Acta Technica *62* (2017), No. 3B, 829–842

Research on data security of hospital information system which is based on internet medical big data

Yuebo Shen[2], Lianru Zhou[3], Shaojun Duan[2], Yuheng Luo[2]

Abstract. With the rapid development of medical information technology at home and abroad, and the wide application, popularization, improvement of the hospital information system, security issues of information systems and data are becoming increasingly prominent. This paper based on the use of advanced security technology to design the security control measures, strategies, programs, structures and the configuration of hardware and software function needed under the cloud computing environment, all of which are suitable for hospital big data. The aim of this paper is to conduct a good job in all aspects of security and defense measures, to design data security programs for hospital information system, so as to provide a reliable guarantee for the safe operation of the system.

Key words. big data, hospital, information system, data security, research.

1. Introduction

Hospital information system (HIS) refers to the use of modern means like computer hardware and software technology and network communication technology to comprehensively manage hospitals and the stream of people, logistics, financial flow of each department, and to acquire, store, process, extract, transmit, gather and transform the data generated in all stages of medical activities into various information, thus to provide for the overall operation of the hospital a comprehensive, management-automated information system which supplies a variety of services. Hospital information system is an indispensable infrastructure and supporting environment in the construction of a modern hospital, whose key function is clinical

[1]Acknowledgment - We acknowledge the foundation of Hebei Health and Family Planning Commission Research Projects: Research on data security of hospital information system which is based on Internet Medical big data. And the code is: 20160419.

[2]Workshop 1 - Department of Information, Children' Hospital of Hebei Province

[3]Corresponding author: Lianru Zhou ;email:zhoulianru@126.com

application. The system can meet the clinical application of the hospital to serve the patients. From this point of view, hospitals setting up this system can achieve the goal in two aspects, namely, medical quality control and work efficiency improvement. However, the two goals are achieved from three levels and four aspects. Three levels refer to the business layer, management layer, and decision-making layer. Hospital information system can meet different levels of needs of hospital staff to increase the efficiency and quality of work. Since the work of the three levels of hospital staff involves people, money, material and business, so it can be said that the hospital information system can meet the needs of different levels of work of different staff in the hospital, improving the efficiency of hospital work and medical quality, thus to better serve the patients. The hospital information system is a multi-module, multi role, multi service system that its security threat is relatively complex. This paper designs a role-based access control model based on constraints like time and space environment, in order to improve the traditional one to help it better meet the safety needs of hospital information system. At the same time, through the improved AES encryption algorithm, this paper has verified that the S- box constructed in the algorithm has better algebraic properties, enhancing the security of data encryption.

2. Principles of data security

2.1. Security management principles of data access

The application of hospital information system in all departments of hospitals has become more and more widely, and various information sharing. Exchange and transfer continue to expand. All these factors easily lead to data leakage or damage. Therefore, it is needed to develop reasonable safety management limit, such as access control, identity authentication, data encryption and digital signature, etc.

(1)The password management; (2) According to the different management responsibilities, different departments and different properties to divide the use authority; (3) According to personnel identity to arrange their right of storage and accessing to the database ;(4) some servers without needs are closed.

2.2. Redundancy principle

Hospital information system belongs to online transaction system that needs twenty-four hours of uninterrupted operation, such as clinical laboratory, hospitalization, medicine distribution and charging, which cannot have any data leakage or loss. Once the data leakage occurs, it will lead to huge losses or even catastrophic consequences. Therefore, the safe operation of the hardware equipment of hospitals is important. In order to ensure the normal operation of them, we have to implement redundancy design of hardware equipment, aiming to ensure that any environment in computer network system can work smoothly, and when there is a problem, the system can automatically switch over the work, not need to interrupt the operation of the system running. The following devices need to implement redundant design in the information system.

(1) The link of the network, including twisted pair and fiber. (2) The server and internal network card, hard disk, fan and power. (3)The storage device and the internal disk controller. (4) The switch, internal fan and power.

