[11] H. Drucker, C. J. C. Burges, L. Kaufman, A. J. Smola, and V. Vapnik. 1997. Support Vector Regression Machines. In *Advances in Neural Information Processing Systems*.

[12] M. Fredrikson, S. Jha, and T. Ristenpart. 2015. Model Inversion Attacks that Exploit Confidence Information and Basic Countermeasures. In *CCS*.

[13] J. Friedman, T. Hastie, R. Tibshirani, et al. 2000. Additive Logistic Regression: A Statistical View of Boosting. *The Annals of Statistics* (2000).

[14] O. Goldreich, S. Micali, and A. Wigderson. 1987. How to Play any Mental Game. In *STOC*.

[15] I. Goodfellow, Y. Bengio, A. Courville, and Y. Bengio. 2016. *Deep Learning*. MIT press Cambridge.

[16] P. Hallgren, C. Orlandi, and A. Sabelfeld. 2017. PrivatePool: Privacy-Preserving Ridesharing. In *Computer Security Foundations*.

[17] J. Hayes, L. Melis, G. Danezis, and E. De Cristofaro. 2019. LOGAN: Membership Inference Attacks against Generative Models. *PETs* (2019).

[18] W. Henecka, A.-R. Sadeghi, T. Schneider, and I. Wehrenberg. 2010. TASTY: Tool for Automating Secure Two-Party Computations. In *CCS*.

[19] D. W. Hosmer Jr, S. Lemeshow, and R. X. Sturdivant. 2013. *Applied Logistic Regression*. John Wiley & Sons.

[20] K. Järvinen, Á. Kiss, T. Schneider, O. Tkachenko, and Z. Yang. 2018. Faster Privacy-Preserving Location Proximity Schemes. In *CANS*.

[21] K. Järvinen, H. Leppäkoski, E. S. Lohan, P. Richter, T. Schneider, O. Tkachenko, and Z. Yang. 2019. PILOT: Practical Privacy-Preserving Indoor Localization using OuTsourcing. In *EuroS&P*.

[22] M. Kesarwani, B. Mukhoty, V. Arya, and S. Mehta. 2018. Model Extraction Warning in MLaaS Paradigm. *Computer Security Applications* (2018).

[23] B. Kulynych, J. Hayes, N. Samarin, and C. Troncoso. 2018. Evading Classifiers in Discrete Domains with Provable Optimality Guarantees. In *NeurIPS Workshop on Security in Machine Learning*.

[24] S. Laur, H. Lipmaa, and T. Mielikäinen. 2006. Cryptographically Private Support Vector Machines. In *Knowledge Discovery and Data Mining*.

[25] J. Liu and E. Zio. 2016. An Adaptive Online Learning Approach for Support Vector Regression: Online-SVR-FID. *Mechanical Systems and Signal Processing* (2016).

[26] D. Lowd and C. Meek. 2005. Adversarial Learning. In *Knowledge Discovery in Data Mining*.

[27] L. M. Manevitz and M. Yousef. 2001. One-Class SVMs for Document Classification. *Machine Learning Research* (2001).

[28] S. Mika, G. Ratsch, J. Weston, B. Scholkopf, and K.-R. Mullers. 1999. Fisher Discriminant Analysis with Kernels. In *Neural Networks for Signal Processing*.

[29] J. H Min and Y.-C. Lee. 2005. Bankruptcy Prediction using Support Vector Machine with Optimal Choice of Kernel Function Parameters. *Expert Systems with Applications* (2005).

[30] K. Pace. 1999. *Boston House Prices Dataset*. http://lib.stat.cmu.edu/datasets/boston_corrected.txt

[31] K. Pace. 1999. *Califonria Housing Dataset*. http://lib.stat.cmu.edu/datasets/houses.zip

[32] P. Paillier. 1999. Public-Key Cryptosystems Based on Composite Degree Residuosity Classes. In *EUROCRYPT*.

[33] N. Papernot, P. McDaniel, I. Goodfellow, S. Jha, Z. B. Celik, and A. Swami. 2017. Practical Black-Box Attacks Against Machine Learning. In *ASIACCS*.

[34] K. Polat and S. Güneş. 2007. Breast Cancer Diagnosis using Least Square Support Vector Machine. *Digital Signal Processing* (2007).

[35] J. R. Quinlan. 1986. Induction of Decision Trees. *Machine learning* (1986).

