ISSN:1991-8178

Australian Journal of Basic and Applied Sciences

Journal home page: www.ajbasweb.com

An Innovative Approach: A Secured Automated Diagnosis System for Heart Diseases

Dr. Velayutham Ramakrishnan, V. CelinJeeva, Mr E. Siva Ganesh

Department of Computer Science and Engineering, Einstein College of Engineering, Sir C.V. Raman Nagar, Tirunelveli- 627012, Tamil Nadu, India.

ARTICLE INFO

Article history:
Received 20 January 2015
Accepted 02 April 2015
Published 20 May 2015

Keywords:
AES Clinical decision support System Diagnosis system Matchmaking algorithm

ABSTRACT

The diagnosis of heart disease is a significant and complicated process that requires a high level of expertise. Development of computer approaches for the diagnosis of heart disease attracts many researchers. This paper has developed an automated diagnosis system to identify various heart diseases like cardiovascular disease, coronary artery disease, cardiomyopathy, heart attack etc. This diagnosis system is a software program or application that identifies the diseases based on the knowledge available at the system. This system procedure symptom of patients to predict the likelihood of a patient getting a heart disease. This diagnosis system is a third party server that is potentially not fully trusted which raises privacy concerns. The use of encryption algorithm before diagnosing preserves the privacy of the patient data and the decision. The patient data is encrypted by using a cryptographic algorithm. The encrypted data is processed by this system to classify the occurrence of heart diseases by using matchmaking algorithm. Hence, the server involved in the diagnosis process is not able to learn any extra knowledge about the patient data and results.

To Cite This Article: Dr. Velayutham Ramakrishnan, V. CelinJeeva, Mr E. Siva Ganesh., An Innovative Approach: A Secured Automated Diagnosis System for Heart Diseases. ***Aust. J. Basic & Appl. Sci.,*** *9(16): 15-18, 2015*

INTRODUCTION

Now a day's, in this world heart disease is one of the major sources of human death. There are many factors that can increase the risk of getting heart disease. Some of these factors are out of control, but many of them can be avoided by choosing to live a healthy lifestyle. Some of the risk factors for heart disease are age, gender, alcohol consumption, unhealthy diet, and obesity, family history of heart disease, increased blood pressure, and blood sugar. The World Health Organization had report that 12 million deaths occur worldwide, every year due to heart diseases. Heart disease is also known as Cardio Vascular Disease (CVD), encloses a number of conditions that influence the heart (Chitra and Seenivasagam, 2013). Heart diseases include functional problems of a heart such as toxicities in heart muscles like myocarditis (inflammatory heart diseases), heart valve abnormalities or irregular heart rhythms etc these reasons can lead to heart failure (Lin and Chen, 2011). Heart is the most vitalorgan in the human body.

In this fast moving world, people are be unable to remember to take care of themselves. They have Hypertension, Diabetic at very early age and they don't spend time to find rest for themselves and even they don't bother about the quality of food, if they fell in sick they follow their own medication, as a result of all these small negligence it leads to a major threat that is heart disease. Therefore, it is very important for a people to go for heart disease diagnosis. This paper has developed a diagnosis system to identify various heart diseases. The purpose of this diagnosis tool is to help people to know the observation about the likelihood of getting heart disease before consulting with a doctor from their home. This diagnosis system is a computer based system which identifies the disease based on the knowledge available at the system.

1. Existing System:

A Clinical Decision Support System (CDSS) is a computerized medical diagnosis process for enhancing health-related decisions (MinalMoharir, 2012). It is helpful for patient or clinicians to diagnosis the diseases. In existing system, it uses a machine learning tool called SVM, which classifies data based on the training and testing phase (Chitra R and Seenivasagam, 2013), (Mai Shouman *et al.*, 2012) and (Shaikh Abdul Hannan, 2010). Now clinicians, who want to verify whether their patients are affected by that particular disease, could send the patient data to perform diagnosis based on the

Corresponding Author: Dr. R. Velayutham, Department of Computer Science and Engineering, Einstein College of Engineering, Sir C.V. Raman Nagar, Tirunelveli- 627012,TamilNadu, India..
Tel: +917373787114, E-mail: rsvel_kumar@yahoo.co.uk

healthcare knowledge at the server. This Decision Support System (DSS) uses various data mining algorithm such as Support Vector Machine (SVM), Artificial Neural Network (ANN), Naive Bayes algorithm to classify the disease (Mai *et al.*, 2012), (Ratnam *et al.*, 2014), (Samesh *et al.*, 2013), (Sellappan and Rafiah, 2008). However, there is now risk that the third party servers are potentially not trusted servers. Hence, releasing the patient data samples owned by the clinician or revealing the decision to the server lead to less protection of patient data and the result of the diagnosis process.

