IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS), ISSN: 2249-9555
Vol. 2, No.5, October 2012

Secure Protocols in Health Care System

A.B Rajesh Kumar,
Dept of Computer Science,
S.V. University, Tirupati, A.P. India
subhashamud@yahoo.com

Prof. M. Padmavathamma
Dept of Computer Science,
S.V. University, Tirupati, A.P. India
prof.padma@yahoo.com

Abstract: The rapid advancement of information technology and explosive growth of information leading to advance on line health care system. Authentication of personal information is playing significant role in every transaction online system. In this paper, we design an authentication protocols used for authentication e-health and utilization of secure health card in e-health care system.

Keywords: Key generation, ID$_3$, Digital Health Card, Authentication, Image encryption.

I. INTRODUCTION

The health care system which helps various medical transactions. Health problems are unpredictable can strike anywhere and anytime for which timely medical intervention are to be taken care. In which protect data from unauthorized access and mutual authentication needed. To provide security for design and development of protocols to make non-representative that is essential to ensure secure health care system. Patient key generation implementation of protocols to develop used on digital health card to implement transactions. Image encryption has been developed in various areas patients are used to register his personal information and divides into two parts one is for name, address and another is for photo used over digital health card which is portable data storage and provides data communicating it used for secure authentication among patients, doctor and hospital authority. [6]

In this paper, we propose an authenticated algorithm used to design of protocols to develop digital health card to implement medical transactions.

II. RELATED WORK

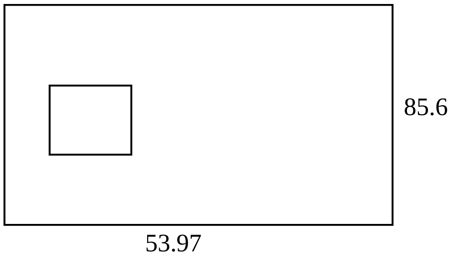
A. Digital Health Card

In terms of physical look and size with one or more semiconductor devices attached to a module embedded in the card. Individual data kept in health card. Health card is portable, secure, low cost, intelligent device, capable of manipulating and storing data. It's intelligence is due to a microprocessor. It has ability to store and secure information and make decisions as required and the card provides particular applications needs. It has read / write capability. Individual access, image and share their health information in a private, secure and confidential environment. The content of the records and rights of access are controlled by the patient. Integrated information such as medical history, results from examining images and documents for which doctor access or authority by the health care team members has to be considered. Patients and clinicians to share decisions – makings and clinical results, reducing barriers and improving continuity of case in treatment.

B. Health Card Architecture

These are of three types

1. A processor to manipulate and interpret data
2. Memory
3. I/O handler



(physical dimensions)

It is usually a 8-bit microcontroller based. Upgraded it to a 16 or 32 bit processor. Memory consist of three types: Rom, RAM, EEPOM. ROM during manufacture. RAM temporary Storage. EEPPOM data segments. The methods of access security can be controlled by very cryptograpy. [8,10]

C. Significance of security in health card

Cryptographic authentication can be supported on health card. If the application presented by the digital land and recorded correctly by the receiver end. It is used to verify the authenticity of the card. Cryptographic algorithm are used to encipher and decipher messages. The kinds of algorithm (1) symmetric (2) secret key for both encryption and decryption (3) asymmetric message is enclosed by public key and decrypted using a private key.

D. Image encryption:

Image encryption process transforms plain – image information into cipher-image for involving the original image with one or more key. Technology that use the same secret key for encryption and decryption under private key techniques asymmetric key technique use two different keys, are public key for encryption and two private keys for decryption. Cryptosystem can be serve all types of attacks they try to violate the system such as, Plain test attack, cipher text attack.

Encryption image:

1. Load the plain image (original image)
2. Calculate the width and height of the input image.
3. Lower horizontal number of blocks = integer (Image – Height/n)
4. Lower vertical number of Blocks = integer (Image = width/n)

No of blocks = horizontal number of blocks x vertical number of blocks [11]

Biometric authentication:

Biometric authentication can be maintained by using finger printing.

E. Decision Tree

ID3 is a decision tree induction algorithm that uses information gaining as the quality function for choosing attributes.

