INTERNATIONAL JOURNAL FOR TRENDS IN ENGINEERING & TECHNOLOGY
VOLUME 4 ISSUE 1 – APRIL 2015 - ISSN: 2349 - 9303

A Secure Decision Making Process in Health Care System Using Naive Bayes Classifier

K.M.Ruba Malini[1]
[1]K.L.N.College of Engineering,
Computer Science and Engineering,
rubamalini.me@gmail.com

R.Lakshmi[2]
[2]K.L.N.College of Engineering,
Computer Science and Engineering,
RLAKSH_GOPI@yahoo.com

Abstract— A Secure decision support estimation in health care system preserves the seclusion of the patient data, the decision estimation and the server side clinical support system. In order to preserve privacy paillier homomorphic encryption technique is used with naive bayes classification method. Hence the server involved in the diagnosis process is not able to know the diagnosis results of the patients because the patient's data always continue to exist in an encrypted form even during the recognition process in health care system. To validate the performance, evaluate the method of classification using naive bayes classifier on medical datasets and the accuracy of the results is much better. Secure decision support estimation is a computerized medical diagnosis process for enhancing the health related decisions to improve patient's health and also provide the more accurate decision in the diagnosis process.

Index Terms— Classification, Clinical decision support, Data mining, Encryption, Naive Bayes classifier, Privacy.

1 INTRODUCTION

The recent advances in remote outsourcing techniques (i.e., cloud computing) can be exploited in healthcare to provide efficient and accurate decision support as a service. This service could be utilized by any clinician in a flexible manner such as on-demand or pay-per use [2]. Within this context, let us consider the following scenario: a third party server builds a clinical decision support system using the existing clinical dataset (i.e., assume that the server has a rich clinical dataset for a particular disease).

Now clinicians, who want to verify whether their patients are affected by that particular disease, could send the patient data to the server via the Internet to perform diagnosis based on the healthcare knowledge at the server. This new notion overcomes the difficulties that would be faced by the clinicians, such as having to collect a large number of samples (i.e., a rich clinical dataset), and requiring high computational and storage resources to build their own decision support system. However, there is now a risk that the third party servers are potentially untrusted servers. Hence, releasing the patient data samples owned by the clinician or revealing the decision to the untrusted server raises privacy concerns [3]. Furthermore, the server may not wish to disclose the features of the clinical decision support system even if it offers the service to the clinicians.

- *K.M.Ruba Malini is currently pursuing masters degree in computer science and engineering in K.L.N.college of engineering, India, PH-9884132518. E-mail: rubamalini.me@gmail.com*
- *R.Laxmi is currently working as associate professor in computer science and engineering in K.L.N.college of engineering, India, PH-9843045725 E-mail: RLAKSH_GOPI@yahoo.com*

In order to preserve privacy, we redesign this using the Paillier homomorphic encryption technique as one of its building blocks [4].Since the Paillier encryption supports only integers and the system variables are continuous and the Gaussian kernel involves exponentiation of negative values, crucially we develop a novel technique to scale the variables, which overcomes these barriers without deteriorating the privacy and performance.

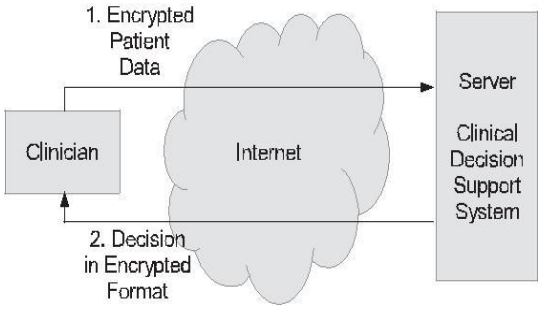

Fig.1.Overview of a privacy-preserving clinical decision support system.

2 NAIVE BAYES CLASSIFIER

Naive Bayes have been widely used in machine learning for data classification [1]. They have a high generalization ability which provides high reliability in real-world applications such as image processing, computer vision, text mining, natural language processing, biomedical engineering, and many more [1]. The goal of Naive Bayes is to separate classes by a classification function, which is obtained by training with the data samples. We describe the classification function of an in the following section.
Depending on the precise nature of the the extent to which something is likely to happen using the naive bayes classifiers can be trained very efficiently in a supervised learning setting. In most appliances naive Bayes models uses the method of

maximum likelihood; simply work with the naive Bayes model without believing in Bayesian probability or using any Bayesian methods.

2.1 **In-Plain Domain**

We start with a training set of samples $\tilde{\mathbf{x}}i \in \mathrm{RN}$, $i = 1, \ldots, N$.... Depending on the separability of the training data, this problem is further divided into either a linear classification problem or a nonlinear classification problem.