2. *Proposed System:*

The main aim of the proposed work is to develop privacy preserved automated diagnosis system. The patient can use this system to diagnose the disease. Patient encrypts each element of his / her data using the cryptographic algorithm and sends the encrypted data and the corresponding public key to the server (Ashwini and Akshay, 2014). The private key resides at the patient side; hence, it is not possible for the remote server which participates in this classification operation to decrypt. This system provides privacy to the patient data by encrypting the patient data before diagnosing (Lin and Chen, 2011). The encrypted data is sent to the server for diagnosing.

The server uses the healthcare information from its own repository and classifies the symptoms by using matchmaking algorithm (Ji and Gligor, 2003). The workflow model for the proposed system is given above in Figure 1.

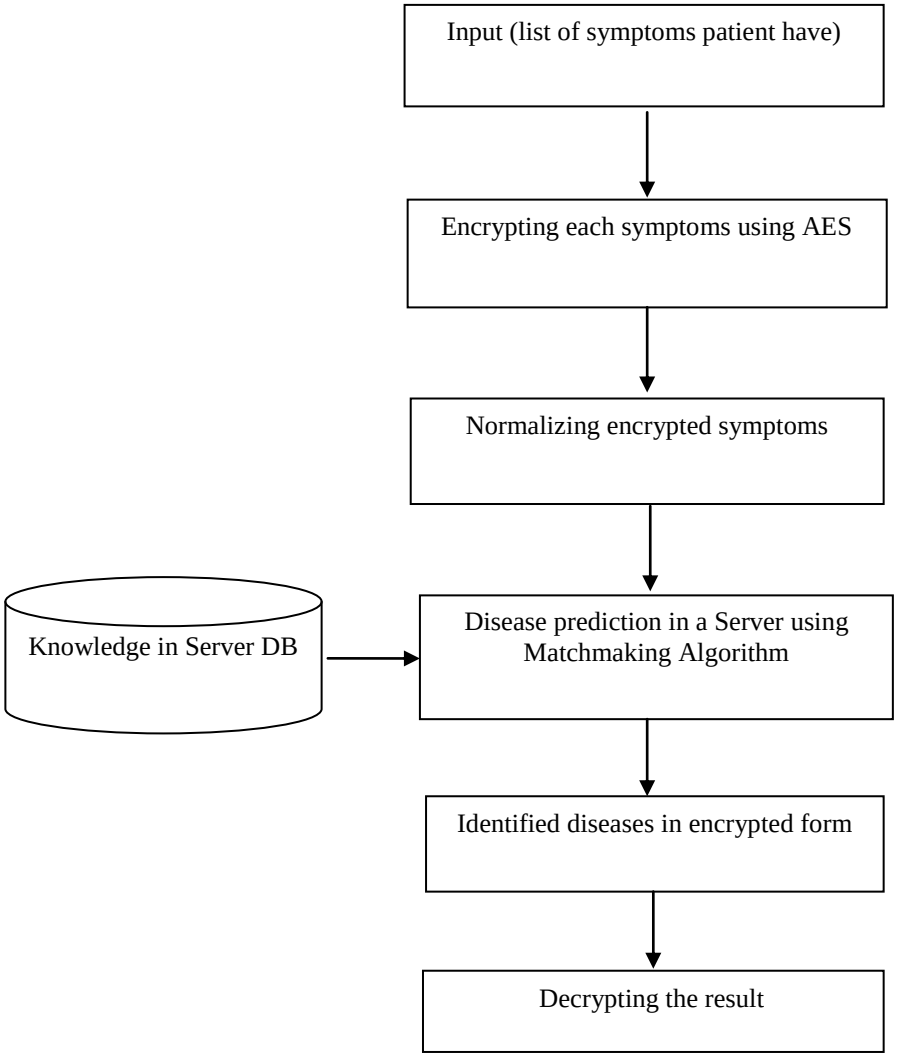

Fig. 1: Workflow diagram of the proposed method.