Information gain is defined as the difference of entropy of data set T before and after it is spitted with attributed A. Information Gain (A) = E(T) – E(T/A) If there are categories Ci …..cl. TC is the set of records where class = ci, and (T) is cardinality of the set, then there entropy E(T) is defined as

$$E(T)=\sum_{i=1}^{l}\left(-\frac{|T_{Ci}|}{|T|}.\log\frac{|T_{ci}|}{|T|}\right)$$

To make classification mark the leaf node with the class that has the highest number of instances. This method of inducing decision tree can be easily extended to distributed data mining process. [3,4]

F. Threshold extended ID$_3$ Algorithm

1. Set of objects $O=\{0_1,0_2,0_3..........0_r\}$

2. Generate the attributes respective to the objects $N=\{n_1,n_2.........n_r\}$

3. Generate primes such that

$$n_i = pi_1, pi_2, pi_3..........pi_k, \forall\ i=1,2,3.......r$$

$$say\ i=1\ \ n_1 = p_{11}.p_{12}.p_{13}..........p_{1k}$$

$$n_i = \underset{k=1}{\overset{k}{\pi}}\ pi_k \qquad i=1,2,..........r$$

4. Key generation procedure for individual and multiparty implementation for each object O$_i$ key generation procedure

4(a) Compute E$_i$ and D$_i$

g.c.d of $(E_i, J_2(n_i))=1$

$\rightarrow \mathrm{D_i} = \mathrm{E_i^{-1}}\ (\mathrm{mod\ J_2(n_i)})$

$4(\mathrm{b})\,\mathrm{D_{ik}} = \mathrm{D[mod(p_i^k-1)]},\ \ \mathrm{k}=1,2,\ \ \ \mathrm{i}=1,2.......\mathrm{r}$ 5)

$\rightarrow \mathrm{D_i} = \mathrm{Di_{_1}}, \mathrm{Di_{_2}}$

Public key (k, Ei, ,ni)

5 (a) Private key (k, Di, ni)

5(b) Individual Transactions (E_i, Di_1)

$Di_k = \{Di_1, Di_2\}$

$Di_1 \rightarrow$ refers to secret key for individual transactions

$Di_2 \rightarrow$ refers to polynomial generations for multiparties

6) Select the polynomial of degree k-1 say

$q(x)=a_0x^{k-1}+a_1x^{k-1}+..........a_{k-1}$

7) Choose a set $X=(D_{11},D_{22},.......D_{rr})$ with minimum ‘r’ elements

8) shares computation

Compute $\rightarrow q(Di_k) \qquad\qquad k=1,2,........r$

8(a) Distribution phase
The computed shares distributed to the parties
$(S_1, S_2, ...S_r)$
Classification Phase:

- If all objects in O have the same category O_i then
- Return a left ,node whore category is set of O_i
- End if Data mining the attribute A that best classifies the objects in O and assign it as the test attribute for the current tree node
- Create a new node for every possible value a_i of A and recursively call this method on if with $R^1 = (R - \{A\})\ and\ O^1 = O(ai)$
- Each party among the attribute selected and the attribute value and three parties its local data set accordingly.

G. System Model

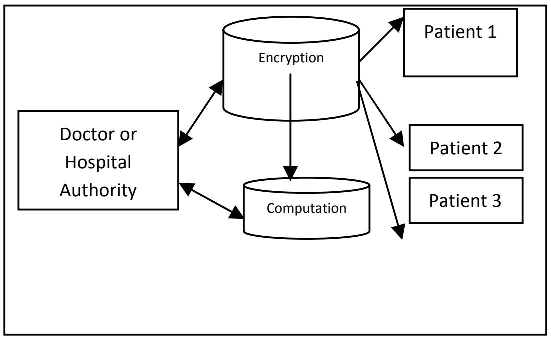


Fig:1 Architecture Design

III. METHODOLOGY

Health card usually microprocessor chip inside patients authenticate themselves to the card. In the microprocessor patient information can be provided in which cryptographic algorithm can be implemented to ensure confidentiality and authentication. An algorithm can be generated MJ$_2$RSA which are used as public key is used for patient utility and private key is used for doctor and hospital authority to provide necessary medical interventions. Required data can be obtained and stored and updated from time to time. Diagnosis and permits a comparison and decision can be made and protection of patient data can only be read when patient and doctor, hospital authority have been authenticated. Healthcare professionals have instantaneously access such information when needed and update the content. Digital health card provides medical records and treatment such as personal information, diagnosis, medical conditions, sensitive private information and family history. By performing cryptographic algorithms on the card itself. It is possible to write confidential information to the card that can never be read outside.

IV. PROPOSED PROTOCAL FOR SECURE GENERATION OF E- HEALTH CARE

Secure Communication protocol between patient and Administrative Authority

Patient	→	Administrative Authority
Request for Secure health card	→	Allows for Health card response
Fills the Health card process	←	
In which open (public)		
Closed data base (Private)	→ ←	Open data base encryption Hash value ni in which patient details Name - n1 Type – n2 Addres – n3…..nr $n = \overset{r}{\underset{i=1}{\pi}} ni$
		Using J$_2$ RSA e_1, d_1, d_2 encryption for Health card using Image encryption of closed details of Photo and details of health eligibilities of treatment

(A)

1. Patient starts the process with administrative authority request for secure health card.
2. Administrative authority (AA) allows for health card response.
3. Patient fills the health card process in which open database (public) and closed data base (private).
4. Administrative authority open database encryption of health value ni (patient details) $n = \overset{r}{\underset{i=1}{\pi}} ni$ (n1, n2 …..nr) encryption e1, d1, d2.

