Scheme for Health File Privacy Protection Based on Trusted Computing Technology

Xingkui Wang*, Jing Bian
School of Software, Taiyuan University of Technology, Jinzhong, Shanxi, China
**Corresponding Author.*

Abstract

Our objectives were to construct a security and reliable health information system protection measure and to provide a trusted terminal environment for medical information system. This scheme is to melt the credible computing idea into the medical information privacy protection. This melting makes the medical information be able to find a trust source and trust foundation in this application environment with high sensitivity and to further extend to the safety of the entire business system. In this scheme, TPM chip will take advantage of its own key management function, encryption and decryption function, platform identity attestation function and so on to provide the security support that is based on hardware for the file safety protection in HIS system. Designed a HIS file privacy protection scheme by adopting trusted computing technology. This module is to protect the files of all subsystems in HIS and to ensure that the files can reach a certain security requirements in the confidentiality, integrity and non-repudiation. This paper designed a scheme of medical file privacy protection based on trusted computing technology. Scheme on the basis of HIS system, through the analysis of files in the HIS system, security protection scheme is put forward based on trusted computing. From the aspects of confidentiality and integrity of medical records to privacy protection, and trusted computing use in the field of health information protection of high sensitivity based on hardware security features.

Keywords: *Health Information System (HIS), trusted computing, trusted computing platform, Merkle tree, privacy protection, digital signature*

I. Background

With extensive application of health information system, and the IT environment becomes more and more complex, that the security problem also gradually aroused people's concern and attention. The patient profile and detailed medical records are high-grade personal privacy in HIS system. Drug resource information, medical equipment procurement information and various resources usage records belong to the hospital's confidential information. Once this information is used by illegal to steal, which will give patients and hospitals caused great damage [1, 2]. Therefore, how to ensure the sensitive data don't be stolen and tampered, that is an important research direction.

Therefore, our must use security technology to solve problems related to privacy protection in medical treatment activity. At present, there have been a variety of methods and techniques used in the medical information privacy protection. To sum up basically has the following: deployment of firewall and intrusion detection system [3], vulnerability scanning to whole network through the security evaluation system, install antivirus system and safety management operation system, establish a data backup plan [4], building security management platform, encrypt data and safe storage.

In the above description of technological methods, the security of security measures depending on physical device is higher. But due to the high cost and problems that are difficult to be deployed, the good practicability and universality can't be able to be reached. But as for the safety measures that take the system software as means, although they have better flexibility and practicability and it is also relatively easy in upgrade and maintenance, in the malicious attacks, they can't still ensure the safety and completeness of the system. When considering the

security problems, it can only be believed that this software is the reliable source, but it is unable to confirm that whether this source is illegally tampered and attacked.

The core of credible computing platform is TPM security chip and the purpose of trusted computing is to protect the most sensitive information of client-side. When the attack occurs, the sensible encryption key will be protected. The design of TPM is very flexible and it can be applied in any problems in security field. TPM can gain the goals of protecting the security of terminal mainly through protecting the private security, detecting the malicious code, preventing the malicious code from using private key and protecting the safety of encryption key. These goals are accomplished by the public key authentication function, the integrity measurement function and identification function in TPM chip [5, 6].

In recent years, the information security circle closely combines the computing technology at the bottom and the password technology to promote the research on information security technology to enter the credible computing technological stage and this also makes the application of TPM wider and more comprehensive. As a means of protecting the safety of the terminal, the credible computing has been applied in all kinds of information security field and at the same time in medical information security field, the credible computing also has very big developmental space. Therefore in this paper, the credible computing technology is melted into the medical information privacy protection research schemes and TPM chip is used as the security trust source so as to construct a safe and reliable medical information system protection measure and to provide a credible terminal environment for medical information system.