1) ***Linear Classification Problem****:* The goal of linear classification is to obtain two parallel hyperplanes. $\mathbf{w}\_\mathbf{x} + b = -1$ and $\mathbf{w}\_\mathbf{x} + b = +1$, where $\mathbf{w}$ and b are classification parameters obtained during the training process. Both hyperplanes separate the training data of the two classes such that the distance between those hyperplanes is maximized.After the training stage we can classify an unlabeled test sample, $\tilde{\mathbf{t}} \in \mathrm{RN}$.

2) ***Nonlinear Classification Problem****:* In the previous section, we discussed the classification problem where the training data samples were linearly separable. However, it has been proven in the literature that a similar approach can be used for a nonlinear classification problem using kernel methods [1]. Hence, the nonlinear classification algorithm is formally similar to the linear classification algorithms except that the dot product between the data samples is replaced by various nonlinear kernel functions. These kernel functions transform the nonlinear classification problem into a linear classification problem by mapping data samples into a higher dimensional feature space.

3 A SECURE DECISION SUPPORT SYSTEM

In this section, we develop an algorithm which utilizes the healthcare knowledge available in the remote location via the Internet while preserving privacy. Hence, we consider a client–server scenario where the remote server uses (6) as a decision making tool. Clinician sends the patient data **t** over the Internet and obtains support from the server to make a decision however the clinician is reluctant to reveal the patient data or the decision to the server due to privacy concerns. At the same time the server desires not to leak any parameter values of the classification function as this would be a breach of privacy of the training clinical data samples which relate to other patients.

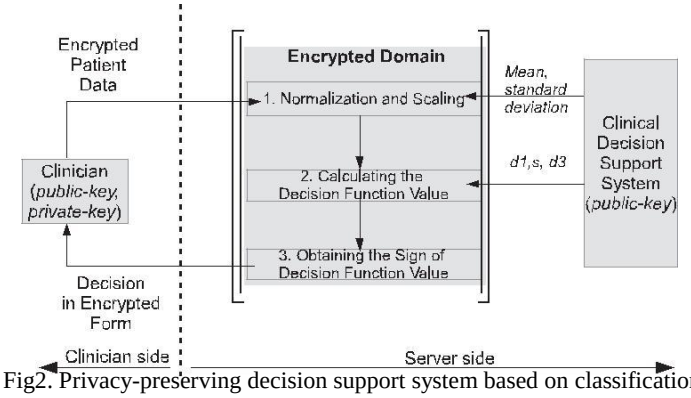

Fig2. Privacy-preserving decision support system based on classification

3.1 **Homomorphic Encryption**

One of the building blocks of our technique is homomorphic encryption. For concreteness and without loss of generality, our descriptions are based on the Paillier cryptosystem [4] although any other homomorphic encryption schemes could be used. The Paillier cryptosystem is an additively homomorphic public-key encryption technique is provable semantic security is based on the decisional composite residuosity problem.

3.2 **Decision Support Function in the Encrypted Domain**

The clinician encrypts each element of the patient data using the public key and sends the encrypted data and the corresponding public key to the server. Due to the encryption is performed with the clinician's public key, no one including the server could decrypt this to obtain the values of the elements; thus, the patient data are protected against being revealed even to the server taking part in this process. Since the server only has the encrypted patient data, it has to compute in the encrypted domain using homomorphic and two-party secure computation properties. Since the Paillier cryptosystem only supports integers, all the variables in will be quantized to the nearest integer value during the computation in the encrypted domain.

3.3 **Information Leakage**

In this algorithm, the private key resides at the clinician side; hence, it is not possible for the remote server which participates in this classification operation to decrypt the test sample or the classification result. However, the remote server interacts with the clinician when the homomorphic properties of Paillier cryptography are not sufficient to complete the task. During the interaction any encrypted values sent by the server could be decrypted by the clinician. It is possible to formally analyze whether this interaction can reveal any server side parameters to the clinician.

4 PERFORMANCE ANALYSIS

In this section, we analyze the performance of the proposed encrypted-domain algorithm. We compare the accuracy of the proposed encrypted-domain method with the conventional plain-domain method. For the experiment, we consider two datasets from the UCI machine learning repository called the Wisconsin Breast Cancer (WBC) and Puma Indian Diabetic (PID) datasets [5]. The WBC dataset contains 681 samples where 444 samples are benign (noncancerous) and 237 samples are malignant (cancerous), while the PID dataset contains 768 samples where 500 samples are malignant and 268 samples are benign. The number of features for each sample in WBC and PID datasets are nine and eight respectively (excluding class label attribute).Table1 shows some examples of training samples after normalization from the WBC and PID datasets.

4.1 Experiments in the Plain Domain

In all experiments, we assume that the training data are not linearly separable and therefore we use the naive bayes method as in (6). Initially, we need to determine empirically an appropriate

value for γ in (6).