2.3. Principle of reliability

We can elaborate the reliability principle from four aspects. First, the intrusion detection technology; at present, one of the main factors influencing the network security is hacker intrusion. To prevent hackers hacking hospital LAN, it is necessary to build a special regulatory monitoring system to achieve the real-time monitoring of each of the key nodes in the computer network, and collect relevant information and make analysis to figure out relative strategies to make fight and defense. Second, the desktop management; use the same control center configuration of different modules to make computer desktop management, monitoring every workstation running situation through the relevant measures, including a variety of port control, server management, IP address management, license control and supervision of software, vulnerability monitoring system and the management, software upgrade, remote control, patch distribution and problems prevention of hardware asset, in order to discover and solve the problems as far as possible. Third, the hardware firewall, a simple firewall filter, which is also called gateway, can not only manage and supervise network data by setting access and accessed rules, but also it can make the network control strategy, monitor and filter information in the network, and record faithfully activities and information contents through computer firewall. If there appears a network attack, it can be in a timely manner and the system will give an alarm, thus to exclude unauthorized and malicious intrusions, protecting the data security of network internal sensitivity. Fourth, the backup of the database; realize the database protection through the disk array and software backup, image technology, full cooperation of the tape library.

3. Data security prevention strategies

3.1. Hardware security measures

Physical security refers to the physical protection of various hardware information assets of a hospital information system from man-made or natural damages. This requires designing security policy of different types of information assets respectively, including the maintenance of center room, server, and workstation, and hardware interface equipment management.

The center room, as a processing center of hospital information, should strictly maintain its working environment, and according to the requirements of the equipment in the engine room to strictly control the indoor temperature and relative humidity; take the necessary control access system to control personnel flow; use multiple power supply, and equip with backup uninterrupted power supply to ensure the stability and continuity of the power supply in the center room; install and properly use lightning protection device, anti-magnetic field interference device and

other devices.

As the core of the hospital information system, the server plays a leading role in the hospital information system, if the server fails, it may occur data loss, business interruption, even system participation. Therefore, to ensure that the server can work uninterrupted, and ensure its stable, reliable, efficient operation, we should apply the redundancy set, and adopt multi machine fault-tolerant and multi machine hot backup solutions. Using the dual server, no matter when the main server has problems, the subordinate server can substitute the function of the core server. In addition, it is needed to equip the server with UPS power in high quality, high reliability, which can work for a long time, and also to take redundant configuration.

The workstation is the terminal PC equipment used by doctors, nurses from various departments of the hospital, and each workstation can be regarded as an independent business module of a hospital information system. Workstations are spread in departments and wards, so the environments of their location are very different. Since the workstation itself does not store data, it is necessary to do a good job in heat dissipation, dust proof and damp-proof of it to a largest degree under a relatively suitable work environment; strictly regulate the use of floppy disks and CD ROMs; forbid the installation of floppy drives, CD-ROM, and USB interface shielding; monitor users' behavior and equipment information through network management software.

Hardware interface equipment management includes the maintenance and management of all routers, switches, twisted pair and fibers which can access to the interface equipment. The switches, routers, hubs and other equipment are required to be locked in the cabinet. External mobile PC access is prohibited. In addition, it is also vital to conduct registration management on the port of transmission cable and to establish strict equipment management system.

3.2. Identity authentication strategies

In this paper, we propose an identity authentication algorithm based on the key sequence characteristics, and the algorithm is described as follows:

(1). Data processing

According to the assumptions of Saleh Bleha and Leggett et al., the time series of the strike are satisfied with the normal distribution. The reason why we sort the key sequence into 2 matrices:$A_{mn}(pr), A_{mn}(pp)$ is that use only the two matrices can calculate all the key sequences and intervals, among which, the element of $A_{mn}(pr)$ is the interval between a key is pressed down and uplift again, while the element of $A_{mn}(pp)$is the interval between a key is pressed down and another key is pressed down.

(2). Training process

All the collected m vectors are organized as the sample matrix:$A_{mn} = [a_1, a_2, ..., a_m]^T$??$a$ is the row vector of the n-dimensional vector. Calculate the mean and standard deviation of each dimension of the matrix elements:

$$\mu_k = \frac{\sum_{i=1}^{m} \alpha_{ik}}{m}, k \in (1, n) \tag{1}$$

$$\sigma_k = \sqrt{\frac{\sum_{i=1}^{m}(\alpha_{ik} - \mu_k)^2}{m-1}} \tag{2}$$

For each vector elementα_{ik} to calculate $\Delta = \alpha_{ik} - \mu_k$, if $\Delta > 3\sigma_k$, thenα_{ik} is removed from the matrix??replaced by μ_k, and carry out the operation recursively until no elements are satisfied with$\Delta > 3\sigma_k$. Record the final vectors$\mu_k$andσ_k, and also formation vectorsμandσ.