II. Trusted Computing Platform

The purpose of trusted computing is to protect the most sensible information and when the attack occurs, the sensible key will be protected and not be used by malicious code. The trusted computing platform is a kind of comprehensive entity of software and hardware and it is able to provide the trusted computing service for system and to secure the reliability and availability of system and the security of information. The trusted platform module TPM is the core of trusted computing platform [7]. And TPM uses the password technique as the basic support and takes the protection of the safety of operating system as the core task and it is targeted at building a crucial systematic structure in information security filed.

The TPM system has two characteristics: one is to take advantage of the equipment on the platform to provide the unlimited security storage and the other is that the singly peerless status of TPM can ensure that the platform can record the system startup sequence in TPM in a trusted way [8, 9]. The TCG technical committee will realize the goal of protecting the terminal security by TPM through public key authentication function, integrity measurement function and identification function in TPM design.

The TPM has been designed to protect security by ensuring the above function. TPM ensure private keys cannot be stolen or given away、the addition of malicious code is always detected、malicious code is prevented from using the private keys、encryption keys are not easily available to a physical thief. For instance，malicious programs, such as spyware and Trojans, will be detected by changes in the PCR measurement, which can then cause the TPM to refuse to unseal sensitive data, or to refuse to use private keys for signing or decryption. If vulnerable or misconfigured programs are exploited, any changes they make to files can similarly be detected, and sensitive data protected. Any attempts to gain authentication secrets, such as by phishing or pharming, will fail, as the owner of the authentication private keys cannot give the keys away. Data encrypted under keys sealed by the TPM will be much harder to access in the case of theft, as the attacker would need to open up the chip to get its storage root key in order to be able to unseal the protected keys. (While possible, this is really difficult and expensive.) Similarly, encrypted communications are much more immune to eavesdropping, if the encryption keys are exchanged or stored by a TPM.

III. Merkle Tree

Merkle tree is also called as Hash tree. It was invented by Ralph Merkle in 1972, referring to such a tree structure: Each leaf node of the tree is a formation of Hash value of a block of data and the Hash value of all children nodes below each parent node are combined together to do Hash computing to get their parent nodes. This process can always go on until the root node of the tree is got. In 1989, Merkle further put forward the idea of credible tree and in the certification on credible tree advocated by Merkle, the signer can realize the certification on a large amount of data by a signature. Afterward, Merkle proposed the Merkle credible tree signature scheme based on credible tree. Merkle tree has been widely used in data encryption technology field and distributed storage field. The Hash value of root nodes can be regarded as public key and the authentication path can be used to detect the legality of corresponding data [10, 11]. Figure 1 just illustrates the basic structure of Merkle tree.

In the field of information security, Merkle tree is often used to solve the problem of "using smaller credible storage space to protect the large amount of data object that are stored in unreliable memorizer". Its basic idea is that the trusted components are responsible for the maintenance of Merkle tree and the read or updating operations on any data object must be implemented by trusted components and the trusted components must firstly use Hash tree to verify the integrity of data object before any operation [12]. In actual practice, as long as the root Hash is ensured to be safely stored in trusted memorizer, even if the nodes of Hash tree are stored in unreliable memorizer, the knowability of data tampering can also be realized. Because the Hash calculated value of interior nodes of Hash tree adopts non-collision Hash algorithm, if we can just make sure that the root Hash is reliably protected, so even if the attacker tampers some nodes of Hash tree, these nodes can still not be utilized to construct a Hash tree that owns the original root Hash but owns different children nodes.