TABLE I
SOME EXAMPLES OF NORMALIZED TRAINING SAMPLES OF THE WBC AND PID DATASETS

	Fea. 1	Fea. 2	Fea. 3	Fea. 4	Fea. 5	Fea. 6	Fea. 7	Fea. 8	Fea. 9
Sample 1 [WBC]	-0.1243	0.1970	-0.6986	-0.7383	-0.6366	-0.5541	-0.6966	-0.1754	-0.6101
Sample 2 [WBC]	-0.1196	0.1970	0.2823	0.2666	0.7585	1.6919	1.7700	-0.1754	-0.2827
Sample 3 [PID]	-0.8443	-1.1227	-0.1551	0.5306	-0.6944	-0.6745	-0.3681	-0.1902	-
Sample 4 [PID]	-0.8443	-0.9976	-0.1551	0.1544	0.1195	-0.4858	-0.9209	-1.0412	-
Sample 5 [WBC]	-0.0967	1.2590	2.2442	2.2764	1.8048	1.6919	1.7700	2.2964	1.3543
Sample 6 [WBC]	-0.0570	0.1970	-0.0447	-0.0684	0.0609	-0.5541	-0.1485	0.2365	0.3721
Sample 7 [PID]	0.6395	0.8478	0.1524	0.9067	-0.6944	0.2057	0.4612	1.4266	-
Sample 8 [PID]	1.2331	1.9425	-0.2576	-1.2874	-0.6944	-1.0894	0.5964	-0.1051	-

Hence, we have obtained Tables for the WBC and PID datasets, respectively, in the plain domain using the method described in Section II. These tables show the classification accuracy for various γ values. Let us explain the sixth result column (i.e., γ = 10) in Table III. When γ = 10, the total number of correctly classified benign samples is 433 out of 444 (97.52%) and that of malignant samples is 229 out of 237 (90.72%).

In total, 662 samples were correctly classified out of 681 (97.21%). Similarly, when γ = 15 for the PID dataset as in Table IV, the total number of correctly classified benign samples is 482 out of 500 (96.40%) and that of malignant samples is 239 out of 268 (89.17%). In total 721 samples were correctly classified out of 768 (93.88%). Since γ = 10forWBC dataset and γ = 15for the PID dataset provide higher accuracy than other values in this experiment, without loss of generality, we use γ = 10 for WBC dataset and γ = 15 for the PID dataset for the experiments in the encrypted domain. We also noted that the average number of support vectors used for WBC and PID datasets are 205 and 535, respectively.

4.2 Experiments in the Encrypted Domain

We have now evaluated our algorithm with 2048-bit key size. We tested our proposed privacy-preserving algorithm in a computer with 3.40 GHz processor and 8 GB of RAM running on Windows 64-bit operating system. The algorithm is written in C++ using GNU GMP library version 4.2.4.

Both the server and clinician were modeled as different threads of a single program, which passes variables to each other. As we mentioned in Section III-B, the scaling factors $c1$, $c2$, $c3$, and $c5$,s have influence on the classification accuracy in the encrypted domain due to the fact that the Paillier cryptosystem only encrypts integers. When we set $c1$ = 1, $c2$ =1, $c3$ = 0, and $c5$,s = 0, the classification accuracy reduced to 0%, which shows the importance of the scaling factor in the encrypted domain.

4.3 Communication Complexity

The communication cost of the proposed algorithm depends highly on the size of Paillier cryptography in our implementation the size of an encrypted sample is 2048 bits long. Sending an encrypted test sample with N number of features consumes 2048N bits of bandwidth in the communication channel.

In the proposed algorithm, the server interacts with the clinician for three times. During the second interaction (i.e., for exponentiation) the server sends $|S|$ number of encrypted values (i.e., equal to the total number of support vectors), while in the first and last interaction the server sends only one value. Thus the cost of communication for this algorithm is upper bounded by the second interaction which requires 2048$|S|$kbits of band-width. Since the number of support vectors should be less than the size of the dataset, the worse case bandwidth requirement for both WBC and PID datasets are 0.174 and 0.197MB, respectively.

4.4 Computation Complexity

We measure the computation complexity in terms of the average runtime required for the proposed algorithm when the size of the security parameter N = 2048. The average time required for WBC and PID datasets are 41 and 92 s, respectively. It is noted that average time is increasing linearly, with the number of support vectors used for the classification.

5 RELATED WORK

In general, data classification is a combination of two phases: training phase and testing phase. The first phase, training a classifier, requires a large collection of data. There are various organizations which publish their customers' data for research and monetary purposes. Publishing person-specific dataset (e.g., data related to patients of a cancer hospital) may reveal an individual's identity and breach the privacy of patients.