(3). Detection process

Step 1 Determine test vector$t = (t_1, t_2, ...t_n)$,among which, t_k has the following formula:

$$p_1(t_k) = 1 - 2\int_{\mu_k}^{\mu_k + |\mu_k - t_k|} \frac{1}{\sqrt{2\pi}\sigma_k} \exp[-\frac{1}{2}(\frac{t_k - \mu_k}{\sigma_k})^2]d_t \tag{3}$$

In achievement of programming, we can use the cumulative distribution function of C++ standard library function to calculate the probability of the fixed point in the test vector, that is:

$$p_1(t_k) = 2 * CDF[\mu_k - ABS(\mu_k - t)] \tag{4}$$

This avoids the cumbersome process of seeking points. CDF refers to the cumulative distribution function, while ABS is the function to of taking the absolute value.

Step two: take the 10 minimum values of the generated probability:$(s_1, s_2, ..., s_{10})$, and carry out weighted processing on them.

Step three: the weighting procedure is as follows:

1. For the given vectors$(s_1, s_2, ..., s_{10})$, endow weight$\widetilde{w} = (\frac{1}{10}, \frac{1}{10}, , ..., \frac{1}{10})$,based on the following formula:

$\overline{s} = \frac{1}{10}\sum_{i=1}^{10} S_i$ $\sigma_s = \sqrt{\frac{1}{9}\sum_{i=1}^{10}(\overline{s} - s_i)^2}$ (4)

To figure out the mean$\overline{s}$and standard deviationσ_s. At that time, with$\overline{s}$andσ_s,a normal distribution is determined:$N(\overline{s}, \sigma_s^2)$

1. For the given vectors$(s_1, s_2, ..., s_{10})$ use the mean $\overline{s}$and standard deviation σ_s to do standardized treatment, that is:

$\beta_i = \frac{s_i - \overline{s}}{\sigma_s}$, obtaining $(p_1, p_2, ..., p_{10})$

1. According to the following function, we can figure out the possibility$(q_1, q_2, ..., q_{10})$of p_i in $(p_1, p_2, ..., p_{10})$ in the normal distribution$N(\overline{s}, \sigma_s^2)$.

$$q(p_i|\,\overline{s}, \sigma_s) = \frac{1}{\sqrt{2\pi}\sigma_s} e^{-\frac{(p_i - \overline{s})^2}{2\sigma_s^2}} \tag{5}$$

2. For the obtained $(q_1, q_2, ..., q_{10})$??according to the following formula??

$$w_i = \frac{q_i}{\sum_{j=1}^{10} q_j} \tag{6}$$

Do unit processing to get$(\omega_1, \omega_2, ..., \omega_{10})$ that is the weight vector.

Step four: finally, we can get$score = \frac{\sum_{i=1}^{10} s_i \omega_i}{10}$.

3.3. Access control policies

At present, in the process of rapid development of hospital information system, the traditional access control policy based on role and static authorization mode cannot adapt to the development trend of the current information system's distribution and complexity.

The model designed in this paper is as follows:

1. The basic idea of the model: users of information system access to the information system in a certain role, and their access behaviors are restricted by the access control rules of the time and space. In this way, by the addition of specific access constraints of time and space in the access behavior, we can effectively control the access behavior.

2. The basic principles of the model as shown below:

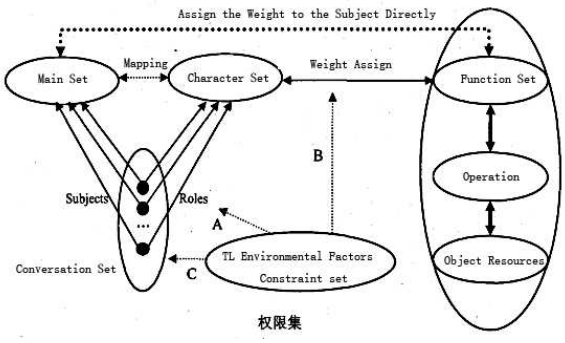

Fig. 1. Schematic diagram of model principle

The Model theory mentioned above includes two aspects:

(1) Develop all kinds of sheets of a hospital information system, and establish the database. This includes the following work: first, based on user subject classification and information asset identification, hospital information security departments establish user table and object resource table to describe the characteristics of both; second, according to the scope of administrative levels and responsibilities of the main users to create a role table for the hospital information system; third, determine the relationship between the subject and the role to form session set; fourth, on the basis of the function modules contained in hospital information system to create operations that can be achieved and to establish a corresponding authority list of object sources.