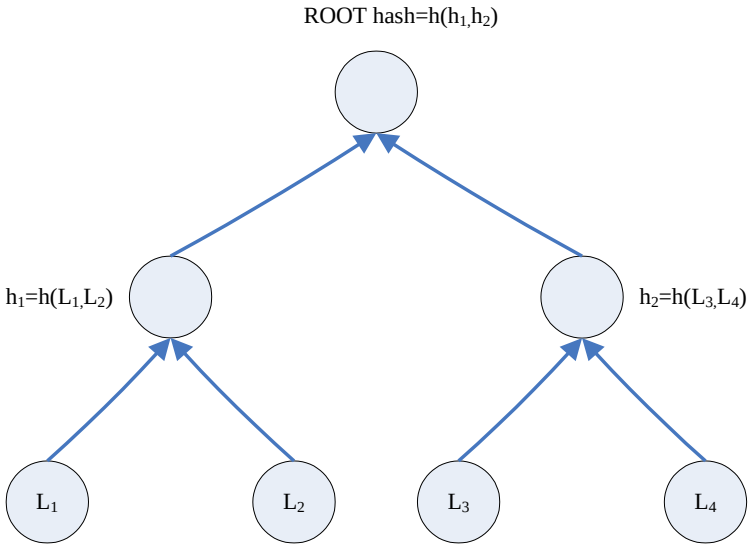

Fig 1: Merkle tree structure

In the application of the validation of trusted tree, Merkle Tree is used to carry out the integrity protection on keys in the signature process so as to ensure the safety of signature. In this scheme, Merkle Tree is also utilized for integrity protection but the protected object is the signed data so as to reach the purpose of using the same signature by many files. The use of this kind of digital signature method can solve the complicatedness and inconvenience at the time of signature by many associated files at the same time and moreover, the storage space that digital signature takes up can be reduced [13]. Merkle Tree method can verify the integrity of any one of files that constitute the signature. Once the file is tampered with, its Merkle Tree signature will correspondingly have the obvious change.

IV. File Privacy Protection Scheme for HIS

The privacy protection scheme mentioned in this paper is the file privacy protection scheme of HIS system shown in Figure 2 and the core feature of this scheme is to melt the credible computing idea into the medical information privacy protection. This melting makes the medical information be able to find a trust source and trust foundation in this application environment with high sensitivity and to further extend to the safety of the entire business system. This important goal can be gained by TPM.

In this scheme, TPM chip will take advantage of its own key management function, encryption and decryption function, platform identity attestation function and so on to provide the security support that is based on hardware for the file safety protection in HIS system.

(1). Key management function: TPM is used to generate and manage the master key and signature key of users and to store the encrypted key of protected files.

(2). Cryptography function: TPM key is utilized to encrypt the symmetric key and to protect the encrypted key of file. The digital signature is used to make signatures on files and platform information and to protect the data integrity.

(3). Identity authentication function: The identity of TPM is used to prove the AIK key, make signatures on relevant data on the platform, prove the credibility and integrity of platform and provide the identity authentication function of the platform.

