REFERENCES

[1] Z. Hussain, A. Akhunzada, J. Iqbal, I. Bibi, and A. Gani, ``Secure IIoTenabled industry 4.0,'' *Sustainability*, vol. 13, no. 22, p. 12384, Nov. 2021.

[2] R. K. Barik, H. Dubey, K. Mankodiya, S. A. Sasane, and C. Misra, ``Geo-Fog4Health: A fog-based SDI framework for geospatial health big data analysis,'' *J. Ambient Intell. Hum. Comput.*, vol. 10, no. 2, pp. 551_567, Feb. 2019.

[3] S. Khan, S. Parkinson, and Y. Qin, ``Fog computing security: A review of current applications and security solutions,'' *J. Cloud Comput.*, vol. 6, no. 1, pp. 1_22, Dec. 2017.

[4] J. Malik, A. Akhunzada, I. Bibi, M. Talha, M. A. Jan, and M. Usman, ``Security-aware data-driven intelligent transportation systems,'' *IEEE Sensors J.*, vol. 21, no. 14, pp. 15859_15866, Jul. 2021.

[5] Z. Ning, X. Hu, Z. Chen, M. Zhou, B. Hu, J. Cheng, and M. S. Obaidat, ``A cooperative quality-aware service access system for social internet of vehicles,'' *IEEE Internet Things J.*, vol. 5, no. 4, pp. 2506_2517, Aug. 2018.

[6] X. Wang, Z. Ning, M. C. Zhou, X. Hu, L. Wang, Y. Zhang, F. R. Yu, and B. Hu, ``Privacy-preserving content dissemination for vehicular social networks: Challenges and solutions,'' *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1314_1345, 2nd Quart., 2019.

[7] Z. Ning, Y. Li, P. Dong, X. Wang, M. S. Obaidat, X. Hu, L. Guo, Y. Guo, J. Huang, and B. Hu, ``When deep reinforcement learning meets 5Genabled vehicular networks: A distributed of_oading framework for traf_c big data,'' *IEEE Trans. Ind. Informat.*, vol. 16, no. 2, pp. 1352_1361, Feb. 2020.

[8] X.Wang, Z. Ning, and L.Wang, ``Of_oading in internet of vehicles: A fogenabled

real-time traf_c management system,'' *IEEE Trans. Ind. Informat.*,

vol. 14, no. 10, pp. 4568_4578, Oct. 2018.

[9] H. Dubey, J. Yang, N. Constant, A. M. Amiri, Q. Yang, and K. Makodiya,

``Fog data: Enhancing telehealth big data through fog computing,'' in *Proc.*

ASE BigData Socialinform., 2015, pp. 1_6.

[10] W. U. Khan, T. N. Nguyen, F. Jameel, M. A. Jamshed, H. Pervaiz,

M. A. Javed, and R. Jäntti, ``Learning-based resource allocation for

backscatter-aided vehicular networks,'' *IEEE Trans. Intell. Transp. Syst.*,

early access, Nov. 18, 2021, doi: 10.1109/TITS.2021.3126766.

[11] A. M. Rahmani, T. N. Gia, B. Negash, A. Anzanpour, I. Azimi, M. Jiang,

and P. Liljeberg, ``Exploiting smart e-health gateways at the edge of

healthcare Internet-of-Things: A fog computing approach,'' *Future Gener.*

Comput. Syst., vol. 78, pp. 641_658, Jan. 2018.

[12] 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.

[13] Q. Yan, F. R. Yu, Q. Gong, and J. Li, ``Software-de_ned networking

(SDN) and distributed denial of service (DDoS) attacks in cloud computing

environments: A survey, some research issues, and challenges,'' *IEEE*

Commun. Surveys Tuts., vol. 18, no. 1, pp. 602_622, 1st Quart., 2016.

[14] S. S. C. Silva, R. M. P. Silva, R. C. G. Pinto, and R. M. Salles, ``Botnets:

A survey,'' *Comput. Netw.*, vol. 57, no. 2, pp. 378_403, 2013.

[15] J. Malik, A. Akhunzada, I. Bibi, M. Imran, A. Musaddiq, and S. W. Kim,

``Hybrid deep learning: An ef_cient reconnaissance and surveillance detection

mechanism in SDN,'' *IEEE Access*, vol. 8, pp. 134695_134706, 2020.

[16] T. Hasan, A. Adnan, T. Giannetsos, and J. Malik, ``Orchestrating SDN

control plane towards enhanced IoT security," in *Proc. 6th IEEE Conf.
Netw. Softw. (NetSoft)*, Jun. 2020, pp. 457_464.

[17] W. U. Khan, J. Liu, F. Jameel, V. Sharma, R. Jäntti, and Z. Han, ``Spectral
ef_ciency optimization for next generation NOMA-enabled IoT networks,"
IEEE Trans. Veh. Technol., vol. 69, no. 12, pp. 15284_15297,
Dec. 2020.

[18] L. Yu, Q. Wang, G. Barrineau, J. Oakley, R. R. Brooks, and K.-C. Wang,
``TARN: A SDN-based traf_c analysis resistant network architecture," in
Proc. 12th Int. Conf. Malicious Unwanted Softw. (MALWARE), Oct. 2017,
pp. 91_98.

[19] E. Rodríguez, B. Otero, N. Gutiérrez, and R. Canal, ``A survey of deep
learning techniques for cybersecurity in mobile networks," *IEEE Commun. Surveys
Tuts.*, vol. 23, no. 3, pp. 1920_1955, 3rd Quart., 2021. [20] T. A. Tang, L. Mhamdi,
D. McLernon, S. A. R. Zaidi, and M. Ghogho,
``Deep recurrent neural network for intrusion detection in SDN-based
networks," in *Proc. 4th IEEE Conf. Netw. Softw. Workshops (NetSoft)*,
Jun. 2018, pp. 202_206.

[21] R. Chen,W. Niu, X. Zhang, Z. Zhuo, and F. Lv, ``An effective
conversationbased
botnet detection method," *Math. Problems Eng.*, vol. 2017, pp. 1_9,
Apr. 2017.

[22] S. Al-mashhadi, M. Anbar, I. Hasbullah, and T. A. Alamiedy, ``Hybrid
rulebased
botnet detection approach using machine learning for analysing DNS
traf_c," *PeerJ Comput. Sci.*, vol. 7, p. e640, Aug. 2021.

[23] A. O. Proko_ev, Y. S. Smirnova, and V. A. Surov, ``A method to detect
Internet of Things botnets," in *Proc. IEEE Conf. Russian Young Res. Electr.*

Electron. Eng. (EIConRus), Jan. 2018, pp. 105_108.

[24] M.Waqas, K. Kumar, A. A. Laghari, U. Saeed, M. M. Rind, A. A. Shaikh, F. Hussain, A. Rai, and A. Q. Qazi, ``Botnet attack detection in Internet of Things devices over cloud environment via machine learning,'' *Concurrency Comput., Pract. Exp.*, vol. 34, no. 4, Feb. 2022, Art. no. e6662.

[25] J. A. Faysal, S. T. Mostafa, J. S. Tamanna, K. M. Mumenin, M. M. Ari_n, M. A. Awal, A. Shome, and S. S. Mostafa, ``XGB-RF: A hybrid machine learning approach for IoT intrusion detection,'' *Telecom*, vol. 3, no. 1, pp. 52_69, Jan. 2022.