https://www.mdpi.com/1424-8220/19/7/1695

Survey on Revocation in Ciphertext-Policy Attribute-Based Encryption

Autor

Ruqayah R. Al-Dahhan 1,2,*,Qi Shi 2,*ORCID,Gyu Myoung Lee 2ORCID andKashif ,Kifayat 3

1:College of Computer and Information Technology, University of Anbar, Al-Anbar 31001 ,Iraq

2:Department of Computer Science, Liverpool John Moores University, Byrom Street, Liverpool L3 3AF, UK

3:Department of Computer Science and Engineering, Air University, Islamabad 44000 ,Pakistan

Sensors 2019, 19(7), 1695; https://doi.org/10.3390/s19071695

Received: 5 February 2019 / Revised: 30 March 2019 / Accepted: 5 April 2019/ Published: 9 April 2019

Abstract

Recently, using advanced cryptographic techniques to process, store, and share data securely in an untrusted cloud environment has drawn widespread attention from academic researchers. In particular, Ciphertext-Policy Attribute- Based Encryption (CP-ABE) is a promising, advanced type of encryption technique that resolves an open challenge to regulate fine-grained access control of sensitive data according to attributes, particularly for Internet of Things (IoT) applications. However, although this technique provides several critical functions such as data confidentiality and expressiveness, it faces some hurdles including revocation issues and lack of managing a wide range of attributes. These two issues have been highlighted by many existing studies due to their complexity which is hard to address without high computational cost affecting the resource-limited IoT devices. In this paper, unlike other survey papers, existing single and multiauthority CP-ABE schemes are reviewed with the main focus on their ability to address the revocation issues, the techniques used to manage the revocation, and comparisons among them according to a number of secure cloud storage criteria. Therefore, this is the first review paper analysing the major issues of CP-ABE in the IoT paradigm and explaining the existing approaches to addressing these issues.

Keywords: cloud computing; internet of things; Ciphertext-Policy Attribute-Based encryption; multiauthority schemes; single authority schemes; revocation.