(2) Achieve the assignment from the subject to the role based on the corresponding relationship between the session set; assign rights and allocate authority for each role in the role list. When the main unit, object and behavior have any change, increase or deletion, we can directly assign permissions on the subject temporarily, avoiding the tedious adjustment of role authorization scheme.

3.4. Authorization policies

This paper mainly adopts the improved hierarchical authorization policy. In hospitals, the highest authority institution can be served by the information security management department of hospitals; and then the department will identify all information assets under distributed environment, and establish the highest authority management strategy; then it allocates the access control permissions of the system resource to the managers of all authorization management institutions in distributed environment; the managers of these institutions set the authorization policy of their own layer, and then according to the hierarchical structure of the subordinate roles to make authorization. In this way, the strategies set by higher managers constitute the upper strategies, while strategies set managers at each distribution point constitute the lower strategies. The upper layer strategies have a restraining effect on the lower level strategies.

In this paper, an improved hierarchical authorization strategy is proposed as follows:

The authorization verification process of this strategy is subdivided into functional modules and data access authorization verification. Module verification is used to identify which function modules users can access to, while data verification is applied to extract the data users can access to. Verification steps are shown in the above figure. It can be seen that users have an obligation to enter the username and password for the user identity authentication. If the authentication is not legitimate, then it will return to the login page. Otherwise, it will enter into the access control process, and the related information and the operating authorization of this legitimate user will be displayed. For example, get the function module information. If the user has the function module permission, then the user data access right will be verified again after obtaining the module. In accordance with the order of user authentication, function module permissions verification and data access verification, the security of access control is enhanced to a large extent.

3.5. Network communication protection strategies

With the gradual improvement of hospital information construction, the core businesses of hospitals become increasingly dependent on the hospital information system. In hospital information system, the financial data, patients' medical records and other information data have long been the key information of the entire hospital. Implementation of hospital business based on information technology, on the one hand, improves work efficiency and reduces management costs; on the other hand, it also prompts some illegal personnel to steal and tamper data to seek illegal

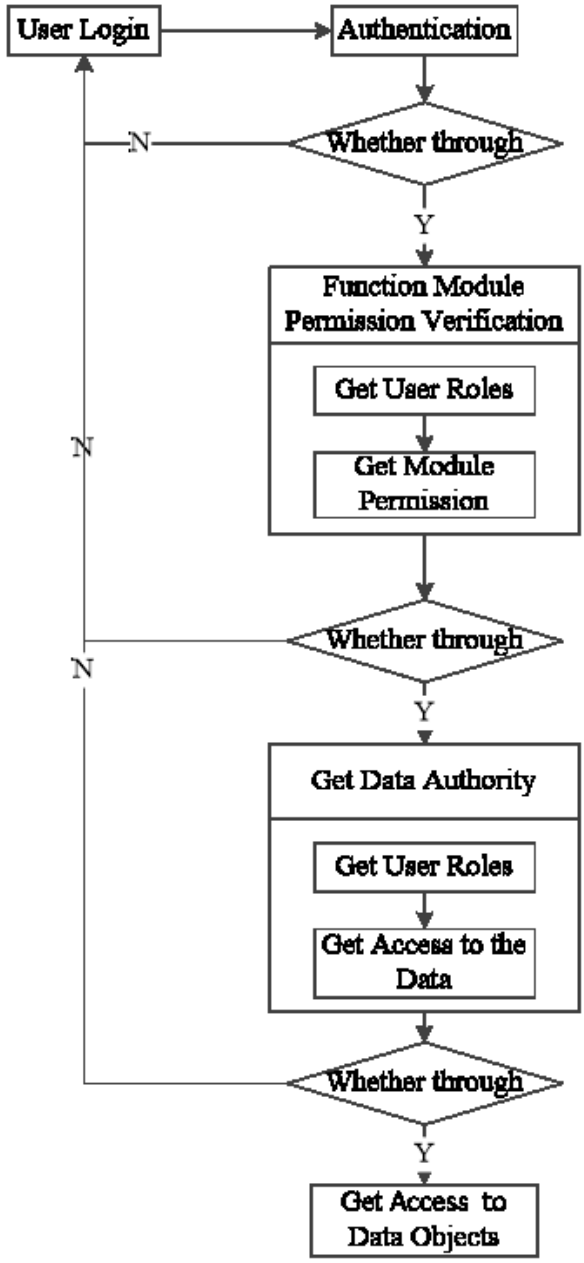

Fig. 2. flow chart of improved hierarchical authorization policy

interests. At the same time, the virus, Trojans and other hazards based on system vulnerabilities are very serious, as many hospitals have the experience that their business communication was interrupted owing to the outbreak of the virus, leading

to the loss of data.