5. AA closed database encryption used for photo and processing details of health eligibilities of treatment for patient.

(B) Service communication protocol between patient and hospital authority.

Patient	→	Hospital Authority
Submission of health card	→	Verification allows for d1 and d2 d1 allows for individual transaction of patient d2 allows for polynomial generation for secret values distribution.
Diagnosis response for hospital authority	→	Allows for response verification
Response for openly hospital	←	Availabilities based on health card
	→ ←	List the doctor details using the extended ID$_3$ algorithm for decision making.
	→	If all objects have the same category Oi then return a left node whose category is set of Oi end if determine the attribute A. that best classifies the object in O accessing the test attribute for the current tree R^{l}=(R-{A}) and O^{l}=O(ai)
Response to the decision	←	
	→	Allows hospital authority
Send for treatment and choosing of doctor list.		

(C)

1. Patient submits of health card to hospital authority
2. Hospital authority allows for d1 and d2. d1 individual transaction, d2 polynomial generation of distribution.
3. HA allows response for verification availabilities based on health card.
4. Patient diagnosis response for hospital authority
5. HA list the doctor details to the patients
6. Patient response for openly hospital
7. HA using ID$_3$ for decision making
8. Patient response the decision sends treatment for selecting doctor to hospital authority.

(D) Secure communication protocols between patient and doctor authority.

Patient	→	Doctor Authority
Request for doctor list	→	
		Response to patient
Request for connection (public key)	← ←	Select the doctor from list
	→ ←	Respond for connection (private key)
Patient sends symptoms and lab test report	→ ←	Determining the doctor for suggesting using decision making algorithm suggesting hospital for treatment based on economic conditions of the patient
Sends response for treatment	→	Closed transaction

(E)

1. Patient start the process with HA requesting the doctor list
2. HA sends the doctor list to patient
3. Patient secrets the doctor from the list
4. Patient request connection with doctor
5. Doctor responds for connection with patient
6. Patient sends symptoms and lab reports to the doctor
7. Doctor analyse the information and make decision
8. Patient sends response for treatment to the doctor authority. Doctor verifies the patients signature by decrypting it with patients public key to obtain a hash value ni and compare it to with the hash value. If the two hash values do not match doctor may respond patient to resend message or terminate the protocol execution.
9. Doctor verifies the patient eligibilities with HA.
10. HA sends the response for doctors.
11. Doctor sends response to the patient.
12. Patients close the transaction session

V. CONCLUSION

This paper describes to consider digital health card and based on authentication as secure and utilization for health care system. These are benefitted to design an authenticated protocols.

VI. REFERENCES

1. Privacy preserving decision tree learning over multiple parties”: F.Emekci, O.D. Sahin, D. Agarwa, A.El Abbadi.

2. New Variant MJ_2 – RSA Crytosystem”: E. Madhusudhan Reddy, B.H. Nagarajasri, A.B. Rajesh Kumar, Prof. M. Padmavathamma.

3. Quinlan, J.R. 1986. Introduction of decision trees. Machine learning, vol.1, 81-106.

4. “General Criteria on Building Decision Trees for Data Classification”: Yo-Ping Haung, Vu Thi Thann Hao

5. Threshold Extended ID3 Algorithm, A.B. Rajesh Kumar, C. Phani Ramesh, E. Madhu Sudhan, Prof. M. Padmavathamma

6. Security Artichtecture for web-basd health insurance systems, Mucahit Mutlugan, Ibrahim Sogukpinar

7. A distributed e-healthcare system based on the service oriented articheture, Firat Kart, Gengxin Miao, L.E. Moser, P.M. Melliar-smith, University of California, Santa Barbara, CA 93106.

8. Security Issues in Smart Card Authentication Scheme, Ravi Singh Pippal, Jaidhar C.D., and Shashikala Tapaswi

9. Design and implementation of a smart card based healthcare information system, Geylani Kardas, E. Turhan Tunali.

10. Smartcard Based Authentication Nalini K. Ratha and Ruud Bolle IBM T.J. Watson research Centre, Yorktown Heights, NY.

11. A novel encryption method for image security: Mohammed Abbas Fadhil A1-Husainy, International Journal of Security and its Applications, Vol. 6 No. 1 January, 2012.

12. Privacy preserving decision tree lerning over multiple parties, F.Emekci.O.D. Sahin,D.Agrawal, A.El Abbadi