International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2015): 6.391

Clinical Decision Support System Using SVM with the Preservation of Privacy

S. S. Bhide[1], S. M. Sangve[2]

[1] S.S.Bhide Computer Engineering Department, Zeal College of Engineering and Research Savitribai Phule Pune University Pune,India

[2]Prof.S.M.Sangve Computer Engineering Department, Zeal College of Engineering and Research, Savitribai Phule Pune University Pune, India

Abstract: ***a clinical decision support system helps clinicians to diagnose various diseases, to check various possibilities regarding diseases and to make correct diagnosis. Late patterns toward remote outsourcing can be misused to give proficient and precise clinical choice backing in medicinal services. In this situation, clinicians can utilize the fitness data located in far flung servers via the net to analyze their sufferers. Then again, the way that these servers are outsider and in this manner conceivably no longer completely trusted increases conceivable protection issues. In this paper, a singular privacy safeguarding system for a clinical choice backing framework is proposed where the patient's data dependably stay in a scrambled shape amid the decision making system. In this it additionally preserves privacy of patient data from clinician and preserve privacy of patient at server side but clinician is also not trusted person so the privacy of the patient data is needed to be preserved. Henceforth, the server included within the conclusion procedure isn't able to recognize any information about the patient data. The exploratory outcomes on mainstream healing datasets from UCI-database display that the exactness of the decision support system remains constant along with the privacy of affected person records.***

Keywords: Classification, clinical decision support system, encryption, privacy, support vector machine (SVM)

1. Introduction

A decision support system frames a fundamental capacity to associate wellbeing diagnosis with wellbeing data for improved social protection [1][2]. Late examples toward remote outsourcing can give capable and exact decision backing in therapeutic administrations [3][4][5][6]. In this circumstance, owner can use the wellbeing data arranged at remote servers to build a decision making system and also patient data can be stored at these remote servers to solve the data storage issue. But on the other hand, these servers are third party and hence possibly not totally trusted raises possible security concerns. In this paper, a novel protection safeguarding convention for a clinical choice backing framework is proposed where the patient's information dependably stay in a scrambled structure during the conclusion process. Henceforth, the server included in the conclusion procedure is not ready to realize any additional information about the patient information and results. The exploratory results on mainstream therapeutic datasets from UCI-database show that the exactness of the proposed convention is up to 97.21% and the privacy of user data is not compromised.

The recent advances in far flung outsourcing techniques (i.e. cloud computing) may be exploited in healthcare to provide efficient and accurate decision assistance as a provider. This carrier will be utilized by any proprietor in a flexible way such that pay-in step with use [7].Inside this context, let us take into account the following state of affairs: a third party server builds a diagnosis support system using the existing dataset. Now proprietor, who want to verify whether their consumers are affected by that precise ailment, could send the person records to the server through the internet to carry out prognosis based totally on the healthcare expertise on the server. This new notion overcomes the problems that might be faced by the owner, inclusive of having to gather a massive variety of samples and requiring high computational and storage assets to build their own decision guide machine. Also user data storage facility is also provided by these third party servers to the proprietor.

In any case, there may be presently a hazard that the outsider servers are likely untrusted servers. For this reason, uncovering the user information possessed by the owner to these servers increases protection worries. This disadvantage can affect the appropriation of outsourcing strategies in social systems [8] [9]. Moreover, the server might not desire to show the components of the selection no matter the reality that it offers the functionality to the proprietor. Hence, in this paper a privacy retaining decision making system is proposed which protects the security of the consumer data, the calculation of decision function value and the server side decision making system parameters , so that the blessings of the growing outsourcing innovation can likewise be overjoyed within the medicinal division.

2. Related Work

2.1 Data Classification

A frequently used revelation protection method was data perturbation. When used for data mining, it was desirable that perturbation preserves statistical relationships between attributes, while given that sufficient protection for individual confidential data. To achieve this goal, a kd-tree based perturbation method is proposed, which recursively partitions a data set into smaller subsets such that data records within each subset are more homogeneous after each partition. The private data in each final subset are then perturbed using the subset average. The proposed method show the effectiveness of experimental study was conducted [10]. In this paper,

define a k-degree-l-diversity anonymity model that considers the security of structural information as well as sensitive labels of individuals. System had seen a novel anonymization methodology based on adding noise nodes. System implemented that algorithm by adding noise nodes into the original graph with the consideration of introducing the least distortion to graph properties. The proposed novel approach is to reduce number of noise nodes to decrease the complexity within networks. System implement this protection model in a distributed environment, where different publishers publish their data independently Most importantly, system present a rigorous analysis of the theoretical bounds on the number of noise nodes added and their impacts on an important graph property. Proposed system conducts extensive experiments to calculate the effectiveness of the proposed technique [11].