[36] Y. Rahulamathavan, R. C.-W. Phan, S. Veluru, K. Cumanan, and M. Rajarajan. 2014. Privacy-Preserving Multi-Class Support Vector Machine for Outsourcing the Data Classification in Cloud. *Dependable and Secure Computing* (2014).

[37] B. I. P. Rubinstein, B. Nelson, L. Huang, A. D. Joseph, S. Lau, S. Rao, N. Taft, and J. D. Tygar. 2009. Antidote: Understanding and Defending against Poisoning of Anomaly Detectors. In *Internet Measurement*.

[38] D. W. Ruck, S. K. Rogers, M. Kabrisky, M. E. Oxley, and B. W. Suter. 1990. The Multilayer Perceptron as an Approximation to a Bayes Optimal Discriminant Function. *Neural Networks* (1990).

[39] A. R. J. Ruiz, G. M. Mendoza-Silva, R. Montoliu, F. Seco, and J. Torres-Sospedra. 2016. *IPIN 2016 Tutorial Dataset*. http://indoorloc.uji.es/ipin2016track3/

[40] A.-R. Sadeghi and T. Schneider. 2008. Generalized Universal Circuits for Secure Evaluation of Private Functions with Application to Data Classification. In *Information Security and Cryptology*.

[41] A. Salem, Y. Zhang, M. Humbert, P. Berrang, M. Fritz, and M. Backes. 2019. Ml-leaks: Model and Data Independent Membership Inference Attacks and Defenses on Machine Learning Models. In *NDSS*.

[42] J. Schmidhuber. 2015. Deep Learning in Neural Networks: An Overview. *Neural Networks* (2015).

[43] Y. Shi, Y. Sagduyu, and A. Grushin. 2017. How to Steal a Machine Learning Classifier with Deep Learning. In *Technologies for Homeland Security*.

[44] R. Shokri, M. Stronati, C. Song, and V. Shmatikov. 2017. Membership Inference Attacks against Machine Learning Models. In *S&P*.

[45] A. J. Smola and B. Schölkopf. 2004. A Tutorial on Support Vector Regression. *Statistics and Computing* (2004).

[46] J. A. K. Suykens and J. Vandewalle. 1999. Least Squares Support Vector Machine Classifiers. *Neural Processing Letters* (1999).

[47] J. Torres-Sospedra, R. Montoliu, A. Martínez-Usó, T. J. Arnau, J. P. Avariento, M. Benedito-Bordonau, and J. Huerta. 2014. *Multi-Building Multi-Floor Indoor Localization Database*. https://archive.ics.uci.edu/ml/datasets/ujiindoorloc

[48] F. Tramèr, F. Zhang, A. Juels, M. K. Reiter, and T. Ristenpart. 2016. Stealing Machine Learning Models via Prediction APIs. In *USENIX Security*.

[49] L. G. Valiant. 1984. A Theory of the Learnable. *Communications of the ACM* (1984).

[50] V. Vapnik, E. Levin, and Y. L. Cun. 1994. Measuring the VC-dimension of a Learning Machine. *Neural Computation* (1994).

[51] B. Wang and N. Z. Gong. 2018. Stealing Hyperparameters in Machine Learning. *arXiv preprint arXiv:1802.05351* (2018).

[52] Q. Wu and D.-X. Zhou. 2005. SVM Soft Margin Classifiers: Linear Programming versus Quadratic Programming. *Neural Computation* (2005).

[53] Z. Yang and K. Järvinen. 2018. The Death and Rebirth of Privacy-Preserving WiFi Fingerprint Localization with Paillier Encryption. In *INFOCOM*.

[54] A. C.-C. Yao. 1986. How to Generate and Exchange Secrets. In *FOCS*.

[55] H. Yu, X. Jiang, and J. Vaidya. 2006. Privacy-Preserving SVM using Nonlinear Kernels on Horizontally Partitioned Data. In *Applied Computing*.

[56] T. Zhang, S. S. M. Chow, Z. Zhou, and M. Li. 2016. Privacy-Preserving Wi-Fi Fingerprinting Indoor Localization. In *International Workshop on Security*.

[57] F. Ö. Çatak. 2015. Secure Multi-Party Computation Based Privacy Preserving Extreme Learning Machine Algorithm over Vertically Distributed Data. In *Neural Information Processing*.