Ad Hoc Networks 35 (2015) 51–64

Contents lists available at ScienceDirect

Ad Hoc Networks

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

A trustworthy access control model for mobile cloud computing based on reputation and mechanism design

Hui Lin*, Li Xu, Xinyi Huang, Wei Wu, Yijie Huang

Fujian Provincial Key Laboratory of Network Security and Cryptology, School of Mathematics and Computer Science, Fujian Normal University, Fuzhou, China

ARTICLE INFO

Article history:
Received 16 December 2014
Revised 19 May 2015
Accepted 10 July 2015
Available online 17 July 2015

Keywords:
Big data
Mobile cloud computing
Access control
Reputation
Mechanism design

ABSTRACT

Mobile cloud computing (MCC) is an emerging technology that has gained ever-increasing popularity, which makes the generation and large-scale collection of private personal data possible. However, new security issues arise when MCC offers big data analytics and management services. In particular, there is an absence of fine-grained secure access control model to protect privacy information from unauthorized access, especially launched by internal malicious nodes with legal identity and authority. To fill the gap, this paper proposes a reputation and mechanism design based trustworthy access control model (RMTAC) to provide secure and privacy-aware big data access control in MCC. The RMTAC integrates the access control scheme with Vickrey–Clark–Groves (VCG) based adaptive reputation mechanism (VARM), the distributed multi-level security scheme and the hierarchical key management protocol to provide secure and privacy-aware access control and defend against the internal attacks. Simulation results demonstrate the superior performance of the VARM in terms of utility, effective recommendation rate, and accuracy rate compared to the existing reputation mechanisms. Moreover, the RMTAC shows better performance in terms of success rate of malicious access and successful acceptance rate compared to the role-based encryption access control model (RBE) mechanism, in the presence of collusion attacks, bad mouthing attacks and information disclosure attacks.

1. Introduction

Mobile cloud computing (MCC) is a new computing paradigm that combines cloud computing with mobile devices and ubiquitous wireless infrastructure [1,2]. MCC has wide applications in different areas [3] such as entertainment, health, games, business, and social networking and may generate and collect large amounts of data. With the rapid development and proliferation of MCC, new challenges arise when MCC offers big data analytics and management services [4,5]. In particular, data security and privacy have been the major concerns [5,6].

MCC mobile clients such as smartphones and tablets are able to acquire and produce various types of information in wireless environment, e.g., individuals' location and phone call logs [7]. However, MCC lacks fine-grained secure access control model to protect data and information from unauthorized access, especially launched by internal malicious nodes with legal identity and authority [1,2,8]. Traditional access control models such as role based access control (RBAC), attribute based access control (ABAC) and context-aware RBAC (C-RBAC) models [6] have been shown to be capable of detecting and preventing unauthorized access effectively for traditional networks. But they cannot provide effective and practical solutions to security problems in MCC, e.g., access from unknown users, privacy protection, unauthorized access from internal malicious nodes and information leaks using legitimate access method [6]. Therefore, there

* Corresponding author. Tel./fax: +86 59183465220.
E-mail address: linhui@fjnu.edu.cn (H. Lin).

http://dx.doi.org/10.1016/j.adhoc.2015.07.007
1570-8705/© 2015 Elsevier B.V. All rights reserved.

is an urgent need for a new secure access control model to address above-mentioned limitations of existing methods by taking in account the characteristics of MCC [6,9].

In MCC, service providers such as mobile clients or cloud servers offer the data and information access based on the prior knowledge they possess about the visitor and also on the sensitivity of the data and information [9]. To design a new access control model that quantifies the prior knowledge and shares the data and information based on this knowledge, it is necessary to analyze the trustworthiness of the relationship between the visitor and provider [7]. As a result, trust based access control has been introduced into MCC to implement secure access, management and the use of data.

Although a number of trust based access control models have been proposed in the literature [5–15], most of them were based on the trusted third party and traditional cryptographic encryption and authentication techniques, thus ignoring internal attacks launched by an inside attacker that has the legal identity and dishonest recommendations used to frame up good parties and/or boost trust values of malicious peers. Moreover, they did not take into account privacy preserving, information leak, and hierarchical fine-grained secure access control [9].

