some schemes are more likely to have security threats. In addition, when the database hierarchy is complex, its efficiency will gradually decrease and the dynamic management of the keys is not easy to carry out.

In 2006, Jeng and Wang [4] proposed an efficient hierarchical access control key management mechanism based on polynomial and elliptic curve public key cryptosystems to solve the hierarchical access control problem. Each class in the hierarchy is allowed to select its own secret key. The problem of efficiently adding or deleting classes can be solved without the necessity of regenerating keys for all the users in the hierarchy, as was the case in previous schemes. The scheme is shown much more efficiently and flexibly than the schemes proposed previously.

In 2008, Chung *et al*. [5] proposed a novel hierarchical access control key management scheme based on elliptic-curve cryptosystem and one-way hash function to solve dynamic access problems in a user hierarchy.

In 2010, Nikooghadam *et al*. [10] proposed a hierarchical access control key management mechanism based on elliptic-curve encryption keys. Although the computing efficiency was improved, their scheme uses the elliptic-curve cryptosystem, and still requires heavy computations.

In 2012, Das *et al*. [11] pointed out that the management schemes proposed by Jeng and Wang [4] and Chung *et al*. [5] had the security problem of key leakage, so they proposed an improved hierarchical access control key management mechanism to solve the security problem.

In 2012, Wu and Chen [12] pointed out that the scheme of Nikooghadam *et al*. [10] lacked formal security analysis, and used elliptic-curve encryption and decryption operations that were slower than symmetric encryption and decryption operations. Wu and Chen also developed a hybrid hierarchical access control in the electronic medical system. Their scheme was developed by adopting elliptic curve and symmetric encryption/decryption systems to improve the operation efficiency.

Subsequently, Nikooghadam and Zakerolhosseini [13] found that the scheme of Wu and Chen could not effectively overcome the man-in-the-middle attack problem. To improve this problem, elliptic-curve signatures were used in their new developed scheme. However, it required a lot of computational operations in the verification process.

Hierarchical database access control schemes without public key infrastructure

In 2013, Odelu *et al*. [14] proposed an efficient key management scheme for hierarchical access control in e-medicine system scheme. Their scheme used symmetric encryption and decryption hash functions, which greatly reduces the complexity of parameter storage and operation. Although the used parameters are reduced in their scheme, many parameters are still required in the case of complex layers.

In 2017, Chao *et al*. [15] proposed an improved hierarchical access control scheme based on the scheme of Odelu *et al*. Although Chao *et al*.'s scheme improves the time and space complexity, it still requires many parameter operations and more symmetric encryption and decryption operations in the case of complex layers.

Performance Comparison

This section compares the performance of related schemes for hierarchical access control in terms of storage space complexity and computational complexity. Assume that there are N SCs in the hierarchy to form the set SC = (SC_1, SC_2,… SC_N); Each SC_i has *vi* high-authority SC*s*. Both keys and parameters are 128-bit in length.

Comparison of storage space complexity

Table 1 lists the storage space comparison of related schemes for hierarchical access control, and compares the key

Table 1: The storage space complexity comparison of related schemes

Schemes	CA	SC	Public parameters
Jeng and Wang, 2006 [4]	163 (2*N*+1)	163	$163\ (\sum_{i=1}^{N}(vi+1)+6N+2)$
Chung *et al*., 2008 [5]	163 (2*N*+1)	163	$163\ (\sum_{i=1}^{N}(vi+1)+6N+2)$
Nikooghadam *et al*., 2010 [10]	163*N*	163	$163\ (2\sum_{i=1}^{N}(vi+1)+2N$
Wu and Chen, 2012 [12]	128+163	163	$128\ (\sum_{i=1}^{N}(vi+1)+N)+163(2N+2)$
Nikooghadam and Zakerolhosseini, 2012 [13]	163 (*N*+1)	163	$163\ (\sum_{i=1}^{N}(vi+1)+N)+5N+2)$
Odelu *et al*., 2013 [14]	128	128	$128\ (\sum_{i=1}^{N}(vi+1)+N)+3N+1)$
Chao *et al*., 2017 [15]	128	128	$128\ (\sum_{i=1}^{N}(vi+1)+N)+2N+1)$

SC: Security class, CA: Certificate authority

and parameter space stored in CA, SC, and public directory, respectively. The storage space of the schemes of Odelu *et al*. [14] and Chao *et al*. [15] in CA, SC, and public directory is significantly lower than that of other related schemes, and do not generate a large number of parameters in the case of complex hierarchy.

Comparison of computational complexity

Table 2 shows the comparison of related schemes for hierarchical access control in terms of computation complexity, which is the sum of the computational complexity of the key generation stage and the key derivation stage. The key generation stage is the calculation time required by the CA to generate parameters and keys for each SC, and the key derivation stage is the time it takes for each SC to derive all keys that meet its own authority. T_{MUL} denotes the time required to perform a multiple operation; $T_{EC_{ADD}}$ denotes the time required to perform a multiplication operation; $T_{EC_{MUL}}$ denotes the time required to perform a multiplication operation on ECC; T_{SHA1} denotes the time required to perform a hash operation; T_{AES} denotes the time required to perform a symmetric encryption/decryption; T_{XOR} denotes the time required to perform an exclusive-OR operation; T_{ADD} denotes the time required to perform an addition operation. The schemes of Odelu *et al*. [14] and Chao *et al*. [15] use AES symmetric encryption/decryption and hash operations, which greatly reduces the computation time compared to previous related works using elliptic curves.

