secret key by itself in each time period in scheme. We compare the key update time on client side between the both schemes in Fig. 3. In scheme, the key update time on the client is related to the depth of the node corresponding to the current time period in binary tree. When the depth of node corresponding to the current time period is 0 or 1 (the node is internal node), the update time is about 12.6ms; when it is 2 (the node is leaf node), the update time is almost zero. In our scheme, the key update time on client side is zero in all time periods.

In our scheme, the communicational messages comprise the challenge message and the proof message. It is clear that the challenge message is linear with the size of blocks.

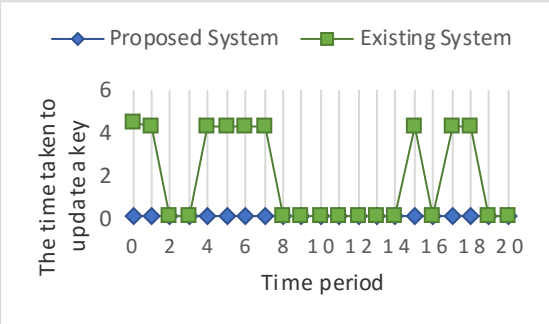

Figure 3: The key update time on client side in the proposed scheme and the existing scheme

7. Conclusion

The client's key exposure is a main problem in cloud storage auditing. Propose a new paradigm called auditing protocol with key-exposure resilience for resist the key-exposure. In such a protocol, the integrity of the data previously stored in cloud can still be verified even if the client's current secret key for cloud storage auditing is exposed.

The problem of client's secret key exposure is reduced by updating the secret key periodically. Also we can retrieve the original data even if the data is lost.

References

[1] W. Pugh. "Skip lists : a probabilistic alternative to balanced trees". Commun. ACM, 33(6):668–676, 1990.
[2] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song., "Provable data possession at untrusted stores," In CCS, pp. 598–609, 2007.
[3] D. L. Gazzoni and P. S. L. M. Barreto, "Demonstrating data possession and uncheatable data transfe," Cryptology ePrint Archive, Report 2006/150, 2006.
[4] R. C. Merkle, "Protocols for Public Key Cryptosystems," Proc. IEEE Symp. Security Privacy, 1980.
[5] Smart, N.P., Warinschi, B., "Identity based group signatures from hierarchical identity-based encryption," In: Proceedings of the 3rd International Conference Palo Alto on Pairing-Based Cryptography, Pairing '09, pp. 150–170, 2009.
[6] Wang, Q., Wang, C., Li, J., Ren, K., Lou, W.: "Enabling public verifiability and data dynamics for storage security in cloud computing.,"In: Proceedings of the 14th European conference on Research in Computer Security, ESORICS'09, pp. 355–370.
[7] Y. Zhu, G.-J. Ahn, H. Hu, S. S. Yau, H. G. An, and C.-J. Hu, "Dynamic audit services for outsourced storages in clouds," IEEE Trans. Services Comput., vol. 6, no. 2, pp. 227–238, Apr./Jun. 2013.
[8] G. Ateniese, R. Di Pietro, L. V. Mancini, and G. Tsudik, "Scalable and efficient provable data possession," in Proc. 4th Int. Conf. Secur. Privacy Commun. Netw., 2008, Art. ID 9.
[9] R. Canetti, S. Halevi, and J. Katz, "A forward-secure public-key encryption scheme," in Advances in Cryptology—EUROCRYPT. Berlin, Germany: Springer-Verlag, 2003, pp. 255–271.
[10] J. Yu, R. Hao, F. Kong, X. Cheng, J. Fan, and Y. Chen, "Forwardsecure identity-based signature: Security notions and construction," Inf. Sci., vol. 181, no. 3, pp. 648–660, 2011.
[11] A.Heitzmann, B. Palazzi, C.Papamanthou, R. Tamassia., " Efficient Integrity Checking of Untrusted Network Storage," in Proc. 14th ACM Conf. Comput. Commun. Secur., 2008.
[12] C. Erway, A. Küpçü, C. Papamanthou, and R. Tamassia, "Dynamic provable data possession," in Proc. 16th ACM Conf. Comput. Commun. Secur., 2009, pp. 213–222.
[13] Q. C. Wang, K. Ren, W. Lou, and J. Li, "Toward publicly auditable secure cloud data storage services," IEEE Netw., vol. 24, no. 4, pp. 19–24, Jul./Aug. 2010.
[14] 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.
[15] C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy preserving public auditing for secure cloud storage," IEEE Trans. Comput., vol. 62, no. 2, pp. 362–375, Feb. 2013.
[16] K. Yang and X. Jia, "An efficient and secure dynamic auditing protocol for data storage in cloud computing," IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 9, pp. 1717–1726, Sep. 2013.
[17] H. Wang, Q. Wu, B. Qin, and J. Domingo-Ferrer, "Identity-based remote data possession checking in public clouds," IET Inf. Secur., vol. 8, no. 2, pp. 114–121, Mar. 2014.
[18] J. Zhang and W. Zeng, "Self-certified Public Auditing for Data Integrity in Cloud Storage" Ninth International Conference on P2P, Parallel, Grid, Cloud and Internet Computing, Nov. 2014.

Author Profile

Niranjana S received the B. Tech degrees in Computer Science and Engineering from Kannur University in 2013 and now doing M. Tech in Computer Science and Engineering from Calicut University.