Chapter 19
Homomorphic Encryption as a Service for Outsourced Images in Mobile Cloud Computing Environment

Mouhib Ibtihal
MoulaySmail University, Morocco

El Ouadghiri Driss
MoulaySmail University, Morocco

Naanani Hassan
Ben'msik University, Morocco

ABSTRACT

The integration of cloud computing with mobile computing and internet has given birth to mobile cloud computing. This technology offers many advantages to users, like Storage capacity, Reliability, Scalability and Real time data availability. Therefore, it is s increasing fast and it is inevitably integrated into everyday life. In MCC, data processing and data storage can be migrated into the cloud servers. However, the confidentiality of images and data is most important in today's environment. In this paper, we mainly focus on secure outsourcing of images. For this purpose, we propose a secure architecture composed by two clouds a private cloud dedicated for encryption/decryption and a second public cloud dedicated for storage. We have implemented the first cloud using openstack while respecting the encryption as a service concept. As an encryption scheme, we have used paillier's homomorphic cryptosystem designed specifically for images. The test of the homomorphic property is done by applying the Watermarking algorithm DWT.

DOI: 10.4018/978-1-7998-1763-5.ch019

INTRODUCTION

Mobile cloud computing has emerged as new technology to empower the mobile computing functionality. As a combination of mobile computing and cloud computing (Buyya, Yeo, Venugopal et al., 2009; Aljawarneh, 2011). The MCC allows to mobile users an empowered the storage capacity, the reliability, scalability and real time data availability. Due to the limited storage and processing capabilities of mobile devices, many user start to save their data as videos, photos and music on clouds. The stored data in public cloud can be accessible by anyone without efficient protection mechanism. Consequently, serious question of security and trust issues has to be addressed. Even if encryption is used to protect sensitive data requires complex process to perform processing on encrypted data. Besides we cannot deny another drawback of hiding the important relationship between documents during the encryption process. In this paper, we are more interested in privacy issue of outsourced images because many images may include private information (Wang, Zhang, Ren & Roveda, 2013; Aljawarneh at el, 2015). Most of encrypted image schemes use the traditional cryptographic which does not provide secure solution to solve the images privacy problem. In this context, we propose as solution a secure architecture based on the encryption as a service concept and the homomorphic encryption. The main advantage in using homomorphic encryption is its computational ability that allows doing an arbitrary number of additions and multiplications on encrypted information without knowing decryption system where the secret key belongs only to the client. the first fully homomorphic encryption scheme was proposed in (Gentry, 2009), Others researchers proposed the variants of Gentry's model with some improvement (Smart, & Vercauteren, 2010) (Van Dijk, Gentry, Halevi, & Vaikuntanathan, 2010) (Stehlé, & Steinfeld, 2010) .There are several partially homomorphic crypto-systems like Goldwasser and Micali (Goldwasser, & Micali, 1984), ElGamal (ElGamal, 1984) and Paillier (Paillier, 1999) on the one hand Partial homomorphic encryption scheme perform one type of operation(addition or multiplication), on the other hand fully homomorphic encryption scheme use both operations. However, despite the good performance of fully homomorphic encryption, it requires a huge generated key using huge calculation number that consequently affect the calculation speed which exceeds 1000 times slower than the non-homomorphic operations. Several researches were constructed in order to improve the effectiveness of the cryptosystem in term of the consumed calculation time and the size of the keys (Naehrig, Lauter, & Vaikuntanathan, 2011). In this study, we are interested particularly by using Paillier cryptosystem because this scheme and its variants are famous for their efficiency" (Fontaine & Galand, 2007; Aljawarneh at el, 2016).

In our paper, we propose a secure architecture to resolve privacy issue for images stored in mobile cloud servers. For this we follow next steps:

1. Implementation of a private cloud using OpenStack (openstack.org) dedicated to encryption services and verified the Encryption as a service concept (Mouhib, ElOuadghiri, & ZineDine, 2016).
2. Development and implementation of a specific program on C language to encrypt/decrypt images by Paillier cryptosystem and implementation on nova hypervisor.
3. Development and implementation of a second program, also on C based on implemented discrete wavelet transform (DWT) on the encrypted domain, this program aim to test homomorphic property of our scheme.