Xin WANG, Bo YANG, Zhe XIA, Hong-xia HOU, 2019. A secure data sharing scheme with cheating detection based on Chaum-Pedersen protocol for cloud storage. *Frontiers of Information Technology & Electronic Engineering*, 20(6):787-800. https://doi.org/10.1631/FITEE.1800066

A secure data sharing scheme with cheating detection based on Chaum-Pedersen protocol for cloud storage

Key words: Data sharing; Chaum-Pedersen proof; Cheating detection; Cloud storage

Contacting author: Xin WANG
E-mail: wangxin@sust.edu.cn

ORCID: http://orcid.org/0000-0003-1904-7821

Motivation

1. With the development of cloud computing technology, data can be outsourced to the cloud and conveniently shared among users.

2. In existing work, the Reed-Solomon (RS) decoding technique is often used to identify dishonest users.

3. RS decoding needs to assume that the number of malicious participants is smaller than one-third of the number of all participants.

4. The non-interactive Chaum-Pedersen zero-knowledge proof to identify every malicious participant is needed.

Main idea

1. Cloud server can assist record search using data file tags; however, it cannot learn any meaningful information about owner's data or personal sensitive information.

2. Users who can access the data file are authorized by the data owner, and they can verify the decryption keys sent by the owner. Even if some partial decryption keys from the authorized users are incorrect, the system can still properly function without affecting the reliability of data.

3. Dishonest users who present fake decryption keys can be identified in advance, without leaking the decryption keys for the honest users. Hence, the ciphertext can be safely and correctly decrypted under the supervision of these groups of users.

Method

1. To protect the owner's personal information, we use the Bloom filter to hide the information, including home address, email address, job, and age.

2. The non-interactive Chaum-Pedersen zero-knowledge proof can identify the dishonest users who have presented false keys in the reconstruction phase.

3. The advantage of the Chaum-Pedersen protocol is that it can identify every malicious participant.

Major results

1. The overload in our scheme is much less than that in Xu et al. (2018) and Dong et al. (2014), and a little more than that in Yu et al. (2010).

Dong X, Yu JD, Luo Y, et al., 2014. Achieving an effective, scalable and privacy-preserving data sharing service in cloud computing. *Comput Secur*, 42:151-164. https://doi.org/10.1016/j.cose.2013.12.002

Xu SM, Yang GM, Mu Y, et al., 2018. Secure fine-grained access control and data sharing for dynamic groups in the cloud. *IEEE Trans Inform Forens Secur*, 3(8):2101-2113. https://doi.org/10.1109/tifs.2018.2810065

Yu SC, Wang C, Ren K, et al., 2010. Achieving secure, scalable, and fine-grained data access control in cloud computing. IEEE Int Conf on Computer Communications, p.1-9. https://doi.org/10.1109/INFCOM.2010.5462174

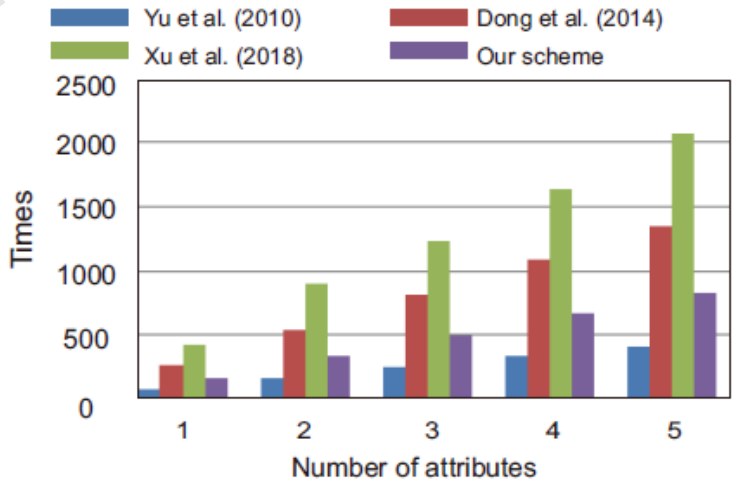

Fig. 2 Comparison of key generation performance

References to color refer to the online version of this figure

Major results (Cont'd)

2. The encryption cost linearly increases with the number of attributes in three schemes, and the proposed scheme has less cost than others.

