**BIBILOGRAPHY**

[1] L. A. Mohammed and K. Munir, “Secure third party auditor (tpa) for ensuring data integrity in fog computing,” International Journal of Network Security & Its Applications (IJNSA) Vol, vol. 10, 2018.

[2] S. Chakraborty, S. Singh, and S. Thokchom, “Integrity checking using third party auditor in cloud storage,” in 2018 Eleventh International Conference on Contemporary Computing (IC3). IEEE, 2018, pp. 1–6.

[3] L. Zhou, A. Fu, S. Yu, M. Su, and B. Kuang, “Data integrity verification of the outsourced big data in the cloud environment: A survey,” Journal of Network and Computer Applications, vol. 122, pp. 1–15, 2018.

[4] J. Ni, K. Zhang, X. Lin, and X. S. Shen, “Securing fog computing for internet of things applications: Challenges and solutions,” IEEE Communications Surveys & Tutorials, vol. 20, no. 1, pp. 601–628, 2017.

[5] S. Khan, S. Parkinson, and Y. Qin, “Fog computing security: a review of current applications and security solutions,” Journal of Cloud Computing, vol. 6, no. 1, p. 19, 2017.

[6] M. Mukherjee, R. Matam, L. Shu, L. Maglaras, M. A. Ferrag, N. Choudhury, and V. Kumar, “Security and privacy in fog computing: Challenges,” IEEE Access, vol. 5, pp. 19 93–19 304, 2017.

[7] V. Moysiadis, P. Sarigiannidis, and I. Moscholios, “Towards distributed data management in fog computing,” Wireless Communications and Mobile Computing, vol. 2018, 2018.

[8] S. Kunal, A. Saha, and R. Amin, “An overview of cloud-fog computing: Architectures, applications with security challenges,” Security and Privacy, vol. 2, no. 4, p. e72, 2019.

[9] A. Alazeb and B. Panda, “Ensuring data integrity in fog computing based health-care systems,” in International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage. Springer, 2019, pp. 63–77.

[10] S. Sagiroglu and D. Sinanc, “Big data: A review,” in 2013 international conference on collaboration technologies and systems (CTS). IEEE, 2013, pp. 42–47.

[11] F. Zafar, A. Khan, S. U. R. Malik, M. Ahmed, A. Anjum, M. I. Khan, N. Javed, M. Alam, and F. Jamil, “A survey of cloud computing data integrity schemes: Design challenges, taxonomy and future trends,” Computers & Security, vol. 65, pp. 29–49, 2017.

[12] Y. Dong, L. Sun, D. Liu, M. Feng, and T. Miao, “A survey on data integrity checking in cloud,” in 2018 1st International Cognitive Cities Conference (IC3). IEEE, 2018, pp. 109–113.

[13] K. Yang and X. Jia, “Data storage auditing service in cloud computing: challenges, methods and opportunities,” World Wide Web, vol. 15, no. 4, pp. 409–428, 2012.

[14] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, “Enabling public auditability and data dynamics for storage security in cloud computing,” IEEE transactions on parallel and distributed systems, vol. 22, no. 5, pp. 847–859, 2010.

[15] B. Shao, G. Bian, Y. Wang, S. Su, and C. Guo, “Dynamic data integrity auditing method supporting privacy protection in vehicular cloud environment,” IEEE Access, vol. 6, pp. 43 785–43 797, 2018.

[16] A. Fu, Y. Li, S. Yu, Y. Yu, and G. Zhang, “Dipor: An ida-based dynamic proof of retrievability scheme for cloud storage systems,” Journal of Network and Computer Applications, vol. 104, pp. 97–106, 2018.

[17] H. Zhao, X. Yao, X. Zheng, T. Qiu, and H. Ning, “User stateless privacypreserving tpa auditing scheme for cloud storage,” Journal of Network and Computer Applications, l. 129, pp. 62–70, 2019.

[18] J. Jeong, J. W. J. Joo, Y. Lee, and Y. Son, “Secure cloud storage service using bloom filters for the internet of things,” IEEE Access, vol. 7, pp.60 897–60 907, 2019