IOSR Journal of Computer Engineering (IOSRJCE)
ISSN: 2278-0661, ISBN: 2278-8727 Volume 5, Issue 6 (Sep-Oct. 2012), PP 21-24
www.iosrjournals.org

Secure E- Health Care Model

[1]A.B Rajesh Kumar, [2] Prof. M. Padmavathamma
Department of computer science, S.V. University Tirupati, A.P. India

ABSTRACT: *With the development of information technology, Information is being exchanged several kinds of networks. Internet is playing an increasing important role in all walks of life. With the advent of Internet it has become technically possible to provide patient access through online. Health care is very important aspect in Human life. In this paper, we propose secure E- Health care system, which provides to the registered users to analyze their health position, To find disease details, about their diseases and treatment. Particularly, to take decision about the Hospital where they have to take treatment, from when they have to take treatment and the required treatment to their disease.*

Keywords: *Image encryption, Biometric, Decryption, Patient privacy.*

I. Introduction

Health care services that benefits both patients, Doctors and Hospitals, due to the advances in communication and information technology an increasing number of health services available. The development of computer network and the advances in digital technologies information is being exchanged several kinds of networks images with biometric information transfer on web for easy accessing and sharing and image with text data can be utilized by means of encryption. In recent years image encryption has been developed in several applications. Here, patients are used to register his personal information and divides information into two parts one is for photo with biometric information and another for name, address. Digital Health card is a portable data storage and data processing capabilities, and transfer of health data and provides data communications and it is used for secure and authenticated data communication between patients and web services.[8,6]

In this paper, we propose secure E- Health care system, which provides to the registered users to analyze their health position, to find disease details, about their diseases and treatment particularly to take decision about the Hospital where they have to take treatment, from when they have to take treatment and the required treatment to their disease.

II. Related Work

2.1 Digital Health Card System:

To secure sensitive information electronic implementation of Digital Health Card and security interoperability like cryptography standards besides, to ensure authenticity of health card. Digital Health Card is used to maintain authentication it has data storage and processing capabilities. In a online based health care system individual data is kept in patient health card.[8]

2.2 Decision tree:

ID_3 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 splitted with attribute A.[4I

Information gain (A) = E(T) – E(T/A)

If there are categories C_1_C_l.
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 make the leaf node with the class that has the highest number of instances.

2.3. Confidentiality and Integrity

In a web service communication health care system is prove to unauthorized people. In this case patient, Doctor and Hospital data may be violated.

Cryptosystem:

There are two kinds of cryptosystems symmetric and asymmetric. Symmetric cryptosystem use the some key to encrypt and decrypt a message and asymmetric cryptosystem use and key (public key) to encrypt a message and a differential key (private key) to decrypt it. Asymmetric cryptosystems are also called public key cryptosystems. More efficient and reliable solution is a public key cryptosystem such as RSA which is used in the popular security. Cryptography is practice of hiding information.

- Cryptography is the art of science encompassing the principles and methods of transforming message (plain text) into one that is unintelligible (cipher text) and then retransforming that message back to its original form.
- One of the famous cryptographic schemes in the RSA scheme. The idea of this scheme is the usage of the properties of Euler's totient function ϕ (n). The generalization function of the above function of the above function is the jordan's Totient function $J_2(n)$. We can general the RSA scheme with the help of the properties of $J_2(n)$.[1]

2.4. 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.[7,8]

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

Biometric authentication:

Biometric authentication can be maintained by using finger printing.