The principal method to solve this problem is to install the intrusion detection system, whose function is to monitor the network traffic and launch a warning for the abnormal traffic. These conditions include the source and purpose, but the information has no significance for network managers to deal with security incidents since to handle network security incidents, we must trace back to find the root of the problem, or even to locate people. Only in this way, can problems be solved thoroughly. As a result, just providing the location is not sufficient. We can link this system with the security policy server to make the hospital information system to become an automatic defense network which has a series of functions, such as automatic network attacks defense, automatic repair of the consequences of attacks, automatic security policy learning, etc.

The protection of network communications equipment also needs to be strengthened, which is mainly shown in the following aspects:

(1)Important switch in the core room should have high performance and adopt the redundancy scheme, using Gigabit bundle to realize the interconnection between two important switches. Except for this, it is also needed to adopt preventive network router or switch fault protocol to achieve hot standby. If one switch does not work due to failure, then another switch can take over all of its business to ensure the normal operation of important application.

(2) In the core switch management process of the center workstation, VLAN technology is used commonly, which distributes the relative servers into special segments, and then in accordance with the properties of department or geographical location to distribute information data into another network segment, providing network management software for the switch, so as to implement effective regulation on data packets, IP resources and traffic.

(3) Manage to cut off the physical connection between INTERNET network and local systems, namely the PACS, LIS, HIS and RIS of hospitals, which can prevent the potential risks. If INTEERNET is integrated with the PACS, LIS, HIS and RIS of hospitals, the preventive measures of virus, external hackers should be strengthened, such as desktop software management, enterprise network anti-virus software and intrusion detection.

3.6. Data encryption strategies

The security case of hospital information system database based on data encryption should be managed well; The key of hospital information system based on data encryption does not leak; The information system authorization information of hospital based on data encryption should not be tampered; the hospital information system based on data encryption should ensure the correctness of the security function provided by the system database safe box. The security function of the hospital information system database based on data encryption on the system database safe box should be authenticated by the hospital information system based on data encryption. Besides, it is necessary to use improved AES encryption algorithm in a hospital information system based on data encryption.

In the whole encryption process of AES algorithm, in addition to the initial and final round of encryption, encryption in other rounds all use the following four switches: Sub Byte, Shift Row, Mix Column and Round Key Addition, while the initial round just adopts Round Key Addition, and the last round does not have Mix Column switch. AES encryption process diagram is shown in figure 4-2:

In the traditional AES algorithm, there are the following problems: the algebraic expression of S-box or inverse S-box is too simple, which is related to the calculation sequence of multiplicative inverse and affine transformation in the construction of S-box, and affine transformation period and iterative output cycle are related to the affine transformation pair adopted, so the algebraic properties of S-box can achieve better results by modifying the order of calculation and adjustment of S- box affine transformation pair. But if only using an affine transformation, it cannot be guaranteed that the algebraic expressions of the S- box and inverse S- box constructed have enough terms. To solve the above problems, this paper put forward the improvement scheme of constructing S- box, which is achieved through three steps: do an affine transformation on the byte elements, and then calculate multiplicative inverse element, finally to do the affine transformation again.

According to the design idea of AES and four principles of affine transformation design, we get 91 pair of (u, v) making $L_{u,v}$has a replacement table with only one cycle 256, expressed as a decimal(1, 4)(2, 109)(7, 156)(8, 111)(11, 219)(22, 39)(25, 238)(31 213)(32 91)(35 85)(37 61) (38 43)(41 49)(42 2)(44 80)(47 156)(50 9)(52 139)(55 110)(61 72) (62 9)(64 2)(67 147)(69 89)(73 6)(76 180)(79 51)(81 53)(87 112) (88 20)(91 178)(94 228)(97 21)(100 147)(104 102)(107 57)(109 6) (112 28)(115 30)(117 73)(118 63)(121 106)(127 3)(128 2)(131 29) (137 35)(138 154)(143 21)(148 126)(151 69)(152 8)(155 154)(157 27) (161 18)(167 111)(168 149)(171 197)(173 175)(174 164)(176 83)(179 56)(181 134)(182 118)(185 197)(188 65)(191 72)(193 95)(194 1) (200 57)(203 57)(206 133)(208 53)(211 53)(213 40)(214 70)(218 32) (220 1)(223 88)(227 219)(229 18)(233 40)(239 3)(241 161)(242 89)(247 126)(248 3)(251 9)(253 28)(254 141).

