**REFRENCES**

[1] 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.

[2] B. Wang, B. Li, H. Li, and F. Li, “Certificate less public auditing for data integrity in the cloud,” in Proceedings IEEE Conference on Communications and Network Security (CNS), 2013, pp. 136–144.

[3] H. Shacham and B. Waters, “Compact proofs of retrievability,” in Proceedings of 14th ASIACRYPT, 2008, pp. 90–107.

[4] C. Wang, Q. Wang, K. Ren, and W. Lou, “Privacy-preserving public auditing for data storage security in cloud computing,” in Proceedings of 29th IEEE Conference on Computer Communications (INFOCOM), 2010, pp. 1–9.

[5] L. Yuchuan, F. Shaojing, X. Ming, andW. Dongsheng, “Enable data dynamics for algebraic signatures based remote data possession checking in the cloud storage,” China Communications, vol. 11, no. 11, pp. 114–124, 2014.

[6] A. F. Barsoum and M. A. Hasan, “Provable multicopy dynamic data possession in cloud computing systems,” IEEE Transactions on Information Forensics and Security, vol. 10, no. 3, pp. 485–497, 2015.

[7] C. Wang, S. S. Chow, Q. Wang, K. Ren, and W. Lou, “Privacypreserving public auditing for secure cloud storage,” IEEE Transactions on Computers, vol. 62, no. 2, pp. 362–375, 2013.

[8] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, “Provable data possession at untrusted stores,” in Proceedings of the 14th ACM conference on Computer and communications security, 2007, pp. 598–609.