


Efficient Escrow-free CP-ABE with Constant Size Ciphertext and Secret Key for Big Data Storage in Cloud

Praveen Kumar Premkamal, National Institute of Technology Tiruchirappalli, Tiruchirappalli, India

 <https://orcid.org/0000-0003-4348-1150>

Syam Kumar Pasupuleti, Institute for Development and Research in Banking Technology, Hyderabad, India

Alphonse PJA, National Institute of Technology Tiruchirappalli, Tiruchirappalli, India

ABSTRACT

Ciphertext-policy attribute-based encryption (CP-ABE) schemes are an appropriate cryptographic technique to enable privacy along with access control in the cloud, but the existing CP-ABE schemes do not directly apply for big data because they have the issue of long ciphertext and long secret key size (LC-LS). To address LC-LS, the constant size ciphertext and secret key (CSC-S) schemes proposed. However, the existing CSC-S schemes suffer from the key escrow security issue and efficiency issue. To address both simultaneously, the authors propose an efficient escrow-free CP-ABE with constant size ciphertext and secret key (EEF-CPABE) for big data storage in the Cloud. The EEF-CPABE scheme reduces the encryption and decryption computation overhead by designing CSC-S. Further, the data owner generates the decryption global key to decrypt the data along with user secret key which solves the key escrow issue. Security and performance analysis demonstrate that the EEF-CPABE scheme resists against authority, and chosen plain-text attacks and more efficient than CSC-S schemes.

KEYWORDS

Access Control, Big Data, Cloud Computing, Constant Size Ciphertext And Secret Key, CP-ABE, Key Escrow, Privacy

INTRODUCTION

Big data has emerged as a new paradigm that gives exceptional value to the large volume of data, which indeed helps the industry, business, engineering, and science to grow (Grover, Chiang, Liang, & Zhang, 2018). On the other hand, storing and managing big data locally is a challenging task for the organizations because the organization should set up the infrastructure. Infrastructure setup in an organization is an expensive and time-consuming process. The cost effective and timely solution is outsourcing the big data into the cloud because the cloud computing offers a diversity of resources such as storage, compute, network, platform and software as services in a pay-per-use model (Hashem et al., 2015). It also supports the scalability, dynamic provisioning and de-provisioning. However, the privacy and security challenges in the cloud restrict the organizations to adopt the cloud (Takabi, Joshi, & Ahn, 2010; Gupta, Agrawal, & Yamaguchi, 2016). The foremost important issues are data privacy and access control.

DOI: 10.4018/IJCAC.2020010103

Copyright © 2020, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

Privacy can be preserved through public key encryption, but it fails to support access control. Later, Identity Based Encryption (IBE) schemes evolved to provide the access control along with encryption. However, the problem with IBE is the user's details should know before the encryption. To overcome this problem, Attribute-Based Encryption (ABE) was introduced by Sahai, and Waters (2005). Later, the variants of ABE Key Policy Attribute-Based Encryption (KP-ABE) (Goyal, Pandey, Sahai, & Waters, 2006) and the CP-ABE (Bethencourt, Sahai, & Waters, 2007) were introduced. Comparatively the CP-ABE is the best approach than KP-ABE because it allows the data owners to set control over their data.

In CP-ABE, the encrypted data is outsourced to the cloud and shared with the users based on the access policy defined. The access policy consists of attributes, which describes what attributes the user should hold. The user decryption key is generated by the authority according to her/his attributes. Later, various efforts have been taken to enhance the basic CP-ABE scheme (Deng et al., 2014; Jiang, Susilo, Mu, & Guo, 2018; Kumar, Kumar, & Alphonse, 2017; Zhang et al., 2017; Premkamal, Pasupuleti, & Alphonse, 2018; Li, Zhang, Chen, & Xiang, 2019a; Liu, Jiang, Wang, & Yiu, 2018; Premkamal, Pasupuleti, & Alphonse, 2019b). While the CP-ABE perfectly addresses the unauthorized access, the previous CP-ABE schemes do not directly deploy for practical big data applications in the cloud due to the higher computation overhead because of long ciphertext, which is proportionate to the attributes in the access policy and long secret key, which is proportionate to the number of user attributes.