III. The Proposed Secure E- Health Care Model

Phase 1: Registration Phase

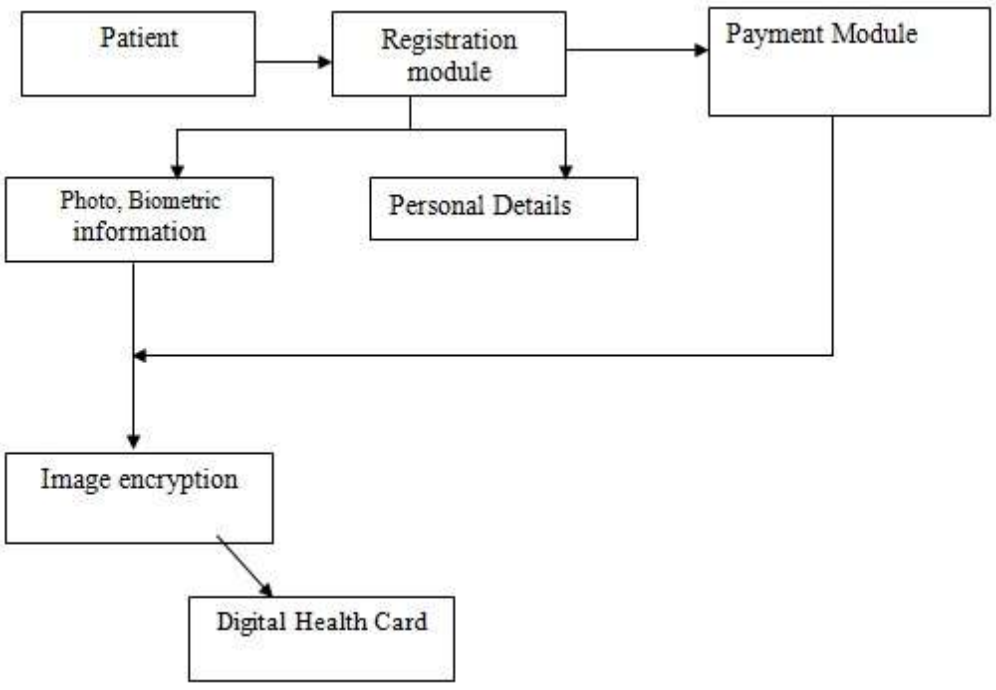

Fig 1: Proposed Secure E- Health care Registration Phase

Phase 2: Decision Making Phase

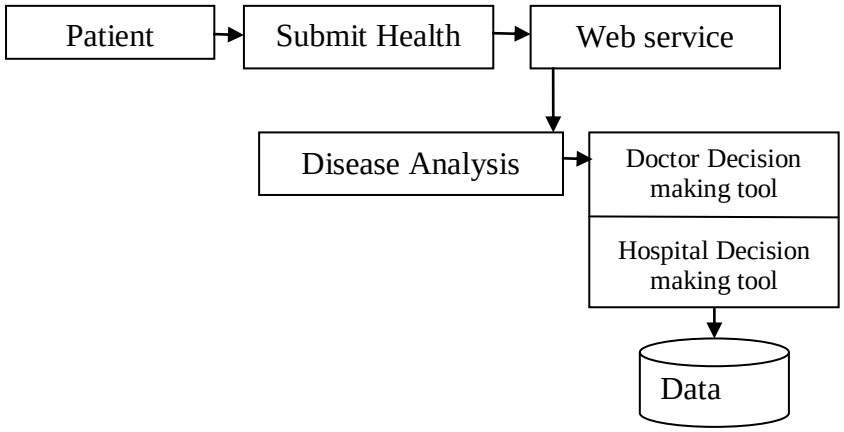

Fig 2: Proposed Secure E- Health care Decision making Phase

3.1 Proposed E-Secure Health care model consists of the following parts and roles:

The process starts with the access to registration phase, patient data consists of with two parts are is used for image with biometric information and the other for name, address, disease, through which encryption can be made in the security module the keys are divided into one for public key with two private keys one private key for patient access control and other private key for Doctor and Hospital control. To generate health card for a patient for allowing a symptoms to make diagnosis with feasible solutions.

By using image encryption process can generate Health card. In this system of Digital card has to be connected to an encryption module at the Doctor's practice where the patients has to enter his perusal information. In the Hospital module decision about doctor given by Hospitals authority because patient needs to get service. Necessary for specialized care for specialized areas in the payment module the process of payment can be made through web service.

3.2. Doctor Decision tree:

Doctor wants to determine where patients in a disease prone or not, the attributes correspond roughly to temperature and stage of a patient by using decision tree