That is to say, carrying out an affine transformation with any of the above coefficients, we can find that the S- box obtained exists in the whole space as for the iteration, and can satisfy the rules of AES affine transformation. Calculate the 91 pairs of affine transformation one by one, finding that the avalanche distance of(1, 4)(2, 109)(7, 156)(8, 111)(11, 219)(22, 39)(25, 238)(31 213)(32 91)(35 85)(37 61) (38 43)(41 49)(42 2)(44 80)(47 156)(50 9)(52 139)(55 110)(61 72) (62 9)(64 2)(67 147)(69 89)(73 6)(76 180)(79 51)(81 53)(87 112) (88 20)(91 178)(94 228)(97 21)(100 147)(104 102)(107 57)(109 6) (112 28)(115 30)(117 73)(118 63)(121 106)(127 3)(128 2)(131 29) (137 35)(138 154)(143 21)(148 126)(151 69)(152 8)(155 154)(157 27) (161 18)(167 111)(168 149)(171 197)(173 175)(174 164)(176 83)(179 56)(181 134)(182 118)(185 197)(188 65)(191 72)(193 95)(194 1) (200 57)(203 57)(206 133)(208 53)(211 53)(213 40)(214 70)(218 32) (220 1)(223 88)(227 219)(229 18)(233 40)(239 3)(241 161)(242 89)(247 126)(248 3)(251 9)(253 28)(254 141) is 428 the avalanche distance of (52 139)(67 147)(104 102)(161 18)(208 53) is 424 the avalanche distance of (87 112)(117 73)(171 197)(174 164) is 412 the avalanche distance of (47 156)(94 228)(118 63)(121 106)(151 69)(157 27)(179 56)(188 65)(203 57)(229 18)(242 89) is 368 the avalanche

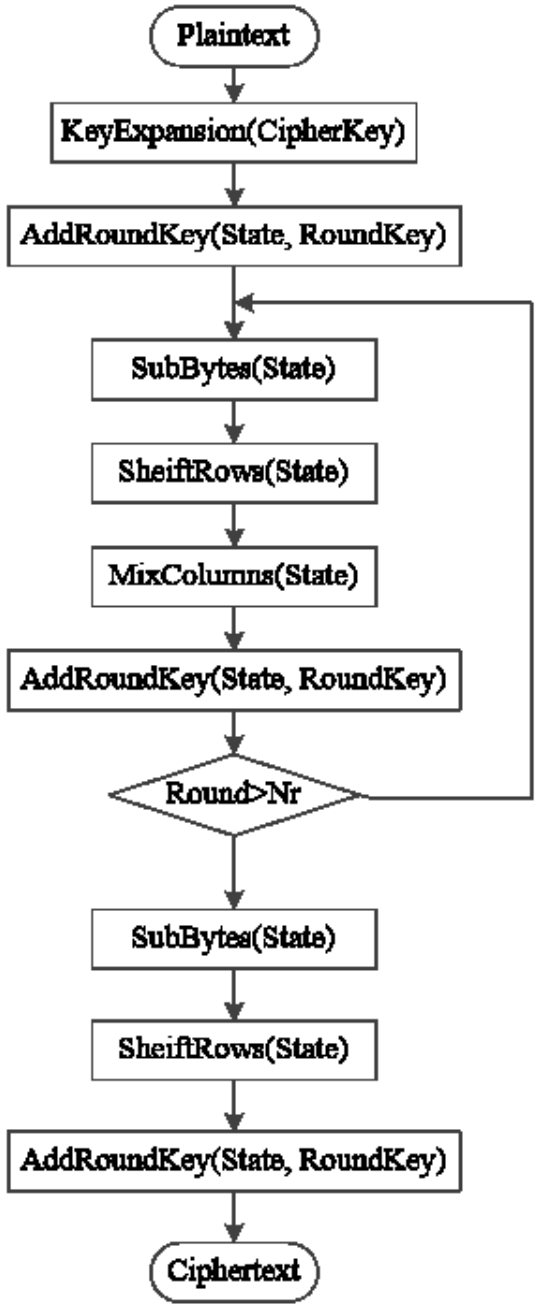

Fig. 3. Encryption process of AES algorithm

distance of (127 3)(191 72)(223 88)(239 3)(247 126)(251 9)(253 28)(254 141) is 348 the avalanche distance of (61 72) (79 51) (167 11)(211 53) (233 40) is 304. Accord-

