

In fact, the unique matrix A_i could not be calculated if the kernel matrix $K(A, A^T)$ is the only known. Therefore, we conclude that the sample x_i could not be calculated if the kernel matrix $K(x_i^T, A_i^T)$ is the only known. So there is no any entity disclose its information from A_i or x_i .

V. Experiments on Datasets

The performance of proposed approach and standard SVM is compared in two datasets: part of PAMAP2 Physical Activity Monitoring dataset and full SMS Spam Collection Data Set. The PAMAP2 Physical Activity Monitoring dataset [24] contains data of 18 different physical activities (such as walking, cycling, playing soccer, etc.), performed by 9 subjects wearing 3 inertial measurement units and a heart rate monitor. The dataset can be used for activity recognition and intensity estimation, while developing and applying algorithms of data processing, segmentation, feature extraction and classification. SMS Spam Collection Data Set [25] is a collection of 425 SMS spam messages was manually extracted from the Grumbletext Web site and a subset of 3,375 SMS randomly chosen ham messages of the NUS SMS Corpus (NSC), which is a dataset of about 10,000 legitimate messages collected for research at the Department of Computer Science at the National University of Singapore. A list of 450 SMS ham messages collected from Caroline Tag's PhD Thesis. Finally, it has 1,002 SMS ham messages and 322 spam messages. Assuming the data of PAMAP2 Physical Activity Monitoring dataset is vertical distributed and held separately as 18 entities by 18 different physical activities. And the data of SMS Spam Collection Data Set is also vertical distributed and held separately as 2 entities by the ham messages and the spam messages. The classification accuracy result of the proposed optimized privacy protection SVM is shown in Table.1 and compared with the standard multi-class classification SVM [26]. The accuracy is improved by the proposed method under two kinds of datasets which has different dimension size. On the PAMAP2 Physical Activity Monitoring dataset, the proposed approach achieved better performance than on SMS Spam Collection Data Set.

TABLE III Classification Accuracy Results

Datasets (Dimension)	optimized privacy protection SVM	multi-class classification SVM
PAMAP2 (2500,18)	93.87%	90.05%
SMS Spam (1324,2)	96.44%	95.19%

VI. Conclusion

The validity and reliability of one novel optimized privacy protection SVM is proved as being greater than standard multi-class classification SVM on privacy-preserving by building and testing on two datasets. Compared with standard approach, the optimized privacy protection SVM has the advantage on the

classification accuracy and the privacy protection. The present study only compared the two procedures on small databases. The testing on additional datasets and different types of data will be necessary to assess the generalisability of these results.

References

- [1] L.M. Kaufman, "Data Security in the World of Cloud Computing," IEEE Security & Privacy, July-Aug. 2009, pp.61-64.
- [2] R. Buyya, C.S. Yeo and S. Venugopal, "Market-Oriented Cloud Computing: Vision, Hype, and Reality for Delivering IT Services as Computing Utilities," Dalian: 10th IEEE International Conference on High Performance Computing and Communications (HPCC 2008), Sept. 25-27, 2008.
- [3] <https://cloudsecurityalliance.org/about/>
- [4] <http://www.opencloudmanifesto.org/opencloudmanifesto1.htm>
- [5] <http://www.cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf>.
- [6] F. Hu, M. Qiu, and J. Li, et al, "A review on cloud computing: Design challenges in architecture and security," Journal of Computing and Information Technology 2011:25-55.
- [7] A. Shamir, "Identity-based cryptosystems and signature schemes," In: Blakely, G.R., Chaum,D. (eds.) CRYPTO 1984. LNCS, Springer, Heidelberg, vol. 196, pp. 47-53, 1985.
- [8] D.Boneh and M. Franklin, "Identity-based encryption from the weil pairing," In Advances in Cryptology-CRYPTO, pp.213-229, 2001.
- [9] J.Baek and Y. Zheng, "Identity-based threshold decryption," Public Key Cryptography – PKC 2004. 2947: pp. 262-276, 2004.
- [10]N.M. Joseph, E. Daniel and N.A.Vasanthi, "A Scalable Privacy-Preserving Verification Correctness Protocol to Identify Corrupted Data in Cloud Storage," International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), 2013, 2(3): pp: 0951-0956.
- [11]M.S. Ackerman., "Privacy in pervasive environments: next generation labeling protocols," Personal and Ubiquitous Computing, 2004, 8(6): 430-439.
- [12]L. Sweeney, "k-anonymity: a model for protecting privacy," International Journal on Uncertainty, Fuzziness and Knowledge-based Systems, 10 (5), 2002: 557-570.
- [13]<http://www.w3.org/P3P/>
- [14]F. Olumofin and I. Goldberg, "Revisiting the computational practicality of private information retrieval," Financial Cryptography and Data Security. Springer Berlin Heidelberg, 2012: 158-172.
- [15]B.Chor, E. Kushilevitz and O. Goldreich, et al, "Private information retrieval," Journal of the ACM (JACM), 1998, 45(6): 965-981.
- [16]A. Ambainis, "Upper bound on the communication complexity of private information retrieval," Automata, Languages and Programming. Springer Berlin Heidelberg, 1997: 401-407.
- [17]D.Asonov, "Querying Databases Privately: A New Approach To Private Information Retrieval," SpringerVerlag, 2004
- [18]O. Goldreich, "Secure multi-party computation," Manuscript. Preliminary version, 1998.
- [19]H. Yu, X Jiang and J. Vaidya, "Privacy-preserving SVM using nonlinear kernels on horizontally partitioned data," Proceedings of the 2006 ACM symposium on Applied computing. ACM, 2006: 603-610.
- [20]V. Keeman, "Learning and soft computing, support vector machines," Neural Networks and Fuzzy Logic Models, The MIT Press, Cambridge, MA, 2001.
- [21]H. Yu, J. Vaidya, X.Jiang, "Privacy-preserving svm classification on vertically partitioned data," Advances in Knowledge Discovery and Data Mining. Springer Berlin Heidelberg, 2006: 647-656.
- [22]V. Vapnik, "The nature of statistical learning Theory," NY:Spring-Verlag,1995
- [23]Reddy, B. Rama Sanjeeva, D. Vakula, and N. V. S. N. Sarma. , "Circular antenna array pattern analysis using radial basis function neural network," IOP Conference Series: Materials Science and Engineering. Vol. 44. No. 1. IOP Publishing, 2013.
- [24]<http://archive.ics.uci.edu/ml/datasets/PAMAP2+Physical+Activity+Monitoring>
- [25]<http://archive.ics.uci.edu/ml/datasets/SMS+Spam+Collection>
- [26]<http://www.csie.ntu.edu.tw/~cjlin/libsvm/>