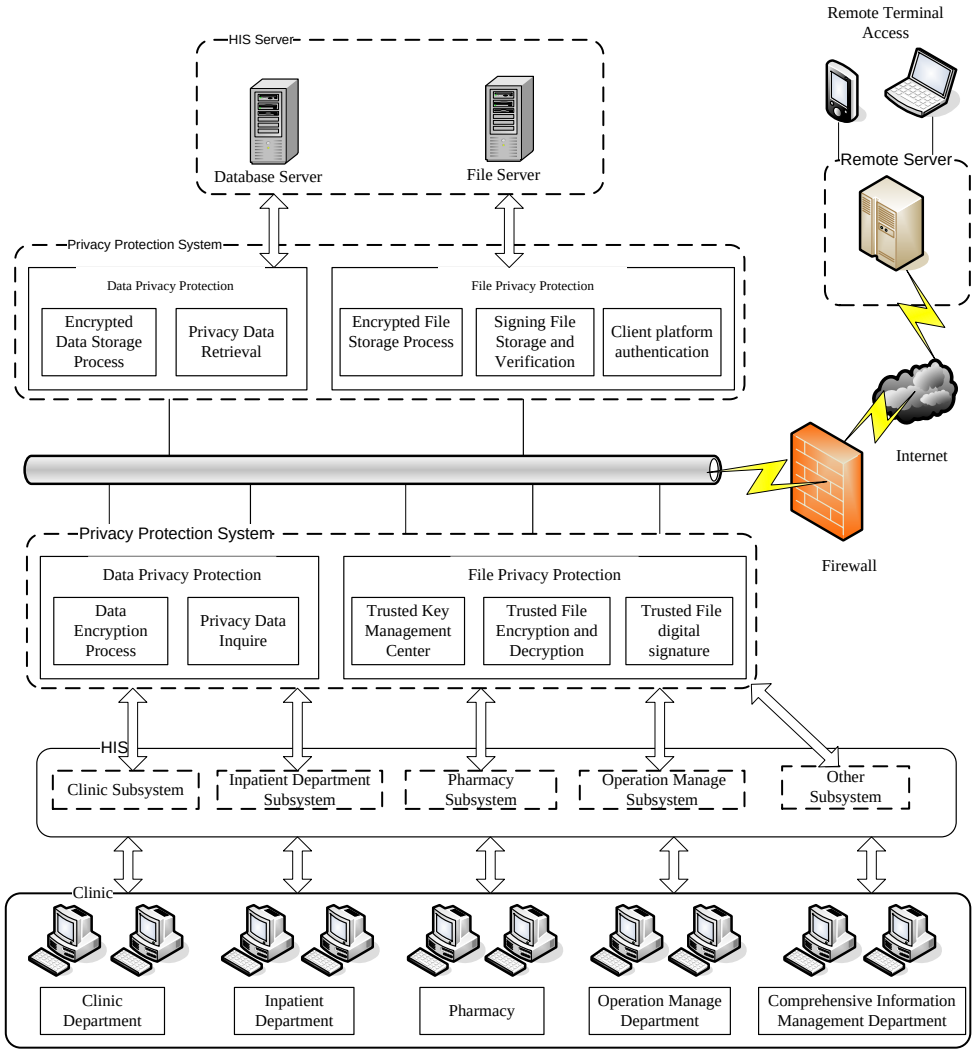

Fig 2: System structure chat of HIS

Except for the trusted root support based on hardware, this scheme also uses the encryption and signature technology in cryptography mechanism and protects the security of files in the process of browsing, visiting and transmission. The function modules that the file protection scheme mainly includes are as follows: key management, file encryption and decryption, file signature and file safety transmission. The purpose of these modules is to protect the files of all subsystems in HIS and to ensure that the files can reach a certain security requirements in the confidentiality, integrity and non-repudiation.

4.1 Demand analysis

4.1.1 Functional demand

The internal privacy protection of hospital information system is mainly for file and data and just as described in the previous part, the file is mainly stored in file server and data is mainly stored in database. This scheme is mainly targeted at the fire for security protection to meet the requirements of HIS on privacy protection function. These requirements can be attained mainly through the following several functions:

(1). File encryption storage: As for files that are not often used and are kept with copies in the daily work of hospitals, such as the patient's medical history out of the hospital, the hospital history information statistics and etc,

there is higher requirement for the confidentiality. Based on the characteristic of its low use frequency, in order to improve the system security, such kind of file is encrypted and stored in file server.

(2). File decryption review: as for files to be encrypted for storage, according to the business needs of hospital, when the material statistics and auditing and other operations are carried out, it needs to check the encrypted files and at this time the decryption function of file will be used.

(3). File signature: As for the data flowed in the daily business process in hospital, its use frequency is higher and it has certain requirements on the instantaneity of operation. Under such circumstance, in order to ensure the security and easy feasibility of files, the files focus on the integrity protection. The method is to do digital signature on files and the signature is mainly performed by operating doctors, administrative staff and other operating personnel who have right for performing files.

(4). File integrity authentication: When the commonly used files in business process is checked or modified, the signed files must be processed, the integrity verification must be done on signed files and the files shall be checked whether to be illegally tampered with.

(5). Key management: The right of users who do encryption and decryption, signature and validation shall be set and the keys of each user shall be managed, including operations such as establishing, modifying, deleting and resetting keys to realize the management of each user on personal key and the management of superior administrator on keys of users at all levels.

