© 2016 IJSRSET | Volume 2 | Issue 4 | Print ISSN : 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

Patient-Centric and Privacy Preserving Clinical Decision Support System Using Naive Bayesian Classification

Manodnya A. Shitole, Manoj A. Wakchaure

Department of computer Engineering, Amrutvahini College of Engineering,Sangmner, Maharashtra, India

ABSTRACT

In the advanced age in which the healthcare area is exploring widely in that Clinical decision support system, which uses advanced data mining techniques to help clinician make proper decisions, has received considerable attention recently. The advantages of clinical decision support system include not only improving diagnosis accuracy but also reducing diagnosis time. The large data id generated in the healthcare system time by time so every patient is provided their personal information to the doctor for making the decision but because the privacy is the major issue for healthcare system of patient. The requirement is to provide the security to the patient data from unauthorized use the privacy preserving clinical decision support system is given in the system. So in the proposed system the patient security is the main part and in that provided the security to the patient by giving the restriction to the doctor accession. In that we check the authorization of the doctor with the OTP generation because of that the data is preserved. And also the effective Naive Bayesian classification use for the patient easiness for getting the results from the doctor about the disease diagnosis also one prominent part provided in this that patient can upload the document of their so doctor will get help to diagnosis the patient.

Keywords : Privacy Preserving, Patient centric, Cryptography, Homomorphic aggregation scheme etc

I. INTRODUCTION

The Measure of healthcare delivery toward the medical sector and the system can substantial gives the results in terms of health outcome, social provision, cost effective and resource utilization. Across Europe there are they will move to develop the healthcare system to extend the role for the primary care sector and the community in the provision of healthcare. Shared the personal information about healthcare is the major issue in the healthcare system, so for that we have to move forward to make the such system in privacy preserving way which provide the security to the patient data. Resources of the hospital are primarily made which are best suited to the patient but if the data is not secured then it's the very dangerous issue in many of the system so system must be secured. So providing the proper security to the patients data firstly we have to know all the things about the system means role of the system all those involved in healthcare delivery as well as making available the best possible support for clinical decision making. Clinical Decision Support System is a computer aided system which is used to make the decision about any healthcare issue in computerized way, organized healthcare knowledge and patient data to improve health and health care delivery [1].

The current thesis is utilizing the locally available database to prepare the clinical decision support system. As an example if we taken then any particular practitioner system is not having the sufficient amount of the sample disease name ,so in that case making the correct diagnosis with the limited amount of samples is unlikely to be successful. The recent improvement in the remote level outward techniques as like the cloud computing can be expand in the clinical system to gives the accurate and efficient results to the system. So this healthcare system is have to flexible so user can use very easily to it and it is on-demand or pay-per use. Within this context, we can consider the look the system as such that the third party can prepare the clinical system by using the existing system which gives the privacy preserving way to the system for the patient from the third party which is unauthorized , and from this system

the doctor can take the data of server by using internet and send result to the patient by using the internet so it can easy for the patient to get the decision, Hence, in this paper we propose a privacy-preserving clinical decision support system which preserves the privacy of the patient data and the privacy is provided from the doctor side which is the party unknown to the patient firstly.

The reminder of this paper organized as: In section II gives the preliminaries which we needed in the proposed system. In III there is the proposed system and its problem statement. In section IV there is the system model and algorithm needed to it and at second last in section V we are having the experimental results and at the last the conclusion and future scope.

II. METHODS AND MATERIAL

A. Preliminaries

A conventional way to plan a manuscript is to construct an outline. An outline has two interacting purposes. One is to shape the technical information in logical order and other is to help in organizing and thinking about paper. It should be flexible. The main text should be divided into several sections and subsection. There should be continuity in the presentation. The style of sections and subsection are generally given in the guidelines of the journal. If nothing is available, it is preferable to see the previous issue of the journal concerned. The complex mathematical derivation should be placed in the appendix of the paper, which is placed at end of the paper.

A] Privacy Preserving Clinical Decision Support System

The computer world is recently getting the big enhancement in the drug science and the healthcare. The computer use in the healthcare system is the most beneficial side for clinician to make decision in proper and efficient way.Different philosophies are put to use for the enhancement of those frameworks. Any machine program that helps specialists in settling on clinical choice goes under the space of clinical decision support system. Utilizing Artificial Intelligence we can make the frameworks that will have the ability to learn and the formation of new clinical information. These frameworks are presently broadly utilized within healing facilities and clinic. They are turned out to be exceptionally valuable for patient and for medicinal specialists in making decisions. The best available method for gathering the data and to present output data is distinctive in diverse strategies. This issue of securing critical private data of associations/organizations is referred as corporate security.