ing to the definition of avalanche distance, the smaller the distance is, the better the spread of algorithm is. So randomly choose one pair from (61 72)(79 51)(167 111)(211 53)(233 40) and the operation steps of the improved scheme of S- box are as follows:

(1)Do an affine transformation, and the affine transformation selected is (167111), whole corresponding sixteen decimal is ("A7", "6F"). The specific operation is as follows:

$$x^{'} = Lb \times x +' 6F' = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 \end{bmatrix} \begin{bmatrix} x_7 \\ x_6 \\ x_5 \\ x_4 \\ x_3 \\ x_2 \\ x_1 \\ x_0 \end{bmatrix} + \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} \quad (7)$$

(2) Calculate multiplicative inverse??$x^{'} = (x^{n})^{-1} = \begin{cases} (x^{'})^{254}, & x^{''} \neq 0?? \\ 0 & x^{''} = 0 \end{cases}$

(3)Do an affine transformation again, and the affine transformation is??'A7'??'6F'). The output result y is obtained:

$$y = Lb \times x^{'} +' 6F' \quad (8)$$

4. Conclusion

This paper puts forward a set of complete and effective information security strategies and implementation methods for hospital information system. The method is composed of five parts, respectively, sensible security policy, access control strategy design, authorization strategy, terminal host protection strategy, network communication and protection strategy, and disaster recovery strategy which are closely related to each other. Each link puts forward clear logic, easy operation methods, which have high efficiency and usability in the design, implementation, operation, supervision and management of the system, providing a standard paradigm for the information security of the hospital information system. In the security strategy, this paper proposes the identity authentication algorithm based on fundamental sequence characteristics, improving the reliability of the identity authentication. This paper introduces a role-based access control model based on constraints like time, space environment, etc., to improve the traditional role-based access control model, so as to better meet the security requirements of a hospital information system. Besides, this paper also presents an improved AES encryption algorithm, verifying the algebraic properties of S- box constructed in the algorithm, which has strengthened the security of the data encryption.

References

[1] M. Tapiador: *Fuzzy Keystroke Biometrics on Web Security.* Proceedings of IEEE Workshop on Automatic Identification Advanced Technologies (2010), 133–136.

[2] M. S. Obaidat, B. Sadoun: *Verification of Computer Users Using Keystroke Dynamics.* IEEE Trans. on Systems, Man and Cybernetics *27* (2011), No. 2, 261–269.

[3] O. BAUDRON, H. GIBERT: *Report on the AES Candidates.* Second Advanced Encryption Standard Candidate Conference (2013), 53–67.

[4] C. Pt7eeger, P. PlaceShari: *Security in Computing.* Upper saddle placeCityRiver (2012).

[5] K. Anil, A. Ross: *An Introduction to Biometric Recognition.* IEEE Transactions On Circuits And Systems For Video Technology *14* (2014), No. 1, 4–2.

[6] B. Saleh, S. Charles: *Balsam IEEE Transaction on Pattern E. Computer-access Security Systems Using Keystroke Dynamics.* Analysis and Machine Intelligence *12* (2010) 1217–1222.

[7] R. LIDL, H. NIEDERREITER: *Introduction to finite fields and their application.* Fast Software Encryption *5* (2015), No. 10, 125–140.

[8] Y. F. Zhou: *Information technology Security techniques Guidelines.* the management of IT security (2011).

[9] R. Lal: *Common Criteria for Information Technology Security Evaluation version.* Indian Journal of Pure and Applied Mathematics (2009).

[10] N. C. Broering, M. Corn, W. R. Ayers: *a diagnostic prompting computer system, at the placePlaceNameGeorgetown PlaceTypeUniversity PlaceNameMedical PlaceTypeCenter.* Implementing RECONSIDER *76*, (2012), No. 2, 155–158.

Received November 16, 2017