Table 2: The computational complexity comparison of related schemes

Scheme	Computational complexity
Jeng and Wang, 2006 [4]	$(\sum_{i=1}^{N}2(vi^2+vi)\cdot T_{MUL}+2N\cdot T_{EC_{ADD}}+(4N+2\sum_{i=1}^{N}(vi+1))\cdot T_{EC_{MUL}}+2\sum_{i=1}^{N}(vi+1)\cdot T_{SHA1})$
Chung *et al*., 2008 [5]	$(\sum_{i=1}^{N}2(vi^2+vi)\cdot T_{MUL}+2N\cdot T_{EC_{ADD}}+(3N+2\sum_{i=1}^{N}(vi+1))\cdot T_{EC_{MUL}}+2\sum_{i=1}^{N}(vi+1)\cdot T_{SHA1})$
Nikooghadam *et al*., 2010 [10]	$N\cdot T_{INV}+(N+2\Sigma_{(i=1)}^{N}(vi+1)\ T_{EC\_MUL})+(N+\Sigma_{(i=1)}^{N}(vi+1))\ T_{SHA1}$
Wu and Chen, 2012 [12]	$(2N+1)T_{EC_{MUL}}+2(N+\Sigma_{(i=1)}^{N}(vi+1))\ T_{AES}+2N\ T_{SHA1}$
Nikooghadam and Zakerolhosseini, 2012 [13]	$(2\Sigma_{(i=1)}^{N}vi)\cdot T_{XOR}+(N+\Sigma_{(i=1)}^{N}vi)\cdot T_{ADD}+(2N+\Sigma_{(i=1)}^{N}vi)\ T_{MUL}+(2N+1+4\Sigma_{(i=1)}^{N}vi)\ T_{EC_{MUL}}+(N+2\Sigma_{(i=1)}^{N}vi)\ T_{SHA1}$
Odelu *et al*., 2013 [14]	$(3N+2\Sigma_{i=1}^{N}(vi+1))\cdot T_{AES}+(5N+1)\cdot T_{SHA1}$
Chao *et al*., 2017 [15]	$(2N+2\sum_{i=1}^{N}(vi+1))\ T_{AES}+NT_{SHA1}$

Discussion

From performance comparisons of related schemes in Section 3, the schemes of Odelu *et al*. and Chao *et al*. are developed using symmetric encryption/decryption and hash operations, and more efficient than related works in terms of storage space complexity and computational complexity.

Based on the related studies review in this article, most current lightweight computing authentication schemes are mainly based on key exchange and agreement. There are few studies discussing the key management and database access control, even applicable to electronic medical records and health-care records with security/privacy regulations. In addition, most studies related to database access control are complex in structure and require heavy computations. Some studies may have security problems, including the confidentiality of medical records cannot be ensured, and the integrity of medical records cannot be achieved, and noncompliance with security/privacy regulations where keys are authorized by the patient to control.

Conclusion and future work

This study divides hierarchical access control schemes into access control schemes compliant with HIPAA privacy/security regulations and hierarchical database access control schemes. The hierarchical database access control schemes are also classified into PKI-based hierarchical database access control schemes and hierarchical database access control schemes without PKI.

A hierarchical database access control scheme without PKI is more computationally efficient and preserves security requirements. The future work plans including other lightweight operations, such as PUF, and the development of privacy/security compliant database access control schemes for e-health-care systems.

Financial support and sponsorship

This research was funded by the Ministry of Science and Technology of the Republic of China, grant number MOST 110-2221-E-320-005-MY2.

Conflicts of interest

There are no conflicts of interest.

References

1. The USA Government. HIPAA. Washington, D.C: The USA Government; 1996, p. 104-91.
2. Ray S, Biswas GP. A Certificate Authority (CA)-based cryptographic solution for HIPAA privacy/security regulations. Comput Sci Inf Syst 2014;26:170-80.
3. Akl SG, Tayior PD. Cryptographic solution to a problem of access control in a hierarchy. ACM Trans Comput Syst 1983; 1: 239-248.
4. Jeng FG, Wang CM. An efficient key-management scheme for hierarchical access control based on elliptic curve cryptosystem. J Syst Softw 2006;79:1161-7.
5. Chung YF, Lee HH, Chen TS. Access control in user hierarchy based on elliptic curve cryptosystem. Inf Sci 2008;178:230-43.
6. Lee WB, Lee CD. A cryptographic key management solution for HIPAA privacy/security regulations. IEEE Trans Inf Technol Biomed 2008;12:34-41.
7. Hu J, Chen HH, Hou TW. A hybrid public key infrastructure solution (HPKI) for HIPAA privacy/security regulations, Comput Stand Interfaces 2010;32:274-80.
8. Huang HF, Liu KC. Efficient key management for preserving HIPAA regulations. J Syst Softw 2011;84:113-9.
9. Lee WB, Lee CD, Ho KI. A HIPAA-compliant key management scheme with revocation of authorization. Comput Methods Programs Biomed 2014;113:809-14.
10. Nikooghadam M, Zakerolhosseini A, Moghaddam ME. Efficient utilization of elliptic curve cryptosystem for hierarchical access control. J Syst Softw 2010;83:1917-29.
11. Das AK, Paul NR, Tripathy L. Cryptanalysis and improvement of an access control in user hierarchy based on elliptic curve cryptosystem. Inf Sci 2012;209:80-92.
12. Wu S, Chen K. An efficient key-management scheme for hierarchical access control in e-medicine system. J Med Syst 2012;36:2325-37.
13. Nikooghadam M, Zakerolhosseini A. Secure communication of medical information using mobile agents. J Med Syst 2012;36:3839-50.
14. Odelu V, Das NY, Goswami A. An efficient and secure key-management scheme for hierarchical access control in E-medicine system. J Med Syst 2013;37:9920.
15. Chao WY, Tsai CY, Hwang MS. An improved key-management scheme for hierarchical access control. Int J Netw Secur 2017;19:639-43.