The step by step process of proposed method is as follows.

1. The list of diseases associated with heart and the related symptoms are collected from the medical resources.

2. The collected symptoms are uploaded into server database through generator tool in an encrypted file format. The purpose of the generator tool is to store the data such as name of the disease and the associated symptoms.

3. The patient sends the list of symptoms that he / she may feel to the server. These data must be encrypted by using the cryptographic algorithm (Ashwini and Akshay, 2014), (Moharir *et al*., 2012). The use of encryption algorithm before diagnosing preserves the privacy of patient data.
4. The encrypted data to be processed by the server is normalized. Normalization splits the encrypted symptoms into each individual symptom. This normalized data is in unreadable form.
5. This diagnosis server process the normalized data to classify the disease based on the knowledge available in its database. The classification of heart disease is done by using matchmaking algorithm (Ji and Gligor, 2003).

3. Methodology:

The proposed work involves four modules: data collection, client-server communication, encryption and decryption and normalization.

3.1 Data Collection:

Data collection is a most important step in any type of diagnosis system. The various diseases related to heart and the associated symptoms are collected from medical resources for better decision-making. All these data must be uploaded into server database through the use of generator tool. The generator tool uploadsthese details in an encrypted file format. This information will be used by the diagnosis system during the diagnosis process. This data will be used for two main purposes: First, the data will be used in extracting useful knowledge and provide scientific decision-making. Second, the data will be used in evaluating the outcomes of the symptoms.

3.2 Client-Server:

This step performs the node creation and communication between the source and destination. The client and server communication is done through sockets. Socket is a software endpoint that establishes the bidirectional communication between the client and the server. In this application, we can create a number of clients that can communicate with the server at the same time. The client is a user of the system i.e. the patient. The patient sends the list of symptoms they may feel to the server via the network. The server processes those symptoms and provides a response to the user.

3.3 Encryption and Decryption:

Use of encryption before diagnosis preserves the privacy of both patient data and the result of the diagnosis process. AES (Advanced Encryption Standard) encryption algorithm is used for encrypting the patient. AES is a symmetric block cipher. This means that it uses the same key for both encryption and decryption. AES algorithm accepts the block size of 128 and may use either 192 or 256 bits key size. In this algorithm, entire data block is processed in parallel during each round using substitutions and permutations. The input is a single 128 bit block for both encryption and decryption and is known as the in matrix. This block is copied into state array which is modified at each stage of the algorithm and then copied to an output matrix (Ashwini and Akshay, 2014), (Moharir, 2012).
The four stages of the AES encryption algorithm are as follows:
1. Substitute bytes
2. Shift rows
3. Mix Columns
4. Add Round Key

3.4 Normalization:

The normalization is done on the encrypted data before diagnosing. Normalization splits the encrypted symptoms into individual symptom. This normalized data is in unreadable form. Hence, the server is not able to learn any information about the patients. In normalization function, it also performs scaling. It is done to avoid the occurrence of errors. The normalized data is processed by the server to classify the patient's symptoms. The server uses matchmaking protocol to classify the patient disease.

3.5 Matchmaking Algorithm:

Matchmaking algorithm is done to find the perfect match for the symptoms to identify the disease (Ji and Gligor, 2003).
1. At first the symptoms entered by the patient is splitted into separate symptoms.
2. Then each symptom is matched with the data in the database one by one.
3. For each symptom, the possible disease and its symptoms are listed.
4. Now the symptoms of each disease are matched with the splitted data one by one.
5. If all the symptoms entered by the patient is matched with the symptoms in the database means then the disease is diagnosed easily.
6. If the group of symptoms produces more than one disease, then the system will display all the relevant disease.