(6). File security transmission: The file of HIS system is stored in file server in the form of cipher text and the file must be uploaded onto the file server through security transmission channel after the file is generated by the client-side. This function includes two sub-functions of the integrity verification of client-side and the file encryption transmission and the two functions are able to do file transmission after firstly determining the credibility of client-side platform, thus improving the security of file transmission.

4.1.2 Security requirements

(1). Confidentiality

Confidentiality is a character that the information cannot be utilized or revealed by the unauthorized, entity or process. Since the target information protected by HIS is in the form of files and database, it involves the storage, researching and disclosure safety of information. Confidentiality is an indispensable major character in privacy protection. The confidentiality of this project is guaranteed by using cryptology technology. The confidentiality of private data in HIS must be particularly guaranteed, therefore, confidentiality is an important indicator of HIS security requirements.

(2). Integrity

Integrity means that data is tampered and utilized in an unauthorized way. Data integrity service should resist proactive threat, in order to guarantee the authenticity of information. The data in HIS is the information related to the patient’s individual privacy. Therefore, it goes without saying that the authenticity and non-tampering of this information is crucial to the patients. Hence, Integrity requirement is another important indicator of HIS security requirements.

(3). Non-repudiation

Non-repudiation is a character that ensure either party cannot deny the manipulation they once conducted in a system composed of receiving and sending parties, so that to be cheated halfway.

4.2 Conceptual design

The project proceeds from the fundamental principle of the protection for confidentiality and integrity of important files in health information system. Based on dependable computing as safety technical support, the files protection scheme is designed in combination with related characters of file system and medical data.

4.2.1 Multilayer key protection structure

In the trusted computing, the key security will be directly related to the safety of the entire trusted computing platform. Apart from the key algorithm, key management is an important measure of key security assurances and plays an important role in the Trusted Computing System.

The security of TPM root key is protected by a hardware chip. The key tree structure is constructed on the base of the root key, and is encrypted layer upon layer from the root key to protect the nodes in the tree. Therefore, the nodes of key tree structure corresponds to the nodes of the tree structure of the file system and TPM key tree structure can be introduced to the security of the entire file system. The key structural design of the program is shown in Figure 3.

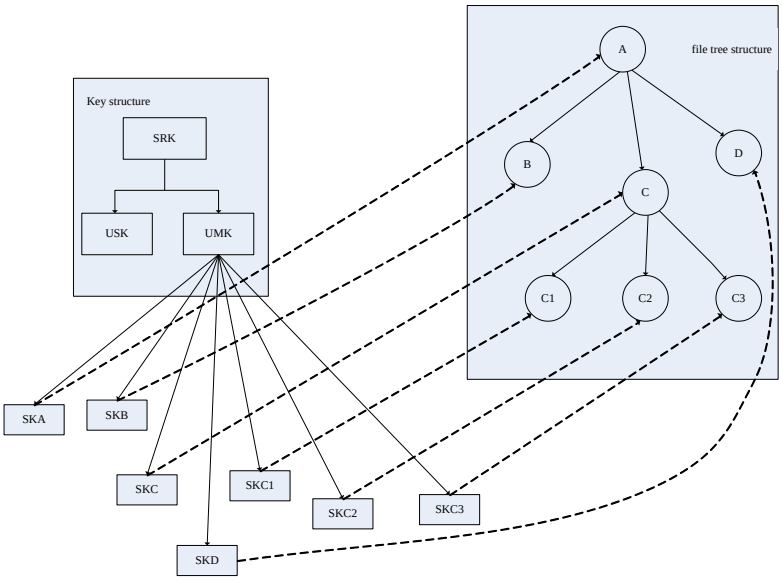

Fig 3: Cryptography key architecture chat

The basic idea of the key structure in Figure 3 is:

(1). Each TPM has only one storage root key SRK, bound together with a TPM chip and stored in the TPM inside. SRK is the root key of TPM key structure and is responsible for storing and protecting other keys. Each user has a master key UMK, which is to store and protect other keys for this user. The master key is generated in TPM, based on SRK as the root key as well as other keys that TPM produces, and it is responsible for encrypted storage and protection.