However, there are various privacy preserving techniques (i.e., anonymization techniques and data perturbation techniques) have been well studied in the literature to preserve the privacy of individuals in the datasets (see [1] and references therein).

However, the proposed study in this paper considers the privacy in the second phase of the data classification task, where clinicians only require to send the test data of their patient to the remote server where the classifier is already established. Since the proposed method preserves the privacy of the training dataset, it is possible for any organization with large data to provide a classification as a service to anybody through the Internet rather than anonymize and publish the dataset in a plain domain. Hence, our method is different from the data anonymization and data perturbation-based methods.

A classification approach has been used in biomedical engineering to diagnose various diseases in the plain domain ([6] and references therein). Note that, any algorithm in the plain domain cannot be used to provide decision support via the Internet due to the privacy issue. Recently, Mathew and Obradovic proposed a privacy preserving framework for clinical decision support using a decision tree-based machine learning technique [1].The study in [7] proposed, for the first time, a strong privacy enhanced protocol for a polynomial kernel-based naive bayes classification using cryptographic primitives; where the authors assumed that the training data are distributed. Hence, to preserve privacy, they developed a protocol to perform secure kernel sharing, prediction, and training using secret sharing and

homomorphic encryption techniques.

At the end of the training each party will hold a share of the secret. In the testing phase, all parties collaboratively perform the classification using their shared secrets. At the end of the protocol each party will hold a share of the predicted class label.

Since the work is based on secret sharing, all the parties must be involved in every operation of calculating the kernel values and predicting the class. Hence, it is suitable only for the distributed scenario and not for the client-server model considered in this paper.

In the client-server model, the client just sends the new data in the encrypted domain and is minimally involved in interactions with the server during the classification process. Moreover, the method developed in [7] considered only the polynomial kernel and so it cannot be modified directly to work with the Gaussian kernel-based naive bayes classifier is considered in this paper as these kernel functions are of different forms.

The recent study in [8] discusses the issue of releasing the trained naive bayes classifier without violating the privacy of patient's results. While the Gaussian kernel was considered, a Taylor series was exploited to approximate the infinite dimension of the Gaussian kernel into finite dimension subject to negligible performance loss. Since this works purely in the plain domain, it cannot be modified to the clinician-server scenario considered in this paper.

6 CONCLUSION

In this paper, we have proposed a privacy-preserving decision support system using a Gaussian kernel based naive bayes classifier. Since the proposed algorithm is a potential application of emerging outsourcing techniques such as cloud computing technology, rich clinical datasets (or healthcare knowledge) available in remote locations could be used by any clinician via the Internet without compromising privacy, thereby enhancing the decision-making ability of healthcare professionals. We have exploited the homomorphic properties of the Paillier cryptosystem within our algorithm, where the cryptosystem only encrypts integer values. Hence, we proposed a novel technique to scale the continuous variables involved in the process without compromising the performance and privacy. To validate the performance, we have evaluated our method on two medical datasets and the results showed that the accuracy is up to 97.21%. Importantly, the benefit of our encrypted-domain method is that patient data need not be revealed to the remote server as they can remain in encrypted form at all times, even during the diagnosis process.

7.1 Acknowledgments

We would like to thank UCI repository of machine learning databases for the use of several of their public datasets.

8 REFERENCES

[1]Rahulamathavan, Y. Veluru, S. Phan, R.C.-W. Chambers, J.A. Rajarajan, M. "Privacy-Preserving Clinical Decision Support System Using Gaussian Kernel-Based Classification", IEEE Journal of BioMedical And Health Informatics, Volume 18,No. 1,pp:56-66,2014.

[2] 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.

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

[4] P. Paillier, "Public-key cryptosystems based on composite degree residuosityclasses." in *Advances in Cryptology—EUROCRYPT'99*. Springer, Berlin, Heidelberg, 1999.

[5] O. L. Mangasarian,W. N. Street, andW. H.Wolberg, "Breast cancer diagnosis and prognosis via linear programming," *Oper. Res.*, vol. 43, pp. 570–577, Jul./Aug. 1995.

[6]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.

[7] K. Chen and L. Liu, "Privacy preserving data classification with rotation perturbation," in *Proc. 5th IEEE Int. Conf. DataMining*, Washington, DC,USA, 2005, pp. 589–592.

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

[9] B. H. Cho, H. Yu, K. Kim, T. H. Kim, I. Y. Kim, and S. I. Kim, "Application of irregular and unbalanced data to predict diabetic nephropathy using visualization and feature selection Methods," *Journal Artificial Intelligence in Medicine.* 2008, vol. 42, pp. 37-53.

[10] H. N. A. Pham and E. Triantaphyllou, "Prediction of Diabetes by Employing a New Data Mining Approach Which Balance Fitting and Generalization," *Computer and Information Science.* 2008, vol. 131, pp. 11-26.