**REFERENCES**

[1] F. R. Yu, “Connected vehicles for intelligent transportation systems [Guest editorial],” IEEE Trans. Veh. Technol., vol. 65, no. 6, pp. 3843–3844, Jun. 2016.

[2] K. Abboud and W. Zhuang, “Impact of node mobility on single-hop cluster overlap in vehicular ad hoc networks,” in Proc. 17th ACM Int. Conf. Modeling, Anal. Simulation Wireless Mobile Syst. (MSWiM), 2014, pp. 65–72.

[3] Y. Guo, Q. Yang, F. R. Yu, and V. C. M. Leung, “Cache-enabled adaptive video streaming over vehicular networks: A dynamic approach,” IEEE Trans. Veh. Technol., vol. 67, no. 6, pp. 5445–5459, Jun. 2018.

[4] P. Tyagi and D. Dembla, “Investigating the security threats in vehicular ad hoc networks (VANETs): Towards security engineering for safer on-road transportation,” in Proc. Int. Conf. Adv. Comput., Commun. Informat. (ICACCI), Sep. 2014, pp. 2084–2090.

[5] M. N. Mejri, J. Ben-Othman, and M. Hamdi, “Survey on VANET security challenges and possible cryptographic solutions,” Veh. Commun., vol. 1, no. 2, pp. 53–66, Apr. 2014.

[6] Y. He, F. R. Yu, Z. Wei, and V. Leung, “Trust management for secure cognitive radio vehicular ad hoc networks,” Ad Hoc Netw., vol. 86, pp. 154–165, Apr. 2019.

[7] P. Mach and Z. Becvar, “Mobile edge computing: A survey on architecture and computation offloading,” IEEE Commun. Surveys Tuts., vol. 19, no. 3, pp. 1628–1656, 3rd Quart., 2017.

[8] Y. Mao, C. You, J. Zhang, K. Huang, and K. B. Letaief, “A survey on mobile edge computing: The communication perspective,” IEEE Commun. Surveys Tuts., vol. 19, no. 4, pp. 2322–2358, 4th Quart., 2017.

[9] Z. Xiao and Y. Xiao, “Security and privacy in cloud computing,” IEEE Commun. Surveys Tuts., vol. 15, no. 2, pp. 843–859, 2nd Quart., 2013.

[10] M. Liu, F. R. Yu, Y. Teng, V. C. M. Leung, and M. Song, “Distributed resource allocation in blockchain-based video streaming systems with mobile edge computing,” IEEE Trans. Wireless Commun., vol. 18, no. 1, pp. 695–708, Jan. 2019.

[11] R. Yang, F. R. Yu, P. Si, Z. Yang, and Y. Zhang, “Integrated blockchain and edge computing systems: A survey, some research issues and challenges,” IEEE Commun. Surveys Tuts., vol. 21, no. 2, pp. 1508–1532, 2nd Quart., 2019.

[12] P. K. Sharma, M.-Y. Chen, and J. H. Park, “A software defined fog node based distributed blockchain cloud architecture for IoT,” IEEE Access, vol. 6, pp. 115–124, 2018.

[13] J. Xie et al., “A survey of blockchain technology applied to smart cities: Research issues and challenges,” IEEE Commun. Surveys Tuts., vol. 21, no. 3, pp. 2794–2830, 3rd Quart., 2019.

[14] C. Qiu, F. R. Yu, H. Yao, C. Jiang, F. Xu, and C. Zhao, “Blockchainbased software-defined industrial Internet of Things: A dueling deep Q -Learning approach,” IEEE Internet Things J., vol. 6, no. 3, pp. 4627–4639, Jun. 2019.

[15] W. G. Ethereum, “A secure decentralised generalised transaction ledger,” Ethereum Project Yellow Paper, vol. 151, pp. 1–32, Apr. 2014.

[16] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, “Blockchain for secure EHRs sharing of mobile cloud based E-health systems,” IEEE Access, vol. 7, pp. 66792–66806, 2019.

[17] H. G. Do and W. K. Ng, “Blockchain-based system for secure data storage with private keyword search,” in Proc. IEEE World Congr. Services (SERVICES), Jun. 2017, pp. 90–93.

[18] D. Shibin and G. J. W. Kathrine, “A comprehensive overview on secure offloading in mobile cloud computing,” in Proc. 4th Int. Conf. Electron. Commun. Syst. (ICECS), Feb. 2017, pp. 121–124.

[19] S. Han et al., “Energy efficient secure computation offloading in NOMAbased mMTC networks for IoT,” IEEE Internet Things J., vol. 6, no. 3, pp. 5674–5690, Jun. 2019.

[20] I. Elgendy, W. Zhang, C. Liu, and C.-H. Hsu, “An efficient and secured framework for mobile cloud computing,” IEEE Trans. Cloud Comput., early access, Jun. 18, 2018, doi: 10.1109/TCC.2018.2847347.

[21] R. Xu, Y. Chen, E. Blasch, and G. Chen, “BlendCAC: A smart contract enabled decentralized capability-based access control mechanism for the IoT,” Computers, vol. 7, no. 3, p. 39, Jul. 2018.

[22] O. J. A. Pinno, A. R. A. Gregio, and L. C. E. De Bona, “ControlChain: Blockchain as a central enabler for access control authorizations in the IoT,” in Proc. IEEE Global Commun. Conf. (GLOBECOM), Dec. 2017, pp. 1–6.

[23] I. Satoh, “Toward access control model for context-aware services offloaded to cloud computing,” in Proc. IEEE 35th Symp. Reliable Distrib. Syst. Workshops (SRDSW), Sep. 2016, pp. 7–12.

[24] J. Xu, L. Chen, K. Liu, and C. Shen, “Designing security-aware incentives for computation offloading via device-to-device communication,” IEEE Trans. Wireless Commun., vol. 17, no. 9, pp. 6053–6066, Sep. 2018.