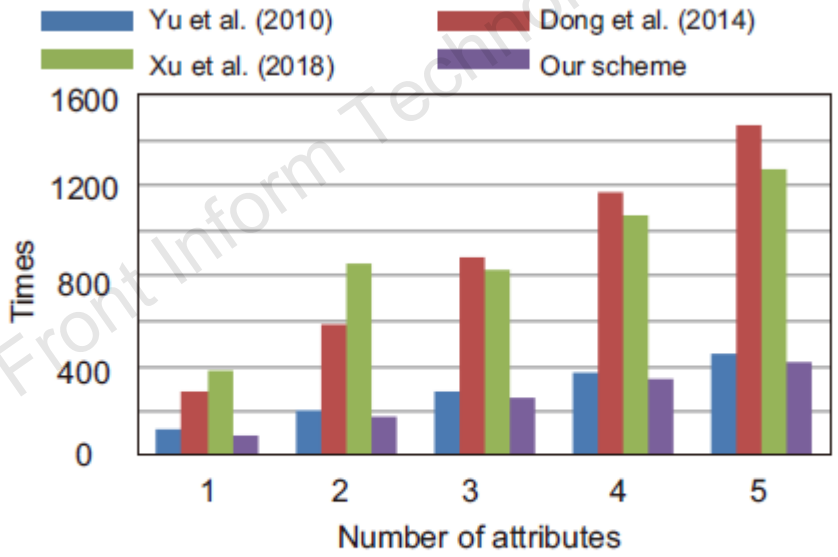

Fig. 3 Comparison of encryption performance

References to color refer to the online version of this figure

Major results (Cont'd)

3. The overhead in the proposed scheme is almost the same as that in Xu et al. (2018) and less than that in Yu et al. (2010).

Xu SM, Yang GM, Mu Y, et al., 2018. Secure fine-grained access control and data sharing for dynamic groups in the cloud. *IEEE Trans Inform Forens Secur*, 3(8):2101-2113. https://doi.org/10.1109/tifs.2018.2810065

Yu SC, Wang C, Ren K, et al., 2010. Achieving secure, scalable, and fine-grained data access control in cloud computing. IEEE Int Conf on Computer Communications, p.1-9. https://doi.org/10.1109/INFCOM.2010.5462174

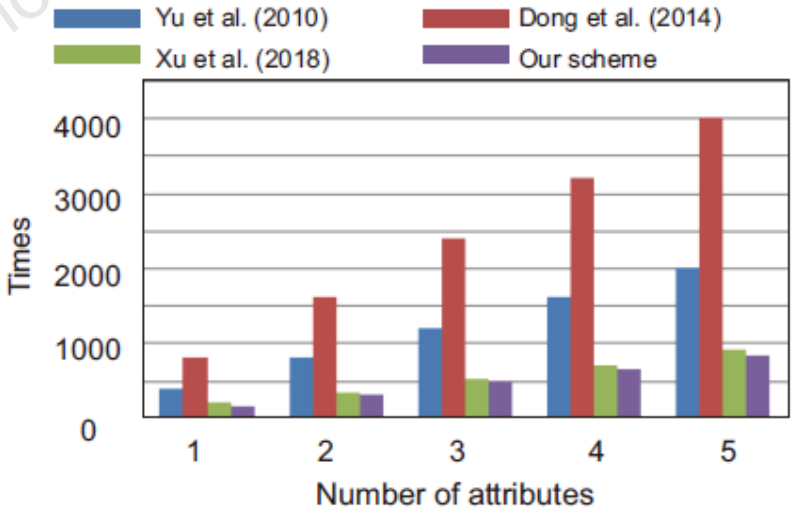

Fig. 4 Comparison of decryption performance

References to color refer to the online version of this figure

Conclusions

1. The security and reliability of the data file can be adequately protected.

2. The proposed scheme achieves cheater identification without violating the honest person's rights.

3. Our scheme can detect every dishonest user.

4. Efficiency analysis indicated that the proposed scheme has low computational cost and bandwidth usage.