# Accepted Manuscript


A remotely keyed file encryption scheme under mobile cloud computing

Li Yang, Ziyi Han, Zhengan Huang, Jianfeng Ma

PII: S1084-8045(17)30424-1

DOI: 10.1016/j.jnca.2017.12.017

Reference: YJNCA 2037

To appear in: *Journal of Network and Computer Applications*

Received Date: 2 May 2017

Revised Date: 27 September 2017

Accepted Date: 23 December 2017

Please cite this article as: Yang, L., Han, Z., Huang, Z., Ma, J., A remotely keyed file encryption scheme under mobile cloud computing, *Journal of Network and Computer Applications* (2018), doi: 10.1016/j.jnca.2017.12.017.

# A Remotely Keyed File Encryption Scheme under Mobile Cloud Computing

**Li Yang**
*School of Computer Science and Technology*
*Xidian University*
*Xi'an 710071, China*
*yangli@xidian.edu.cn*

**Ziyi Han**
*School of Computer Science and Technology*
*Xidian University*
*Xi'an 710071, China*
*nnthzy@163.com*

**Zhengan Huang**
*School of Computer Science and Educational Software*
*Guangzhou University*
*Guangzhou 510000, China*
*huangza@gmail.com*

**Jianfeng Ma**
*School of Cyber Engineering*
*Xidian University*
*Xi'an 710071, China*
*jfma@mail.xidian.edu.cn*

***Abstract*—***The storage and computing capacity limitations of a mobile terminal pare down the file sharing ability between mobile terminals and public clouds. Moreover, the security of public clouds increases perceived risks. Private clouds represent a very effective platform and can be regarded as a trusted third party for improving the level of security when a user uses a file from public clouds. Thus, we propose a new scheme called FREDP (File Remotely keyed Encryption and Data Protection). This scheme involves three-party interaction among a mobile terminal, private clouds and public clouds. The private clouds share the ciphertext file to the public clouds until the mobile terminal and the trusted third party, the private clouds, finish the encryption of the plaintext file using a remotely keyed encryption algorithm. To ensure security when a mobile terminal uses data, the private clouds as the third party regularly verify the integrity of the data in the public clouds. Finally, the mobile terminal and private clouds decrypt the ciphertext file to allow the user of the mobile terminal to use the data. In addition, we analyze the security of FREDP using BAN. The FREDP satisfies the security standard. In addition, we conduct an experiment to measure the scheme's performance. The results show that FREDP achieves good performance.*

***Keywords*—file encryption, remotely keyed encryption, data integrity, mobile cloud computing, privacy protection**

## 1. INTRODUCTION

With the significant popularity of mobile terminals[1], people have begun to prefer to use mobile terminals to access and use the Internet over traditional terminals such as personal computers[2]. Mobile terminals have many advantages; for instance, such terminals are highly portable, fast, and interactive.

Therefore, mobile terminals have become preferred for a large number of users, and application prospects are extremely broad. However, mobile terminals also have certain shortcomings. Of these shortcomings, the most serious is that their storage and computing capacities are limited[3]. Therefore, they cannot provide a large amount of storage or perform complicated calculations; they can only support certain lightweight file operations. Thus, mobile terminals prefer to export these storage-intensive and computationally complex tasks[4].

Cloud computing environments represent a good platform[5] and have substantial storage and computing resources; therefore, these tasks can be transferred to clouds[6]. Large files are stored in clouds. We can download files from clouds when using mobile terminals; as a result, we effectively save substantial amounts of space[7]. We let Private Clouds (Prc) perform complicated calculations such as encryption[8]. In general, Prc can be built based on a trusted computing platform[9]. To ensure security, the private clouds cannot know the encryption key, that is, the remotely keyed encryption process. In practical applications, we often need to share data to the Public Clouds (Puc) for the sake of reducing the pressure on local storage and improving the convenience of using data. Hence, the public clouds also need to store files. Thus, the private clouds share the ciphertext file to the public clouds. Before a mobile terminal uses the file from the public clouds, the private clouds as a trusted third party[10] verify the data integrity to ensure security. Finally, the public clouds send the ciphertext file back to the private clouds. The mobile terminal and private clouds perform remotely keyed decryption to allow the user to use the data. The interaction scenario is shown in Figure1.

Through the above interaction in our proposed scheme, FREDP, the storage and computing overhead for the mobile terminal can be greatly reduced; we transfer large amounts storage and computing tasks to the private clouds. In addition, the security of the encryption key can also simultaneously be guaranteed for the remotely keyed encryption procedure. No parties other than the user can be allowed to know the encryption/decryption key and decrypt the file. Therefore, the confidentiality of the user's file can be ensured. The privacy of the user is perfectly assured in FREDP. In addition, by sharing the encrypted file from the private clouds to the public clouds, the sharing rate of the file can be greatly improved. In particular, the remotely keyed decryption method between the mobile terminal and the private clouds can guarantee the security of the decryption key as well as the file's usage by the user. Finally, the encryption/decryption performance under FREDP is not reduced.

∗ Corresponding Author. Tel.:+86 13992822998

Email address: yangli@xidian.edu.cn (Li Yang)