Chapter 37
Secure Anonymous Query-Based Encryption for Data Privacy Preserving in Cloud: Moye(Ω)

Martin Konan
https://orcid.org/0000-0002-0201-5172
University of Electronic Science and Technology of China (UESTC), Chengdu, China

Wenyong Wang
University of Electronic Science and Technology of China (UESTC), Chengdu, China

ABSTRACT

Data privacy protection is a paramount issue in cloud applications for the last decade. In addition, data encryption, which is the primary method to impart security in clouds, is proved insufficient to guarantee data privacy protection from some security issues like homogeneity and background knowledge attacks. Therefore, it is important to provide a security mechanism that provide not only anonymous data but also anonymous continuous queries. So, this paper proposes a new scheme (Moye) that tackles this challenge by protecting queries to be linked to specific sensitive data. Specifically, the proposed solution is based on the design of a hybrid implementation of public key encryption with keyword search (PEKS) and subset membership encryption (SME) cryptosystem to enhance both data and query privacy protection. In addition, this approach provides an efficient and anonymous data processing by using an optimized k-anonymity scheme. Doing so, the authors protect searchable keywords and queries from inside and outside guessing attacks for the effectiveness of the proposed solution.

DOI: 10.4018/978-1-7998-8954-0.ch037

INTRODUCTION

Cloud computing seems to be the new paradigm platform where users can not only remotely store their data, but also process and share them across multiple users. However, this new service arises some challenges in terms of user identity and outsourced data privacy protection as the data owner has no more the physical control of his data according to the cloud security alliance (CSA, 2012).To illustrate this fact, the sensed body wireless data for example may contains certain sensitive information like patient identity and location, in addition to values which look innocuous (age, sex, blood group…). So the dilemma is how to securely process these sensitive information through continuous queries-based service from untrusted cloud provider? Therefore several data encryption schemes have been designed as primary method to impart security in clouds (Rene et al., 2012; Fuchun et al., 2014; Rongmao et al., 2016; Fang et al., 2013). But data encryption mainly acts as first safeguard and deals against direct data disclosures by assuring data access control, authentication, and integrity. Thereby, the encryption itself is not sufficient to protect data privacy from some specific attacks like inside and background attacks (Sweeney, 2002). Thus, there is a need to make the data fully anonymous to address data privacy issue efficiently (Sweeny, 2002). In order to achieve this data anonymity, some approaches have been proposed to securely outsource data storing and processing, using k-anonymity scheme (Yu, 2010). Despite the fact that k-anonymity is a popular method to address privacy issue, it is vulnerable to some security issues like re-identification by linking, multiple queries, homogeneity and background knowledge attacks as the data are processed in plaintext (Ashwin et al., 2007; Ninghui et al., 2007; Sweeney, 2002). In this paper, the authors propose a contribution that addresses the above mentioned weaknesses from exiting models. Researchers first design a secure scheme (Moye) that preserves the anonymity of continuous queries from being linking to a specific user or data in order to provide privacy protection. Second, the authors encrypt the data as well as the query using a hybrid cryptosystem (public key encryption with keyword search (PEKS, 2004) and subset membership encryption SME (Fuchun et al., 2014). Furthermore, authors reinforce the data privacy through a logical trusted point (TP) introduced in their previous work (Martin & Wenyong, 2015) and a trusted front-end (TFE) to address the inside attack in PEKS (Bin et al., 2012). Doing so, researchers address in the same time the re-identification by linking, multiple queries, and homogeneity attacks by encrypting the data and queries using their optimized k-anonymity scheme. In this work, authors introduce the mathematical and cryptographic tools used and briefly discuss on existing related works in section 2. Then in section 3, the researchers highlight the concrete construction and implementation of the proposed solution (Moye). The performance and security analysis of the proposed model will be done in section 4. Finally the researchers conclude this paper in section 5.

PRELIMINARIES AND RELATED WORKS

Preliminaries

Bilinear Maps and Bilinear Groups

In this section the mathematical background; bilinear maps explained (Dong, 2010) can be presented as follows: Let G and G_T be two multiplicative cyclic groups of prime order p. Let g be a generator of G and e is a bilinear map e: $G \times G \rightarrow G_T$. The bilinear map e has the following properties: