Cluster Computing (2022) 25:167–185
https://doi.org/10.1007/s10586-021-03382-5

SHARE-ABE: an efficient and secure data sharing framework based on ciphertext-policy attribute-based encryption and Fog computing

Ahmed Saidi[1,2] · Omar Nouali[1] · Abdelouahab Amira[1,2]

Received: 30 October 2020 / Revised: 12 May 2021 / Accepted: 3 August 2021 / Published online: 12 August 2021

Abstract

Attribute-based encryption (ABE) is an access control mechanism that ensures efficient data sharing among dynamic groups of users by setting up access structures indicating who can access what. However, ABE suffers from expensive computation and privacy issues in resource-constrained environments such as IoT devices. In this paper, we present SHARE-ABE, a novel collaborative approach for preserving privacy that is built on top of Ciphertext-Policy Attribute-Based Encryption (CP-ABE). Our approach uses Fog computing to outsource the most laborious decryption operations to Fog nodes. The latter collaborate to partially decrypt the data using an original and efficient chained architecture. Additionally, our approach preserves the privacy of the access policy by introducing false attributes. Furthermore, we introduce a new construction of a collaboration attribute that allows users within the same group to combine their attributes while satisfying the access policy. Experiments and analyses of the security properties demonstrate that the proposed scheme is secure and efficient especially for resource-constrained IoT devices.

Keywords Attribute based encryption · Data sharing · Decryption outsourcing · Fog computing · Collaboration

1 Introduction

Cloud computing is a new and promising paradigm that delivers services to users over the Internet at a low cost [1]. However, this technology suffers from high data transport latency between the user and the Cloud [2]. To address this issue, Cisco introduced a new computing paradigm named Fog Computing, which brings Cloud facilities to the edge network [3], as illustrated in Fig. 1. Fog computing enhances the network performance, as it acts as an intermediate between the users and the Cloud by relocating data, computing, and networking closer to the user [4]. Fog Computing is used to offload data processing by bringing the processing near the source of data. This is more interesting when devices have limited resources like in IoT environments [5]. Besides, Fog computing is also deployed to enhance security by introducing, for example, additional firewalls to the network.

Nowadays, data sharing is essential in several domains, such as health care. For instance, whenever up-to-date and interoperable patients' data are available, the providers, patients, and caregivers can cooperate to make fully informed care decisions. Indeed, data sharing ensures that patients receive appropriate tests and medications while avoiding duplicated or conflicting ones. However, when sensitive data is outsourced to the Cloud or is processed by Fog nodes, the owner loses control over it. This can lead to the disclosure of sensitive information without the permission of these data owners [6].

To overcome this issue, Attribute-Based Encryption (ABE) was proposed by Shai and Water in [7]. It allows one to many encryptions and keeps the encrypted data confidential even when the storage server is untrusted. In ABE, descriptive strings named attributes are assigned to each user. These attributes describe the data properties, the

✉ Ahmed Saidi
a.saidi@cerist.dz

Omar Nouali
onouali@cerist.dz

Abdelouahab Amira
amira@cerist.dz

[1] Research Center for Scientific and Technical Information (CERIST), 16000 Algiers, Algeria

[2] Departement Informatique, Faculte des Sciences Exactes, Universite de Bejaia, 06000 Bejaia, Algeria