COMPUTERS & SECURITY 73 (2018) 249–265

Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

Privacy preserving fine-grained location-based access control for mobile cloud

Yaser Baseri [a,*], *Abdelhakim Hafid* [a], *Soumaya Cherkaoui* [b]

[a] *Department of Computer Science and Operations Research, Universite de Montreal, Canada*
[b] *INTERLAB Research Laboratory, Universite de Sherbrooke, Canada*

ARTICLE INFO

Article history:
Received 16 February 2017
Accepted 30 October 2017
Available online 21 November 2017

Keywords:
Location-based services
Dynamic location
Location anonymity
Attribute-based encryption
Outsourcing

ABSTRACT

Mobile cloud computing is a revolutionary computing paradigm for mobile applications, which enables storage and computation migration from mobile users to resource-rich and powerful cloud servers. This migration causes some privacy issues in providing secure data storage, fine-grained access control and anonymity of users. Attribute-based encryption is an end-to-end public key encryption mechanism that ensures security of stored data in the cloud and provides fine-grained access control using defined policies and constraints. Location of a device is one of the contextual policies, which is used to improve data security, authenticate user and provide access to services and useful information. However, unlike other policies and attributes used in attribute-based encryption, location attribute is an intrinsic dynamic attribute. In this paper, we investigate providing *Location-Based Services* (*LBSs*) for attribute-based access control in mobile cloud. More specifically, we propose a multi-authority attribute-based access control scheme to support coexistence of authorities, provide anonymity of users and protect their identity against malicious authorities. The proposed scheme uses dynamic location of mobile users as contextual information about those users, employs location range constraints as a policy in attribute-based encryption and authorizes users with dynamic locations satisfying access policies. The proposed attribute-based encryption is integrated with proxy re-encryption to (a) transform secret information received from different authorities and protect users' identities from disclosure to cloud server, and (b) outsource the computation to a cloud server with unlimited computational power. This results in achieving more efficiency and reducing the computation cost on resource-constrained mobile users.

1. Introduction

In some applications of mobile cloud, *Location-Based Services* (*LBSs*) are popular services provided by mobile devices and remote servers, in which users gain access to features (e.g. health, indoor object search, entertainment, work, personal life (Guo et al., 2008, 2012)) depending on their geographic location. *LBSs* adopt *Data as a Service* (*DaaS*) model (Hu et al., 2013); they are accessible by mobile devices, through the mobile network, and make use of the geographic positions of these devices.

In location-based services, location of a device represents one of the most important contextual information about that device and its owner; it is exploited to improve data security, and to support access to services and information provided by the cloud for mobile users. Indeed, by integrating access control mechanisms with conditions based on the physical position

* *Corresponding author.*
E-mail address: yaser.baseri@umontreal.ca (Y. Baseri).
https://doi.org/10.1016/j.cose.2017.10.014

of users, we can improve data security and immune users data against unauthorized accesses and disclosures. Furthermore, in some applications, we need this information to provide convenient services for mobile users based on their positions (e.g. social networking as an entertainment service which uses information on the geographical position of the mobile device).

The main challenge of location-based access control is the release of information only to authorized users satisfying predefined conditions; this is called fine-grain access control. In traditional access control approaches, to provide secure fine-grained access control and limit the release of information to authorized users, data owners should encrypt data for each user, which imposes high computational overhead. *Attribute-Based Encryption* (*ABE*) technique is a promising approach to achieve fine-grained access control (Goyal et al., 2006; Sahai and Waters, 2005). It provides access control over encrypted data using defined access policies and assigned set of attributes embedded in ciphertexts and secret keys. In particular, *Ciphertext Policy ABE* (*CP-ABE*) provides access such that encrypted data can be decrypted only by a user possessing a set of attributes. Thus, based on access policy embedded in ciphertext, different users are able to access different pieces of information based on the attributes they are assigned. Since *ABE* encrypts data without exact knowledge of receivers, it is suitable for large-scale systems.