2.2 SVM Support Vector Machine

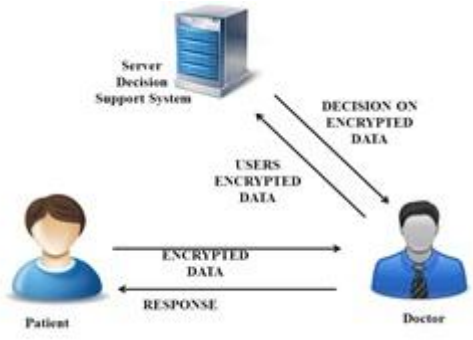
The paper proposes utilizing support vector machines (SVMs) for the diagnosis of diabetes. In particular, paper uses an additional explanation module, which turns the "black box" model of an SVM into an intelligible representation of the SVM's analytic decision. Results on a real-life diabetes dataset show that intelligible SVMs provide a promising tool for the prediction of diabetes [12]. The system proposes private protocols implementing the support vector machine learning algorithms, gives private classification protocols [13]. The classifier or the classifications in encrypted form is that they can be decrypted only by a common agreement by the protocol participants and gives new protocols that return their outputs as the decision value. The system also shows how to use the encrypted classifications to privately estimate many properties of the data and the classifier. The standard cryptographic definitions with SVM classifiers are used [14].

3. Proposed System

3.1 Description

In this situation, Owner can exploit the wellbeing learning situated in remote servers through the Internet to analyze their users. In any case, the way that these servers are outsider and accordingly possibly not completely trusted raises likely protection worries. In this paper, proposed a novel security preserving system for a decision support system where the user's information dependably stays in an encoded structure during the finding method. Hence, the server included in the conclusion procedure is not able to realize any additional learning about the patient information and results. In this it additionally preserves privacy of patient data from clinician side along with preservation of privacy of patient at server side as clinician is also not trusted person so patient data privacy is needed to be preserved .

3.2 System Architecture



In this architecture, the data is sent to the server in encrypted form, the result is calculated on the basis of this data that has been sent to the server and the response is returned to the client . So data remains at server side in an encrypted format in a secure manner during the diagnosis and decision which has been calculated on this encrypted data is sent to the client.[1]

3.3 Mathematical Model

Let S is the Whole System Consists:

S = { PD , S , R }.

1. PD is a set of patient data.
   PD= {PD1 , PD2….PDn}.
2. S .is set of separated data.
   S= {S1 , S2….Sn}.
3. R is set of result given by third party.
   R={R1,R2…..Rn}.

Step 1: clinician send the patient data to diagnoses to third party in encrypted form.

PD= {PD1,PD2….PDn}.

Step 2: At server side data is separated as per requirement .

S= {S1,S2….Sn}.

Step 3:After separating data is diagnosis and result is given in encrypted form.

R= {R1,R2…..Rn}.

Output: Secure patient data.

3.4 Used Algorithm

3.4.1 Support Vector Machine

Machine learning for data classification generally utilizes SVM. For example, image processing, computer vision, text mining, natural language processing, biomedical engineering, and many more have a high assumption capacity which gives high reliability in true applications. Preparing with the data samples the objective of a SVM is to isolate classes by a classification function.[12][13]

Algorithm:

1. Finding the Closest Pair of Points
2. Adding a Point to the Support Vector Set
3. Pruning
4. Scaling

3.4.2 Advanced Encryption Standard

The encryption procedure uses a set of especially derived keys known as round keys. Those are implemented, at the side of other operations, on an array of statistics that holds exactly one block of information be encrypted.

The following AES steps of encryption for a 128-bit block are given below:

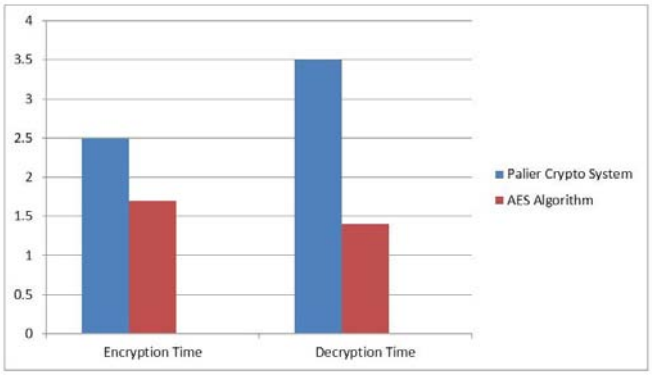
1) Derive the set of round keys from the cipher key.
2) Initialize the state array with the block data (plaintext).
3) Add the initial round key to the starting state array.
4) Perform nine rounds of state manipulation.
5) Perform the tenth and final round of state manipulation.
6) Copy the final state array out as the encrypted data (ciphertext).

