Efficient Identity-Based Distributed Decryption Scheme for Electronic Personal Health Record Sharing System

ABSTRACT:

The rapid development of the Internet of Things (IoT) has led to the emergence of more and more novel applications in recent years. One of them is the e-health system,which can provide people with high-quality and convenient healthcare. Meanwhile, it is a key issue and challenge to protect theprivacy and security of the user's personal health record. Somecryptographic methods have been proposed such as encryptuser's data before sharing it. However, it is complicated toshare the data with multiple parties (doctors, health departments,etc.), due to the fact that data should be encrypted under eachrecipient's keys. Although several (t, n) threshold secret sharingschemes can share the data only need one encryption operation,there is a limitation that the decryption private key has tobe reconstructed by one party. To offset this shortcoming, in this paper, we propose an efficient identity-based distributeddecryption scheme for personal health record sharing system.It is convenient to share their data with multiple parties anddoes not require to reconstruct the decryption private key. Weprove that our scheme is secure under chosen-cipher text attack (CCA). Moreover, we implement our scheme by using the Javapairing-based cryptography (JPBC) library on a laptop and anAndroid phone. The experimental results show that our systemis practical in the electronic personal health record system.

SYSTEM REQUIREMENTS:

HARDWARE REQUIREMENTS:

- System : Pentium i3 Processor.
- Hard Disk : 500 GB.
- Monitor : 15'' LED
- Input Devices : Keyboard, Mouse
- Ram : 4 GB

SOFTWARE REQUIREMENTS:

- Operating system : Windows 10.
- Coding Language : Java
- Web Framework : Flask

REFERENCE:

Y. Zhang, D. He, M. S. Obaidat, P. Vijayakumar and K. -F. Hsiao, "Efficient Identity-Based Distributed Decryption Scheme for Electronic Personal Health Record Sharing System," in IEEE Journal on Selected Areas in Communications, vol. 39, no. 2, pp. 384-395, Feb. 2021, doi: 10.1109/JSAC.2020.3020656.