**REFERENCES**

[1] Z.Wang, S. Yan, and C. Zhang, “Active learning with adaptive regularization,”

*Pattern Recognit.*, vol. 44, no. 10/11, pp. 2375–2383, 2011.

[2] B. Gutierrez-Nieto, C. Serrano-Cinca, and J. Camon-Cala, “A credit score

system for socially responsible lending,” *J. Bus. Ethics*, vol. 133, no. 4,

pp. 691–701, 2016.

[3] L. Thomas, J. Crook, andD. Edelman, *Credit Scoring and its Applications*,

vol. 2. Philadelphia, PA, USA: SIAM, 2017.

[4] R. Zeidan, C. Boechat, and A. Fleury, “Developing a sustainability credit

score system,” *J. Bus. Ethics*, vol. 127, no. 2, pp. 283–296, 2015.

[5] L. Zhou, K. K. Lai, and L. Yu, “Least squares support vector machines

ensemble models for credit scoring,” *Expert Syst. Appl.*, vol. 37, no. 1,

pp. 127–133, 2010.

[6] Y. Li, J. Gao, A. Z. Enkavi, L. Zaval, E. U.Weber, and E. J. Johnson, “Sound

credit scores and financial decisions despite cognitive aging,” *Proc. Nat.*

*Acad. Sci. USA*, vol. 112, no. 1, pp. 65–69, 2015.

[7] G. N. Masters, “Partial credit model,” in *Handbook of Item Response*

*Theory*, vol. 1. London, U.K.: Chapman & Hall, 2016, pp. 137–154.

[8] S. Y. Sohn, D. H. Kim, and J. H. Yoon, “Technology credit scoring model

with fuzzy logistic regression,” *Appl. Soft Comput.*, vol. 43, pp. 150–158,

2016. [9] H. J. Smith, T. Dinev, and H. Xu, “Information privacy research: An

interdisciplinary review,” *MIS Quart.*, vol. 35, no. 4, pp. 989–1015, 2011.

[10] D. Malandrino andV. Scarano, “Privacy leakage on the web: Diffusion and

countermeasures,” *Comput. Netw.*, vol. 57, no. 14, pp. 2833–2855, 2013.

[11] Y. Li, W. Dai, Z. Ming, and M. Qiu, “Privacy protection for preventing

data over-collection in smart city,” *IEEE Trans. Comput.*, vol. 65, no. 5,

pp. 1339–1350, May 2016.

[12] D. Malkhi, N. Nisan, B. Pinkas, and Y. Sella, “Fairplay—A secure twoparty

computation system,” in *Proc. 13th Conf. USENIX Secur. Symp.*,

vol. 13, no. 1, pp. 1–20, 2004.

[13] Y. Huang, D. Evans, J. Katz, and L. Malka, “Faster secure two-party

computation using garbled circuits,” in *Proc. 20th USENIX Secur. Symp.*,

San Francisco, CA, USA, no.1, pp. 1–35, 2011.

[14] M. J. Freedman, K. Nissim, and B. Pinkas, “Efficient private matching and

set intersection,” in *Proc. Int. Conf. Theory Appl. Cryptographic Techn.*,

2004, pp. 1–19.

[15] B. Goethals, S. Laur, H. Lipmaa, and T. Mielikäinen, “On private scalar

product computation for privacy-preserving data mining,” in *Proc. 7th Int.*

*Conf. Inf. Secur. Cryptology.*, Seoul, South Korea, 2004, pp. 104–120.

[16] R. Dowsley, J. van de Graaf, D. Marques, and A. C. A. Nascimento, “A

two-party protocol with trusted initializer for computing the inner product,”

in *Proc. 11th Int. Workshop Inf. Secur. Appl.*, Jeju Island, South Korea,

Aug. 2010 pp. 337–350.

[17] C. Gentry and D. Boneh, *A Fully Homomorphic Encryption Scheme*,

vol. 20. Stanford, CA, USA: Stanford Univ. Press, 2009.

[18] M. van Dijk, C. Gentry, S. Halevi, and V. Vaikuntanathan, “Fully homomorphic

encryption over the integers,” in *Proc. 29th Annu. Int. Conf.*

*Theory Appl. Cryptographic Techn.*, 2010, pp. 24–43.

[19] U. Feige, A. Fiat, and A. Shamir, “Zero-knowledge proofs of identity,” *J.*

*Cryptology*, vol. 1, no. 2, pp. 77–94, 1988.

[20] I. Damgård, “On *σ*-protocols,” Lecture Notes, Dept. Comput. Sci., Univ.

Aarhus, Aarhus, Denmark, 2002.

[21] S. Goldwasser, S. Micali, and C. Rackoff, “The knowledge complexity of

interactive proof systems,” *SIAM J. Comput.*, vol. 18, no. 1, pp. 186–208,

1989.

[22] M. Blum, A. De Santis, S. Micali, and G. Persiano, “Non-interactive zero

knowledge,” *Siam J. Comput.*, vol. 20, no. 6, pp. 1084–1118, 1991.

[23] J. Groth, R. Ostrovsky, and A. Sahai, “New techniques for noninteractive

zero-knowledge,” *J. ACM*, vol. 59, no. 3, 2012, Art. no. 11.

[24] P. Paillier, “Public-key cryptosystems based on composite degree residuosity

classes,” in *Proc. Int. Conf. Theory Appl. Cryptographic Techn.*,

Prague, Czech Republic, May. 1999 pp. 223–238.

[25] I. Damgård, M. Jurik, and J. B. Nielsen, “A generalization of Paillier’s

public-key system with applications to electronic voting,” *Int. J. Inf. Secur.*,

vol. 9, no. 6, pp. 371–385, 2010.