3.5 Result Analysis

Table 1: Comparative Analysis Of Security Algorithms

Performance Measure	Paillier Crypto System	AES Algorithm
Encryption Time	2.5 sec	1.7 sec
Decryption Time	3.5 sec	1.4 sec

For File size = 196 kb



4. Conclusion

In this paper, a security protecting decision support system using SVM is studied. Since the proposed computation is a potential usage of rising outsourcing frameworks, rich datasets open in far off areas will be used for building decision making system which is more accurate because of the availability of large training dataset for the SVM classifier and is used by any user by using this system over the internet without fearing about privacy of the personal information. The proposed system uses Advanced Encryption Standard algorithm for data encryption and decryption which is a symmetric key algorithm and is highly secure. Advanced Encryption Standard algorithm is secure from various cryptanalytical arracks so it improves security of the system. Also Advanced Encryption Standard algorithm has faster processing speed for encryption and decryption and hence it increases the performance of the system. Critically ,the gain of our scrambled location method is that now consumer records do not require to be uncovered to the remote server as they are able to stay in encoded structure at all times, during the conclusion procedure.

5. Acknowledgement

It gives me a great pleasure and immense satisfaction to present this special topic on Clinical Decision Support System Using SVM With The Preservation Of Privacy. The success of this topic has throughout depended upon an exact blend of hard work and unending co-operation and guidance, extended to me.

References

[1] Yogachandran Rahulamathavan, Suresh Veluru, Raphael C.-W. Phan, Jonathon A. chambers, Muttukrishnan Rajarajan , " Privacy-Preserving Clinical Decision Support System Using Guassian Kernel-Based Classification ", IEEE Journal Of Biomed and Health informatics, vol. 18 , no.1 ,pp.56, Jan 2014.

[2] A. X. Garg, N. J. Adhikari, H. McDonald, M. P. Rosas-Arellano,P. J. Devereaux, J. Beyene, J. Sam, and R. B. Haynes, "Effects of computerized clinical decision support systems on practitioner performance and patient outcomes: A systematic review," *J. Amer. Med. Assoc.*, vol. 293,no. 10, pp. 1223–1238, 2005.

[3] E. R. Carson, D. G. Cramp, A. Morgan, and A. V. Roudsari, "Clinical decision support, systems methodology, and telemedicine: Their role in the management of chronic disease," *IEEE Trans. Inf. Technol. Biomed.*,vol. 2, no. 2, pp. 80–88, Jun. 1998.

[4] P. J. Lisboa and A. F. G. Taktak, "The use of artificial neural networks indecision support in cancer: A systematic review," *Neural Netw.*, vol. 19,pp. 408–415, 2006.

[5] V. Baskaran, A. Guergachi, R. K. Bali, and R. N. G. Naguib, "Predicting breast screening attendance using machine learning techniques," *IEEETrans. Inf. Technol. Biomed.*, vol. 15, no. 2, pp. 251–259, Mar. 2011

[6] H. Shin and M. K. Markey, "A machine learning perspective on the development of clinical decision support systems utilizing mass spectra of blood samples," *J. Biomed. Informat.*, vol. 39, no. 2, pp. 227–248, 2006.

[7] S. Sundareswaran, A. C. Squicciarini, and D. Lin, "Ensuring distributed accountability for data sharing in the cloud," *IEEE Trans. Dependable Secure Comput.*, vol. 9, no. 4, pp. 555–567, Jul./Aug. 2012.

[8] S. Pearson and A. Charles worth, "Accountability as a way forward for privacy protection in the cloud," in *Proc. 1st Int. Conf. Cloud Comput.*, Beijing, China, 2009, pp. 131–144.

[9] S. Pearson, Y. Shen, and M. Mowbray, "A privacy manager for cloud computing," in *Proc. Int. Conf. Cloud Computer.*, Beijing, China, 2009,pp. 90–106.

[10] X.-B. Li and S. Sarkar, "A tree-based data perturbation approach for privacy-preserving data mining," *IEEE Trans. Knowl. Data Eng.*, vol. 18, no. 9, pp. 1278–1283, Sep. 2006.

[11] M. Yuan, L. Chen, P. S. Yu, and T. Yu, "Protecting sensitive labels in social network data anonymization," *IEEE Trans. Knowl. Data Eng.*, vol. 25, no. 3, pp. 633–647, Mar. 2013.

[12] N. Barakat, A. P. Bradley, and M. N. H. Barakat, "Intelligible support vector machines for diagnosis of diabetes mellitus," *IEEE Trans. Inf. Technol. Biomed.*, vol. 14, no. 4, pp. 1114–1120, Jul. 2010.
[13] I. Guler and E. D. Ubeyli, "Multiclass support vector machines for EEGsignals classification," *IEEE Trans. Inf. Technol. Biomed.*, vol. 11, no. 2, pp. 117–126, Mar. 2007.
[14] H. Lipmaa, S. Laur, and T. Mielikainen, "Cryptographically private support vector machines," in *Proc. 12th ACM SIGKDD Int. Conf. Knowl. Discov. Data Mining*. Philadelphia, PA, USA, Aug. 2006, pp. 618–624.

Author Profile

Shruti S. Bhide, Pursuing M.E. in Department of computer engineering at Zeal Education Society's Zeal College of Engineering & Research Savitribai Phule Pune University , Pune , India.

Prof. S. M. Sangve , Department of computer engineering at Zeal Education Society's Zeal College of Engineering & Research Savitribai Phule Pune University , Pune , India.