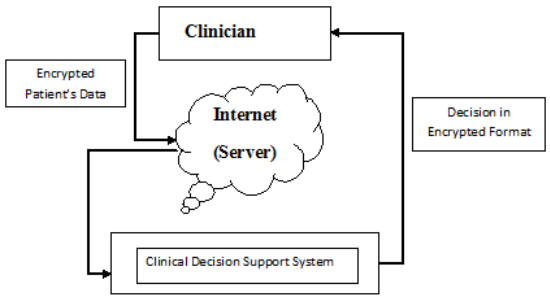


Figure 1. Privacy Preserving Clinical Decision Support System

Protection Preserving Data Mining (PPDM) is a research area concerned with the protection determined by identifiable data when considered for data mining. Hence, PPDM has turned into an increasingly paramount field of research. Various methods and procedures have been produced for protection protecting Preserving privacy is a research zone concerned with the security determined from generally identifiable data at the point when considered. This work focuses the security issue by considering the protection and algorithmic prerequisites at the same time. PPDM is a novel approach research in data mining. Like personal defences, which just considers the agreement of the data, recorded about people, for security purpose it is requires that both the individual things and the examples of the accumulation of information things. History in Clinical Decision Support System Since machine was invented; it has been utilized for aiding medicinal experts. [2]

B] Naive Bayesian Classification

Naive Bays uses the kernel estimator for numeric attributes rather than a normal distribution and utilized Supervised Discretization while converting numeric attributes to normal. With high accuracy in a privacy-preserving way . Our key technical contribution is a privacy-preserving method that allows a data miner to compute frequencies of values or tuples of values in the customers' data, without revealing the privacy-sensitive

part of the data. Bayesian classifiers are statistical classifiers.[3] They can predict class membership probabilities, such as the probability that a given sample belongs to a particular class. Privacy Preserving Patient-Centric Clinical Decision Support System, called PPCD, which based on Naïve Bayesian classification to help doctor to predict disease risks of patients and provide privacy using Paillier encryption techniques It is made to simplify the computation involved and, in this sense, is considered ”naive”. Bayesian classifier is based on Bayes' theorem. Naïve Bayesian classifier is one of the popular machine learning tools, has widely used in health care industry to predict various diseases. It is more appropriate for medical diagnosis in healthcare than complex techniques. PPCD with Naïve Bayesian classifier has offered many advantages and opens a new way to predict patient's diseases. PPCD does not use an advanced encryption method and the Paillier encryption does not achieve multiplication of the plaintext so it uses Secure Multiplication (SM) protocol. Naive Bayesian classifiers assume that the effect of an attribute value on a given class is independent of the values of the other attributes. This assumption is called class conditional independence.[7]

Byes' Theorem

Let X={x1, x2. . .xn} be a sample, whose components represent values made on a set of n attributes. In Bayesian terms, X is considered "evidence". Let H be some hypothesis, such as that the data X belongs to a specific class C. For classification problems, our goal is to determine P(H|X), the probability that the hypothesis H holds given the ”evidence”, (i.e. the observed data sample X).The a posterior probability P(H|X) is based on more information (about the customer) than the a priori probability, P(H), which is independent of X . Similarly, In other words, we are looking for the probability that sample X belongs to class C, given that we know the attribute description of X.P(H|X) is the a posterior probability of H conditioned on X. P (X|H) is the a posterior probability of X conditioned on H. That is, it is the probability that a customer X , is According to Bayes' theorem, the probability that we want to compute P(H|X) can be expressed in terms of probabilities P(H),P(X|H), and P(X) ,The probability of given data is given by the formula,[7]

P(H|X) =P(X|H) P(H) / P(X)

Naive Bayesian Classifier

The naive Bayesian classifier works as follows:

- Let T be a training set of samples, each with their class labels. There are k classes, C1, C2, . . . , Ck . Each sample is represented by an n-dimensional vector,X={x1, x2, . . . ,xn}, depicting n measured values of the n attributes,A1, A2, . . . , An, Respectively.
- Given a sample X, the classifier will predict that X belongs to the class having the highest a posteriori probability, conditioned on X. That is X is predicted to belong to the class C iif and only if P(Ci |X)> P(Cj |X) for 1≤ j≤ m, j Thus we find the class that maximizes P(Ci|X). The class Ci for which P(Ci|X) is maximized is called the maximum posteriori hypothesis. By Bayes' theorem P(Ci|X) -P(X|Ci) P(Ci) / P(X).
- As P(X) is the same for all classes, only P (X |Ci)P(Ci) need be maximized. If the class a priori probabilities, P(Ci), are not known, then it is commonly assumed that the classes are equally likely, that is, P(C1) =P(C2) =. . .=P(Ck), and we would therefore maximize P(X|Ci). Otherwise we maximize P(X|Ci) P(Ci). Note that the class a priori probabilities maybe estimated by P(Ci) = freq(Ci, T)/|T|.
- Given data sets with many attributes, it would be computationally expensive to compute P(X|Ci). In order to reduce computation in evaluating P(X|Ci)P(Ci), the naive assumption of class conditional independence is made. This presumes that the values of the attributes are conditionally independent of one another, given the class label of the sample. Mathematically this means that

$$P(X|Ci) \approx \prod_{Yk=1}^{n} P(xk|Ci).$$

III. RESULTS AND DISCUSSION

A. Problem Definition

The problem is to the determine how to securely store file on server and upload the documents for future use. Also, to develop a new privacy preserving patient centric clinical decision system, which help clinical complementary to diagnose the risk of patients diseases

in a privacy preserving way with finding the top-k diseases names for patients use.

A] Proposed system:

To propose a new privacy-preserving patient-centric clinical decision support system, this helps clinician complementary to diagnose the risk of patients' disease in a privacy-preserving way. In the proposed system the past data are stored in cloud and it can be used for naive Bayesian classifier to compute the disease risk for new coming patients and also patient can retrieve the top-k disease names according to their own preferences without leaking any individual patient medical data. Detailed privacy analysis ensures that patients' information is private and will not be leaked out during the disease diagnosis phase. In addition, performance evaluation via extensive simulations also demonstrates that our system can efficiently calculate patients disease risk with high accuracy in a privacy-preserving way. Our key technical contribution is a privacy-preserving method that allows a data miner to compute frequencies of values or tuples of values in the customers' data, without revealing the privacy-sensitive part of the data.

1) This system will allow patients to upload their case history or reports on common servers from their homes and the doctors will review the reports and suggest treatment accordingly.
2) If the patients are satisfied they can continue with suggested treatment or submit the reports with added comments to other expertise.
3) Finally the suggested medicines will be directly delivered at postal address of the patient.

Algorithm

1) START.
2) Registration of Consumer.
3) Admin Accept Request and Gives the response.
4) Owner login.
5) Owner Allocate Space respective Consumer.
6) File Upload on Server for respective Consumer
7) To create Secrete key as well as master key.
8) Consumer login.
9) File Access or Disease Type search based on Naive Bayes Classifier.
10) Download file=(secrete key, master key)
11) End

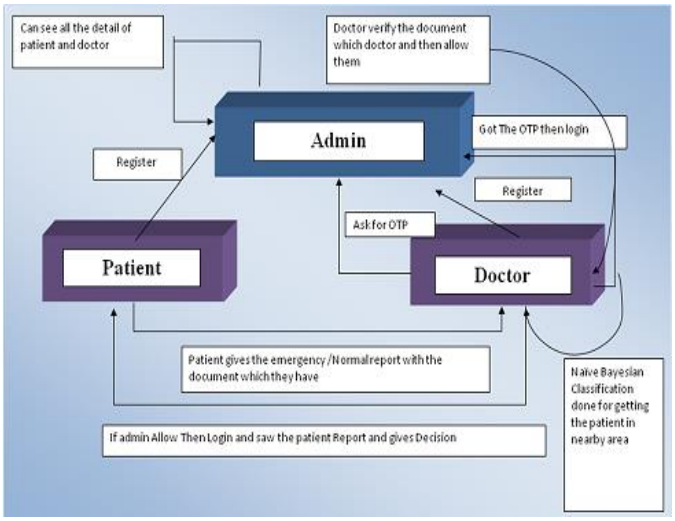
Naive Baye's Classification algorithm used for doctor to got the nearby patient:

1) First f classes select as follows,
2) F (z) =fc1,c2,c3....c ng
3) Take sample
4) X (Z) =fX1, X2....., X ng.....n -input sample
5) A (Z) =fA1, A2, A3...., Ang.....n value attribute
6) The classifier needs to predict X belongs to the class with the highest a posteriori probability, i.e., X is predicted to lie in the class Ci if and only if there exists i, such that gives in Eq.3:
7) Apply Baye's theorem as in Eq. 4
8) To check neural category in the P(X)
9) Sample value as P (C1—X), P(C2—X),P(C3—X).....P(Cn—X)calculated by Eq.5
10) Divide neural word from one site and non-neural word from one site.
11) Result

B. System Model

The design and implementation of an architecture based on the combination of ontology, rules, web services, and the autonomic computing paradigm to manage data in home-based telemonitoring scenarios for the personal use.

1) Today every patient needs to be physically present in front of the doctor for OPD and considering the rate of growth of the population, it won't be possible for doctors to look after all patients.
2) Working people face issues of time for appointment mean there presence at the time when doctors present over there.
3) But we can provide solutions by giving working people facility of home surveillance.
4) Common patients cannot afford fees of highly qualified and renowned doctors. So suggestion will be given by the system to the patient.



The Primitive of frequency mining is simple, but is very useful in data mining applications. Correspondingly, our privacy-preserving frequency mining solution is also quite simple, but is potentially useful whenever Server's Computation Time for a Single Frequency Calculation Privacy is a top concern. In this section, To demonstrate the power of our primitive by showing privacy preserving naive Bayes classifier computation in the fully distributed setting (which can be thought of a horizontally partitioned database in which *each* record is held by a different party).

The below Pie-chart shows,

1) Execute-query on doctor panel one time then, more patient available in emergency panel as compared to Normal panel Using naive classification.
2) In This Doctor got the many no of patient as comparison to the existing and the naïve Bayesian classification is provided at emergency report zone.
3) So as per the classification in proposed system the naïve bayes classification is better than existing system.