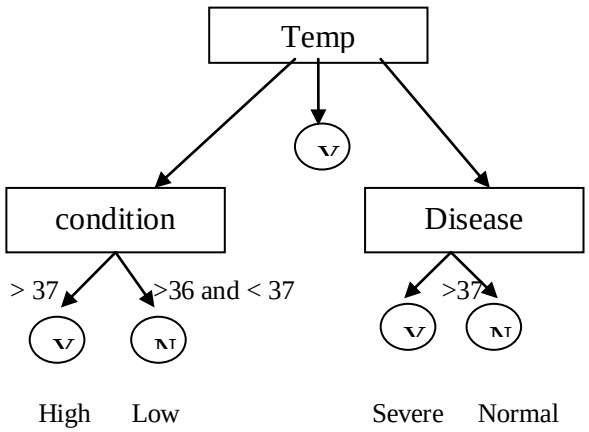

Fig 3: Decision tree

Case	Temp	Condition	Disease	Result
1.	> 37	High	Severe	Yes
2.	>= 36 and <=37	Mild	Moderate	Yes
3.	>=38	High	Severe	Yes
4.	<=37	Low	Normal	No

Fig 4: Decision Table

Patient symptoms a decision tree could be used to determining the patients diagnosis or treatment, forecasting whether patient will affect disease based on data from the repository.

3.3 Hospital Decision Tree:

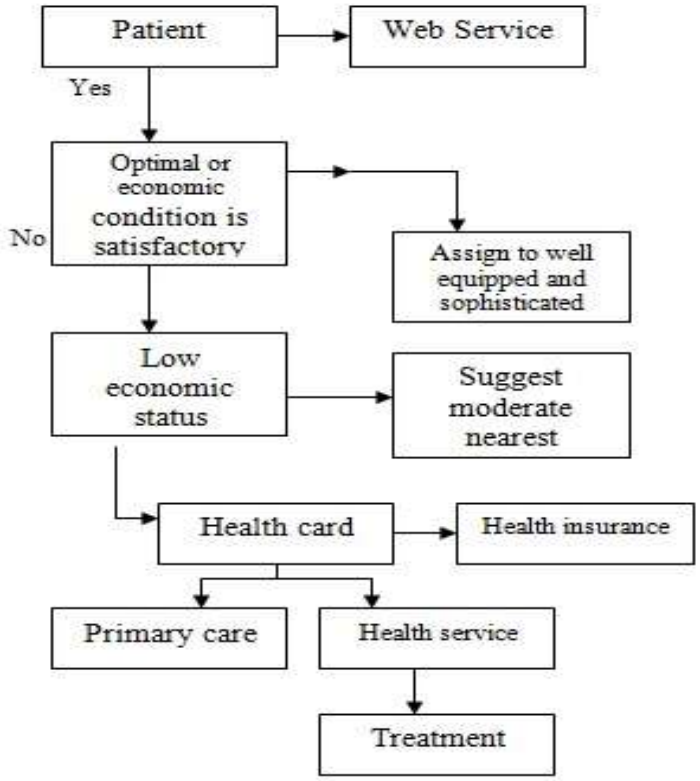

Fig 5: Decision tree Related to Secure E-Health Care

The flow of decision tree is starts from a patient sign in based on health card membership to access into web service. To check his optimum level conditional for choosing better treatment.

IV. Conclusion

In this paper, we have developed a novel approach development of a model architecture for image encryption in securing patient data and serves patient information through web service.

References

[1] "New variant M. J2 – RSA Cryptosystem" : E. Madhusudhan Reddy, B. H. Nagaraiasri, A. B. Rajesh kumar, M. Padmavathamma.
[2] "Threshold Extended ID3 algorithm", A.B. Rajesh Kumar, C. Pani Ramesh, E. Madhusudhan, M. Padmavathamma, ICDIP 2012 International Conference in Malasia.
[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 Hoa
[5] "Privacy preserving decision tree learning over multiple parties ": F. Emekci*. O.D. Sahin , D. Agarwal, A.EI Abbadi.
[6] "A cryptographic key management solution for HIPAA privacy/ security regulations: Wei – Bin Lee, Member, IEEE, and Chien – Ding Lee, IEEE transaction on information technology in biomedicine, vol 12, No.1, January 2008.
[7] Image encryption using block – based transformation algorithm:Mohammad Ali Bani Younes and Aman Jantan IAENG international journal of computer science, 35: 1, IJCS _35_1_03.
[8] Design and implementation of a smart card based healthcare information system: Geylani Karda, E. Turhan Tunali* Computer methods and programs in biomedicine 8I(2006) 66-78.
[9] A novel encryption method for image security: Mohammed Abbas Fadhil A1- Husainy, internation journal of security and its applications Vol. 6 No. 1 January, 2012.