RESULTS AND DISCUSSION

This section explains the results of the proposed diagnosis system. The diagnosis is done by providing various symptoms the patient feel. These symptoms are encrypted to preserve the privacy of the patient data. The diagnosis system processes the symptoms in an encrypted form. The patient data always remain in an encrypted form during the diagnosis process and also the disease identified by the system is in unreadable form this can preserve the privacy of both patient data and the diagnosis result. At last the patient decrypts the result. If the data's provided by the patient is not enough for diagnosing then it will

affect the accuracy and performance of the diagnosis system. While comparing the SVM algorithm with the proposed matchmaking algorithm, the proposed algorithm performs better and reduces the time taken to process the dataset.

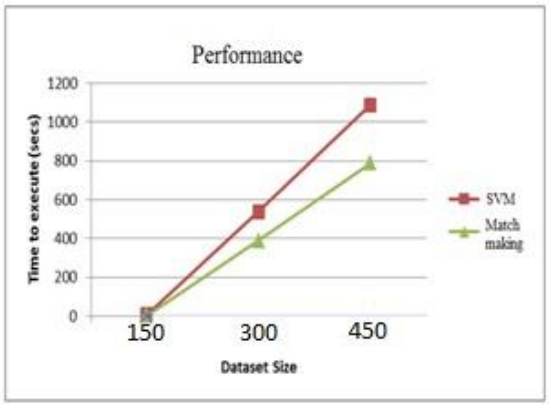

Fig. 2: Performance Analysis.

5. Conclusion and Future Work:

This work has proposed a privacy-preserving diagnosis system for identifying various heart diseases. Since the proposed system is a potential application of emerging outsourcing techniques, rich clinical data sets available in a remote location could be used via the wireless medium without compromising privacy. The proposed system provides privacy to the patient data by using an encryption algorithm. The patient data always remain in an encrypted form during the diagnosis process. Hence, the server is not able to learn any extra knowledge about patient data and results.

In the future, extend the work to include data mining algorithm together with the searching process to provide more efficient and effective diagnosis. Real data from health care organizations are used to improve the decision-making capability of the server. Also, develop the diagnosis system for many diseases and provide solutions to the identified diseases.

REFERENCES

AshwiniR.Tonde, Akshay P Dhande, 2014. 'Review Paper on FPGA based implementation of Advanced Encryption Standard Algorithm', International Journal of Advanced Research in Computer and Communication Engineering, 3(1).

Chitra, R. and V. Seenivasagam, 2013. 'Heart Disease Prediction System Using Supervised Learning Classifier', International Journal of Software Engineering and Soft Computing, 3(1).

Ji Sun Shin, Virgil D. Gligor, 2003. 'A New Privacy Enhanced Matchmaking Protocol', IEICE trans.commun, E96- B, 8: 2049-2059.

Lin, K.P. and M.S. Chen, 2011. 'On the design and analysis of the privacy preserving SVM classifier,' IEEE trans. Knowl. Data Eng.

Mai Shouman, Tim Turner and Rob Stocker, 2012. 'Using Data Mining Techniques in Heart Disease Diagnosis and Treatment', IEEE transaction on Computer Science and Engineering.

Minal Moharir, 2012. 'A Novel Approach Using Advanced Encryption Standard to Implement Hard Disk Security', International Journal of Network Security & Its Applications (IJNSA).

Ratnam, D., P. Hima Bindu, V. Mallik Sai, S.P. Rama Devi and P. Raghavendra Rao, 2014. 'Computer based Clinical Decision Support System for prediction of Heart Diseases using Naïve Bayes Algorithm', International Journal of computer Science and Information Technologies, 5(2): 2384-2388.

Samesh Ghwanmeh, 2013. 'Innovative Artificial Neural Network based decision support system for heart disease diagnosis', Journal of Intelligent Learning Systems and Applications.

Sellappan Palaniappan, Rafiah Awang, 2008. 'Intelligent Heart Disease Prediction System Using Data Mining Techniques', IJCSNS International Journal of Computer Science and Network Security, 8(8).

Shaikh Abdul Hannan, 2010. 'Diagnosis and medical prescription of heart disease using SVM and feed forward Back propagation technique', International Journal on computer Science and Eng.