Providing fine-grained access control for attribute-based encryption requires issuing different attributes for each user. Since each authority issues a bunch of attributes for each user, the employed *ABE* (*CP-ABE*) should support coexistence of multiple authorities. *Multi-Authority ABE* (*MA-ABE*) (Jiang et al., 2016; Jung et al., 2015; Lewko and Waters, 2011; Li et al., 2016; Yang and Jia, 2014) is more appropriate for location-based access control for cloud, as users hold attributes issued by different authorities. Moreover, in *MA-ABE*, instead of issuing a secret key by a single authority, each authority issues part of the key corresponding to a bunch of attributes it is responsible for. Hence, it can protect identity and provide anonymity of users.

Using *MA-ABE* in the context of *LBSs* introduces several challenges including (1) location anonymity: mobile users should not be traceable while using *LBSs*; (2) dynamic location update: locations of mobile users change over time; *MA-ABE* should support the dynamic update of location and key related to that location attribute; and (3) computational overhead on mobile devices (users): the execution of the scheme should not impose high computation cost on mobile users with limited resources.

1.1. Contributions

In this paper, aiming to address the above challenges, we propose a new *Privacy Preserving Location-Based Access Control* (*PPLBAC*) scheme for mobile clouds. The proposed *PPLBAC* provides the following properties:

- Confidentiality of stored data: We propose a fine-grained access control mechanism which provides access to encrypted data for authorized users satisfying predefined *static* and *dynamic* conditions.
- User anonymity protection against authorities: The proposed *PPLBAC* exploits secret sharing mechanism to share secret between authorities and provides a novel approach to support coexistence of multiple authorities, protect the identity of users against each authority and reduce the computation overhead on resource-constrained mobile users.
- *Dynamic* location updating of mobile users: Since the location is an attribute which should be dynamically updated, each time the location of a mobile user changes, the entire secret key of that user must be changed. Hence, we propose an efficient location updating method for mobile users without changing their entire secret keys.
- Location privacy for mobile users: To provide location privacy, we incorporate *MA-ABE* with comparative attribute-based encryption (Wang et al., 2015)[1] and proxy re-encryption to (a) simultaneously support location constraint (modeled as range policies) as well as other constraints (modeled as regular policies) in *MA-ABE*, and (b) transform secret information received from authorities such that cloud server would not be able to recognize users and their locations (even if all authorities collaborate).
- Low computational overhead on mobile users: Due to computation overhead, imposed by pairing operations in the decryption, *ABE* is not suitable for mobile cloud. To solve this problem, the proposed *PPLBAC* integrates *MA-ABE* with proxy re-encryption (Lai et al., 2013; Tysowski and Hasan, 2013) and offline big data processing mechanism (Fernandez et al., 2015; Rathore et al., 2015) and provides a new method to (a) outsource costly computational pairing operations in the decryption of *MA-ABE* to cloud server, (b) perform (offline just one time) the static part of computations at registration time and (c) perform the dynamic part of computations at access time.

To the best of our knowledge, this is the first work suitable for dynamic location-based access control in mobile cloud to achieve multi-authority and fine-grained access control, provide dynamic anonymous and unforgeable location and support confidentiality of users without imposing significant computational overhead on mobile devices. We also formally define and prove selective security of the proposed *PPLBAC* against chosen plaintext attacks. Finally, we evaluate *PPLBAC* to show its feasibility for location-based access control in mobile cloud.

1.2. Organization

The remainder of this paper is organized as follows. Section 2 presents the literature review related to our work. Section 3 presents some preliminaries. Section 4 discusses the system and security models. Section 5 describes the proposed scheme. Section 6 analyzes the security of the proposed *PPLBAC* and Section 7 evaluates its performance. Finally, Section 8 concludes the whole paper.

[1] The Boolean formulas that Wang et al. (2015) support has more restrictive format (conjunctions of atomic formulas). Furthermore, it cannot support range attributes and regular attributes simultaneously.