(2). UMK of each user is generated by the TPM, as asymmetric key it can encrypt and autograph for data. Here, we can generate two asymmetric keys for each user, one used for encryption and the other for signature. Both keys are respectively UMK and USK of the user. UMK is used to protect the key SK of encrypted files and USK is used to autograph digest value of data.

(3). The key of direct encrypted files is symmetric key, marked by SK, and using a symmetric key is to ensure the speed and processing efficiency of encrypting files. In order to ensure the safety of files, this program provides

AES encryption algorithm to encrypt files, and provides SHA-1 as a file hash algorithm of summary process.

4.2.2 Encryption and decryption of files

This scheme uses symmetric encryption algorithm in cryptography mechanisms to protect the confidentiality of documents. For the properties and uses of different files and considering the consumption and effects of the encryption process, we should protect documents of different types and levels of security by using encryption algorithm. AES symmetric encryption algorithms provided by this program can guarantee security and finish encryption as quickly as possible. To compensate for defects of symmetric encryption algorithms in security, this article uses the method that the TPM key protects file encryption key to indirectly complete protection of file security.

4.2.3 Digital signatures

(1). The digital signature of a single file

The program uses the signature and verification techniques that TPM chip provides to achieve digital signature of files. Firstly, we should do a hash algorithm processing of the file to form a digital summary of the file. The program uses SHA-1 as a hash algorithm. And then we sign for the hash value through the application layer interface functions provided by the TPM to reach the purpose of tracing file operator and to satisfy non-repudiation of the information source. When browsing files, we determine whether the file has been modified by a third party by verifying the signature checksum.

(2). The signature of multi-file based on Merkle Tree

The files in medical information system are divided by the patient as a unit such as electronic patient records file. After the doctor edits patient electronic medical records, he should sign for the modifications to ensure the integrity and non-repudiation of electronic medical records file.

However, when you autograph a patient's medical history, it will be more trouble in the operation if you turn to sign each subfolder. And it is likely to forget a file signature because of omissions. The program presents a signature scheme based on Merkle Tree according to the storage characteristics of electronic medical records. If you apply this signature scheme, you can make a signature of the whole file of a patient's electronic medical records and can also correctly verify whether the file has been illegally tampered with. This not only has advantages in terms of ease of use but also the guarantee of security and the management of the signature file is also more convenient.

In Merkle Tree signature scheme, the leaf nodes of the tree are the hash value of subfolders of the patient's electronic medical records.These subfolders use the patient as a unit and are independently stored in the system. At the time of signature, we should firstly do a hashing of each subfolder and use the operation result as leaf nodes of the hash tree. We construct a binary tree by these leaf nodes and record the hash value of each node in the binary tree. Finally, we do a digital signature for the hash value in the root location, which used as a signature of the corresponding patient's electronic medical records. When verifying the integrity of a subfolder, we need to use a signature of the hash value of the root node, the corresponding path from subfolders to the root and the public key of signature keys of electronic medical records. Figure 4 is the Merkle Tree structure of a digital signature that electronic medical records file corresponds.

4.2.4 Secure transmission of files

Secure transmission of files consists of two steps, integrity verification of client platform and encryption transmission of files. Server-side requires integrity certification of client platform of upload files and after that, it will generate a session key between trusted client and server, which is used for the next file transfer.