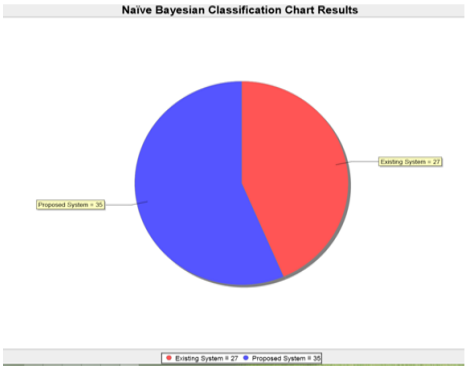


Figure 2. Result Chart of Proposed System

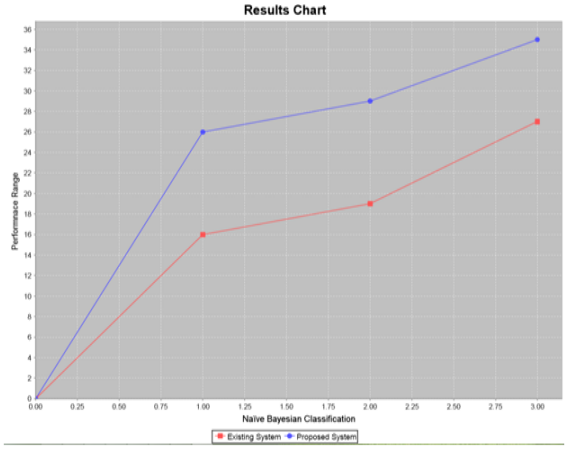


Figure 3. Comparision Of Existing And Proposed System Result

C. Comparison between Existing System and Proposed System

Table 1. Comparison between Existing System and Proposed System

Sr.No.	Parameters	Existing System	Proposed System
1	Privacy Provision	Provide The Security At Service Provider Side(Doctor)	Provide The Security At Service Receiver Side(Patient)
2	Naïve Bayesian Classification	Naïve Bayesian Classification Is Provided At Patient Side For The Quick Decision About Doctor.	Naïve Bayesian Provided At Doctor Side Means The Patient Got To The Doctor And It Gives Fast Reply To The Nearby Patient.
3	Security Scheme	Pailier Homorphic Encryption Is Used For The Security Purpose Which Generates The Private Key.	Here With Pailier Homorphic Encryption Uses The One Time Password Generation Facility For Security Of Patient
4	Access Of Information	Here When Got The Private Key The Doctor Can Access The Patient.	Here We Provided The Security To The Patient Such That Admin Can Allow The Doctor After That The Doctor Can Access The Patient Information Also For More Encryption The OTP Generation Is Used.
5	Categorization Of Report	There Is No Any Categorization At Patient Side For The Report.	In The Proposed System The Patient Can Gives Its Normal Report And Emergency Report Also So Got Reply From Doctor As Per The Report Category.
6	Security Level	This System Is Providing The Good Security To The Patient Personal Information.	Proposed System Provided The Better Security To The Patients Personal Information
7	Specialty Addition	In This System Doctor Cannot Add Their Specialty.	In This System Doctor Can Able To Add The Specialist.
8	Result Analysis	In This System The Patient Got The Good Results About His/hers Diseases.	In This System Patient Got The Better Results About His/hers Disease.

IV. CONCLUSION

From the proposed system finally I conclude that the file can store or upload securely on server and access securely from the server. Also, classification of medical data through naive Bayesian classifier for efficient use of doctor in term of patient.

The Future Enhancement that a cryptographic approach that is efficient even in amany-customer setting, provides strong privacy for each customer, and does not lose anyaccuracy as the cost of privacy. Unlike general-purpose cryptographic protocols, this methodrequires no interaction between customers, andeach customer only needs to send a single flowof communication to the data miner. However,we are still able to ensure that nothing aboutthe sensitive data beyond the desired frequencies is revealed to the data miner.

V. REFERENCES

[1] Ximeng Liu,Rongxing Lu,Jianfeng ,Le Chen, and Baodong Qin"," Privacy-Preserving Patient-Centric Clinical Decision Support System on Näıve Bayesian Classification", "IEEE journal of biomedical and health informatics, vol. xx, no. xx, December 2014"

[2] Jussi Mattila Juha Koikkalainen, Arho Virkki, Mark van Gilsand Jyrki Lotjonen";"Design and Application of a Generic Clinical Decision Support System for Multiscale Data" "IEEE transactions on biomedical engineering, vol. 59, no. 1, January 2012"

[3] Yogachandran Rahulamathavan Suresh Veluru, Raphael C.-W. Phan, Jonathon A. Chambers and Muttukrishnan Rajarajan" ,"Privacy-Preserving Clinical Decision Support System Using Gaussian Kernel-Based Classification"," "IEEE journal of biomedical and health informatics, vol. 18, no. 1, January 2014"

[4] Ewart R. Carson, Derek G. Cramp, Alastair Morgan, and Abdul V. Roudsari"," Clinical Decision Support, Systems Methodology, and Telemedicine: Their Role in the Management of Chronic Disease", "IEEE transactions on information technology in biomedicine, vol. 2, no. 2, June 1998

[5] M. A. Musen, B. Middleton, and R. A. Greenes", "Clinical decision-support systems" , "in Biomedical informatics. Springer, 2014, pp. 643–674".

[6] H. Monkaresi, R. A. Calvo, and H. Yan", "A machine learning approach to improve contactless heart rate monitoring using a webcam","IEEE J. Biomedical and Health Informatics ,vol.18,no.4,pp.1153–1160, 2014

[7] K. M. Leung, "Naive bayesian classifier","Polytechnic University Department Of Computer Science , "Finance and Risk Engineering, Copyright c,mleung@ poly. edu, 2007".

[8] D. Boneh, E.-J. Goh, and K. Nissim, "Evaluating 2-dnf formulas on ciphertexts," in Theory of cryptography". "Springer, 2005, pp. 325–341".

[9] C. Schurink, P. Lucas, I. Hoepelman, and M. Bonten", "Computer- assisted decision support for the diagnosis and treatment of infectious diseases in intensive care units," "The Lancet infectious diseases , vol. 5, no. 5, pp. 305–312, 2005."

[10] J. Vaidya, M. Kantarcioglu, and C. Clifton," "Privacy-preserving naïve bayes classification," VLDB J, vol. 17, no. 4, pp. 879–898, 2008.

[11] K. Lin and M. Chen, "On the design and analysis of the privacy-preserving SVM classifier", "IEEE Trans. Knowl. Data Eng., vol. 23,no. 11, pp. 1704–1717, 2011

[12] H. Li, L. Xiong, L. Ohno-Machado, and X. Jiang, "Privacy preserving rbf kernel support vector machine," Bio-Med research international , vol. 2014, 2014