To overcome the above-mentioned problems, we introduce a reputation mechanism as a key scheme and an effective approach to characterize and quantify nodes' trust, and propose a reputation and mechanism design based trustworthy access control model (RMTAC) in this paper. To the best of our knowledge, the RMTAC is the first secure access control model in MCC integrating the reputation evaluation model with mechanism design and distributed multi-level security scheme to defend against internal collusion attacks, bad mouthing attacks and information disclosure attacks. The major contributions of this work include:

(1) The RMTAC integrates the Vickrey–Clark–Groves (VCG) based adaptive reputation mechanism (VARM), a distributed multi-level security scheme and a hierarchical key management protocol. The combination of these parts can effectively implement the fine-grained secure access control and privacy protection in MCC.
(2) The VARM can adaptively adjust the initial reputation value of an unknown user according to the actual network status, effectively incent users to provide honest recommendation, and thus improve the accuracy and credibility of the reputation evaluation, and the effectiveness of the reputation mechanism. Meanwhile, the proposed distributed multi-level security scheme and hierarchical key management protocol overcome the drawbacks of the centralized security mechanism that needs a trusted third party.
(3) Extensive OPNET simulation experiments demonstrate that the VARM improves the effectiveness of the reputation mechanism compared to the existing RP-CRM (reliable recommendation and privacy preserving based cross-layer reputation mechanism) and FSLR (familiarity and subjective logic based reputation model) mechanisms, and the RMTAC outperforms the existing role-based encryption access control model (RBE) in the presence of collusion attacks, bad mouthing attacks and information disclosure attacks.

The remainder of this paper is organized as follows. Section 2 presents a brief review of the related work; Section 3 describes the network and adversary models; Section 4 introduces the details of the implementation of RMTAC; Section 5 presents the costs analysis and experimental evaluation of the VARM and RMTAC; finally, Section 6 concludes the paper and discusses some future work.

2. Related work

Trust based secure access control mechanisms have been widely studied in cloud computing and MCC to support secure and trustworthy big data access, communications and enhance collaborations among participants.

Choi et al. [6] presented an ontology-based access control model (Onto-ACM) to address the difference in the permitted access control between service providers and users in cloud computing environments. Onto-ACM integrated the ontology reasoning scheme with the semantic analysis method to implement intelligent context-aware access to different cloud computing services differentiated according to security policies. Vidyalakshmi et al. [9] presented a manageable and flexible access control model for smartphones based on trust. The proposed model firstly grouped similar files into categories that are virtual containers. Then, it proposed a way of computing trust values using weights assigned to categories and contexts. Last, with the computed trust value, the access to the categories was controlled. Yu et al. [10] proposed a secure and scalable fine-grained data access control scheme. The proposed scheme combined the attributes based public key encryption scheme KP-ABE with proxy re-encryption and lazy re-encryption to achieve fine-grainedness, data confidentiality, and scalability simultaneously for cloud computing. Zhou et al. [11,12] proposed a role-based encryption access control model (RBE) to enforce access policies on encrypted data and protect data privacy in a cloud storage system. The RBE used cryptographic techniques to allow the owner of the data to encrypt the data to a specific role, so that only the authorized users in this role or the predecessors of this role can decrypt. Xhafa et al. [13] proposed a PHR service system to implement the fine-grained access control to PHR data in hybrid cloud. In PHR, anonymous attribute-based encryption technique is deployed to encrypt a symmetric key which is then used to encrypt the PHR files to achieve secure and fine-grained access control and user privacy protection. Hur et al. [14] presented an attribute based data sharing scheme to enforce a fine-grained data access control for cloud computing. The proposed scheme generated the user secret keys through a secure two-party computation to enhance data privacy and confidentiality, and used an immediate user revocation scheme to achieve more secure and fine-grained data access control. Wu et al. [15] presented a multi-message cipher-text policy attribute-based encryption (MCP-ABE) based access control mechanism. The mechanism implements the secure access control by allowing a content provider to specify an access policy and encrypt multiple messages within one