To address this issue, the constant size ciphertext schemes (Attrapadung et al., 2012; Doshi & Jinwala, 2014; Teng, Yang, Xiang, Zhang, & Wang, 2017; Susilo, Yang, Guo, & Huang, 2018) were presented to reduce the computation cost, but these schemes limit the data access from resource constraint devices because of the large size secret key and decryption computation overhead. Correspondingly, the constant size secret key schemes (Guo, Mu, Susilo, Wong, & Varadharajan, 2014; Li et al., 2017) were presented to improve the data accessibility in the resource constraint devices, but it suffered from large ciphertext size which in turn increases the computation cost of encryption. To achieve both, Emura, Miyaji, Nomura, Omote, & Soshi, (2010) and Odelu et al., (2017) proposed the CSC-S schemes. However, the existing CSC-S schemes suffered with the following issues such as (1) Key escrow: The authority generates the secret key for the users to decrypt the data based on their attributes. The curious authority can decrypt the data with the generated user secret key, which indeed reduces the security. (2) Efficiency: Inefficiency in encryption and decryption computation for large universal attribute set.

To address the key escrow and efficiency problem simultaneously, the authors propose EEFCPABE scheme based on AND gate access structure. To the best of our knowledge, the proposed EEFCPABE scheme solves the key escrow problem in the CSC-S schemes for the first time. The following are the highlights of the contributions.

1. The proposed EEFCPABE scheme attains better efficiency in encryption and decryption operations by achieving constant size ciphertext and secret key.
2. The authors propose a new method to solve the key escrow problem. In the new method, the data owner generates the decryption global key during encryption in addition to the authority generated user secret key. To successfully decrypt the data both decryption global key and user secret key are required, which in turn restricts the curious authority to decrypt the data.
3. The proposed EEFCPABE scheme resists against the authority attack and chosen plain-text attack.
4. Performance analysis shows that EEFCPABE scheme effectively cuts down the computation overhead during encryption and decryption than the CSC-S schemes in the literature.

One of the possible real-life application scenarios for the EEFCPABE scheme is personal health records (PHR) in the healthcare domain. In PHR system, the patient maintains his/her health

16 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/article/efficient-escrow-free-cp-abe-with-constant-size-ciphertext-and-secret-key-for-big-data-storage-in-cloud/240693

Related Content

The Impact of National Culture Dimensions on the Adoption of Cross-Border E-Commerce: A Comparative Study

Isaac Kofi Mensah, Guohua Zeng and Chuanyong Luo (2020). *International Journal of Information Systems in the Service Sector* (pp. 91-112).

www.irma-international.org/article/the-impact-of-national-culture-dimensions-on-the-adoption-of-cross-border-e-commerce/262145

Significance of Qualitative Factors for a Deeper Understanding of Service Productivity

Sabrina Cocca (2013). *International Journal of Service Science, Management, Engineering, and Technology* (pp. 46-59).

www.irma-international.org/article/significance-of-qualitative-factors-for-a-deeper-understanding-of-service-productivity/88103

Coordination in Multi-Agent Planning with an Application in Logistics

Jeroen Valk, Mathijs de Weerd and Cees Witteveen (2005). *Intelligent Techniques for Planning* (pp. 194-224).

www.irma-international.org/chapter/coordination-multi-agent-planning-application/24463

End-User Approach to Evaluating Costs and Benefits of Smart City Applications

Mario Jadri, Tea Mija and Maja ukuši (2022). *International Journal of E-Services and Mobile Applications* (pp. 1-15).

www.irma-international.org/article/end-user-approach-to-evaluating-costs-and-benefits-of-smart-city-applications/296579

International User Interfaces

Barry Jackson (2002). *Internet Management Issues: A Global Perspective* (pp. 87-102).

www.irma-international.org/chapter/international-user-interfaces/24629