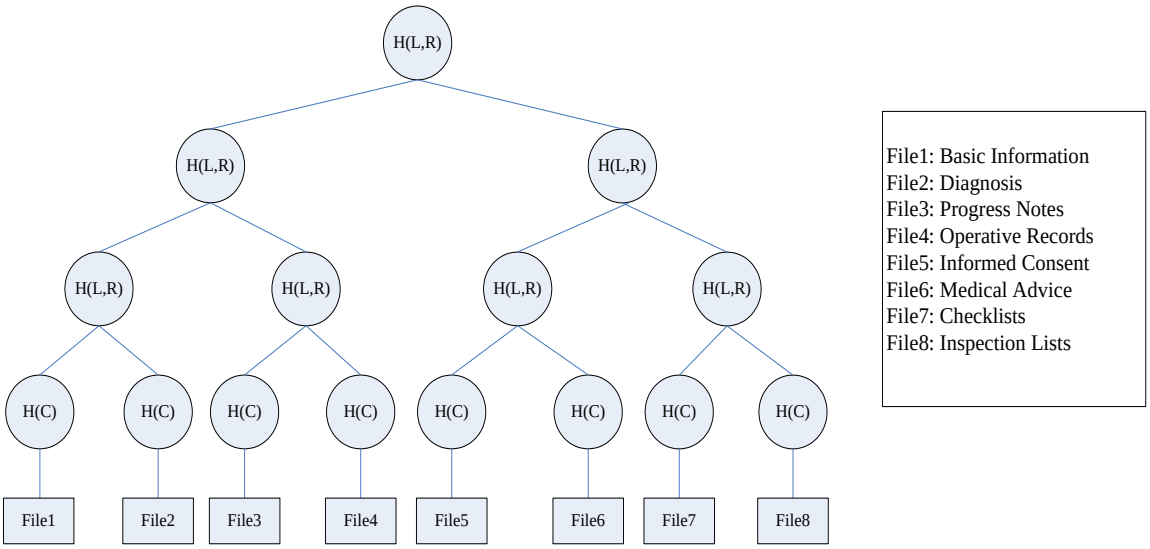

Fig 4: Merkle tree digital signature architecture design chat

On the basis of the platform information collected by PCR, the program uses the platform identity key AIK and make TPM sign the hash value in PCR. When a client requests to the server to upload data, it will send to the server platform status information encrypted by AIK private key in order to prove itself in a trusted state. Credibility certification of platform occurs before a file transfer. So only platform was recognized as a trusted status by the server, file transfer requests will be executed. Figure 5 shows the basic structure and the steps of the secure transmission of documents.

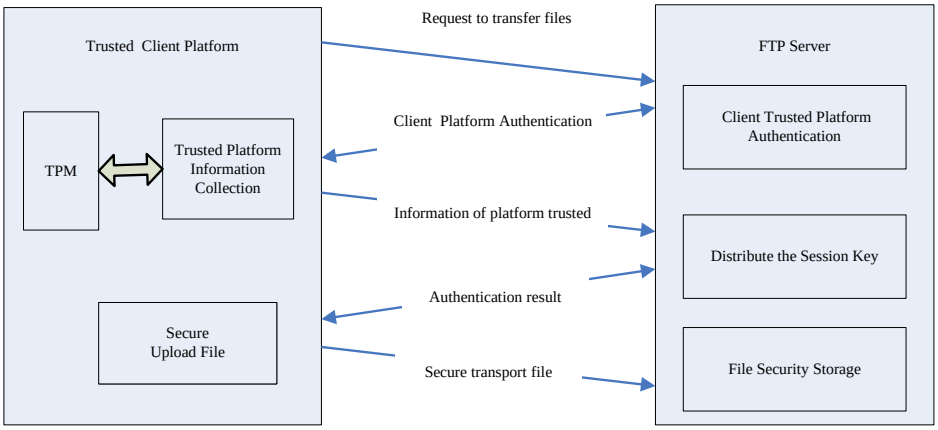

Fig 5: Secure file transmission flow chat

The main function of client is to provide a certification of platform credibility, and transfer files after successful authentication. Server-side tests and verifies platform credibility and provides safe transport key.

(1). Trusted client platform requests to upload files.

(2). Server requires the client to provide credibility certification of platform.

(3). The client uses the identification key AIK of TPM to sign for the platform integrity measurement value and send the certification data to the server.

(4). The server does an identity authentication for the client and sends the session key of secure transmission to the client after successful authentication.

(5). Clients use the session key for file encryption and secure file transfer.

Since a session key has been established between the client and the server during the authentication process, the encryption key is the session key during the file transferring process. To ensure security, data transmission is encrypted by the session key and data is transferred in plain text format. After the server receives the cipher text data, it will decrypt and save. Data here is firstly encrypted by the client's file encryption key and should be stored in the appropriate storage location after decryption of the server.

V. Conclusions

This paper designed a scheme of medical file privacy protection based on trusted computing technology. Scheme on the basis of HIS system, through the analysis of files in the HIS system, safety protection scheme is put forward based on trusted computing, such as Key management, encryption, signature and authorization. From the aspects of confidentiality and integrity of medical records to privacy protection, and trusted computing use in the field of medical information protection of high sensitivity based on hardware security features. This Scheme introduced the design of the specific details. Firstly, we provide key centralization management mechanism, which consists of management，distribution, protection of cryptology key in HIS. Secondly, we Provide trusted file secure storage, it transmit encrypted file to file server. Thirdly, the scheme is put forward a kind of digital signatures based on combination of Merkle Tree structure and trusted computing. It provides integrity protection and reduces storage space and complexity of the signature, while improves computation efficiency. Finally we also proposes trusted platform identity authentication, which based on TPM metrics data, instead of the traditional password-based identity authentication and providing a guarantee to documents transmission. The whole design from the medical data generation and transmission communication to storage, throughout the business process.

References

[1] C.R. Thomas, “Privacy information technology, and health care,” Communications of the ACM, vol. 40, no. 8, pp. 93-100, 1997.
[2] S. Gritzalis, C. Lambrinoudakis, D. Lekkas, “Technical guidelines for enhancing privacy and data,”
[3] X.H. Le, S. Lee, Y.K. Lee, et al., “Activity oriented access control to ubiquitous hospital information and services,” Information Sciences, vol. 180, no. 16, pp. 2979-2990, 2010.
[4] R. Thibadeau, “Trusted computing for disk drives and other peripherals,” IEEE Security & Privacy, vol. 4, no. 5, pp. 26-33, 2006.
[5] TPM Main Specifikation V1.2[DB/OL]．https://www.trustedcomputinggroup.org/home.2003-10．
[6] Trusted Computing Group, “TCG Specification Architecture Overview, Specification Revision 1.4,” https://www.trustedcomputinggroup.org/groups/TCG_1_4_Architecture Overview.pdf, August 2007.
[7] W.F. Edward, “Understanding trusted computing: Will its benefits outweigh its drawbacks?” IEEE Security and Privacy, vol. 1, no. 3, pp. 60-62, 2003.
[8] B. Parno, J.M. McCune, and A. Perrig, “Bootstrapping trust in commodity computers,” IEEE Symp. Security and Privacy, vol. 4, no. 3, pp.414-429, 2010.
[9] S. Gurgens, C. Rudolph, D. Scheuermann, M. Atts, R. Plaga, “Security evalua-tion of scenarios based on the TCG’s TPM specification,” ESORICS, vol. 8, no. 2, pp. 438-453, 2007.
[10] J.K. Hu, H.H. Chen, T.W. Hou, “A hybrid public key infrastructure solution (HPKI) for HIPAA privacy/security regulations,” Computer Standards and Interfaces, vol. 32, no. 5, pp. 274-280, 2010.
[11] R.C. Merkle, “Protocols for public key cryptosystems,” IEEE Symp. Security and Privacy, Washington: IEEE Computer Society, vol. 4, pp. 122-134, 1980.
[12] X.F. Wang, F. Hong, X.M. Tang, “Merkle tree digital signature and trusted computing platform,”

Wuhan Univeraity Joumal of Natural Sciences, vol. 11, no. 6, pp. 1467-1472, 2006.

[13] D. Bauer, D.M. Blough, D. Cash, "Minimall information Disclosure with Efficiently Verifiable Credentials," The 4th ACM Workshop on Digital Identity Management (DIM2008), Alexandria, Virginia, USA, vol. 10, pp. 112-120, 2008.