Computer Communications 68 (2015) 61–72

Contents lists available at ScienceDirect

Computer Communications

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

Robust access control framework for mobile cloud computing network

Fei Li [a], Yogachandran Rahulamathavan [a,*], Mauro Conti [b], Muttukrishnan Rajarajan [a]

[a] School of Engineering and Mathematical Science, City University London, London, United Kingdom
[b] Department of Mathematics, University of Padova, Padova, Italy

ARTICLE INFO

Article history:
Available online 11 July 2015

Keywords:
Access control
Smart devices
Attributes
Encryption
Cloud computing

ABSTRACT

Unified communications has enabled seamless data sharing between multiple devices running on various platforms. Traditionally, organizations use local servers to store data and employees access the data using desktops with predefined security policies. In the era of unified communications, employees exploit the advantages of smart devices and 4G wireless technology to access the data from anywhere and anytime. Security protocols such as access control designed for traditional setup are not sufficient when integrating mobile devices with organization's internal network. Within this context, we exploit the features of smart devices to enhance the security of the traditional access control technique. Dynamic attributes in smart devices such as unlock failures, application usage, location and proximity of devices can be used to determine the risk level of an end-user. In this paper, we seamlessly incorporate the dynamic attributes to the conventional access control scheme. Inclusion of dynamic attributes provides an additional layer of security to the conventional access control. We demonstrate that the efficiency of the proposed algorithm is comparable to the efficiency of the conventional schemes.

1. Introduction

Nowadays organizations demand a host of tools, including desktop and smart devices, email, instant messaging, voice mail, presence information and audio, video and web conferencing. When these tools are integrated into a system that allows seamless data sharing among devices then it's called unified communications network. Integrating smart devices within traditional network increases productivity among employees as well as new security vulnerabilities. Traditionally, organizations store data in local servers while employees access the data using access control techniques. However, the recent trend towards cloud computing, outsourcing, smart devices or Bring-Your-Own-Devices (BYOD), and high bandwidth mobile broadband has enabled organizations to share information anywhere and anytime. Data could be shared using public data storages such as cloud computing infrastructure which can provide flexible computing capabilities, reduced costs and capital expenditures and charge based on to usage.

In particular, BYOD became a hot topic after the 2012's Cisco survey which has found that 95% of the employees are allowed to use their mobile devices within their organizations [14]. Since then the number users use their personnel device for work has increased exponentially across the globe [15,16]. This trend is against the tradition where employees are allocated with company devices embedded with specific softwares and policies to achieve security. Currently researchers are focusing on developing techniques to securely virtualize the user device hence the corporate data will be protected from data breaches [41,42]. Samsung and BlackBerry use technologies called KNOX, and BES12, respectively to enforce the corporate security policies on user's device [29,30].

This trend requires new ways to control the access of data stored in cloud. Traditionally, we assume that data owners, users, and storage server are in the same domain and also that the server is fully trusted [1–9]. However, in BYOD, cloud computing and outsourcing environments, data confidentiality is not guaranteed since the data is stored and processed within the third party environment. Personnel information of the data owners and commercial interests of users can be leaked to third party if the data owners store decrypted data in public servers. To overcome this challenge, the data confidentiality in a distributed environment is achieved via attribute based encryption (ABE) technique [10–13].

ABE is considered as a promising cryptographic technique and supports both the data confidentiality and access control simultaneously [10–13]. Using ABE, the data owners can encrypt the data using fine-grained access policies. For instance, let us assume, an employer uploads encrypted file to the cloud using ABE, where access policy of that file is defined using the following attributes and functions AND and OR: "Manager" OR "Finance Office" AND "Company A". Hence, an

* Corresponding author. Tel.: +44 0207040 8377; fax: +44 0207040 8566.
E-mail addresses: fei.li.1@city.ac.uk (F. Li), yogachandran.rahulamathavan.1@city.ac.uk (Y. Rahulamathavan), conti@math.unipd.it (M. Conti), R.Muttukrishnan@city.ac.uk (M. Rajarajan).

http://dx.doi.org/10.1016/j.comcom.2015.07.005
0140-3664/

employee who is a "Manager" employed at "Company A" can decrypt the file. There are two major types of ABE schemes: single authority based ABE [11] and multiple authorities based ABE (MA-ABE) [32] schemes. In a single authority based ABE scheme, only one authority called attribute authority (AA) is responsible for monitoring all the attributes. In MA-ABE, in contrast to the single authority ABE scheme, there are multiple attribute authorities responsible for a disjoint sets of attributes.

When it comes to BYOD, the ABE cannot directly be used to protect the data due to the user's mobility. It should be noted that the data confidentiality in the ABE schemes relies only on predefined static attributes such "Manager", "Finance Office", and "Company A". Let us consider the previous example, where an employee has the long term credentials for the following attributes: "Manager", and "Company A". Hence, she can access the encrypted file while she is traveling in public transport using her personnel mobile device. However, the risk level associated in this context is high. In fact, people in her proximity might easily see confidential data via shoulder surfing. It is also possible for an adversary to steal the employee's mobile device, and get unauthorized access to the corporate data if there is no real-time verification (assuming that the credentials for static attributes are stored within mobile). Hence, evaluating the data collected by smart device's sensors in real-time provides additional layer of security. In particular smart device attributes such as location, app usage patterns, unlock failures, Wi-Fi networks and proximity of devices could be exploited for real-time verification. We refer the attributes collected via smart devices as dynamic attributes since they change every time with the user's mobility.

In this paper, we propose a new algorithm which supports the organizations to incorporate dynamic attributes within the ABE scheme for robust access control. The novelty of our algorithm are listed below:

1. New algorithm enforces the dynamic attributes to the conventional ABE scheme.
2. New algorithm does not compromise the security of the conventional ABE scheme.
3. New algorithm supports both the single authority and multi authority schemes.
4. Performance of the new algorithm is comparable with the conventional ABE scheme.

The reminder of this paper is organized as follows: we review related works in Section 2. We describe the system architecture and various types of attacks in Section 3. In Section 4, we propose the static and dynamic ABE scheme for single authority scheme followed by a MA-ABE scheme in Section 5. We compare the performance of the proposed schemes against the conventional ABE schemes in Section 6. Section 7 is dedicated for analyzing the security and privacy issues of the proposed schemes. Conclusions, limitations and future works are discussed in Section 8.

2. Related work

Access control is a classical security issue. Various access control models have been proposed in literature. In 1996, Sandhu et. al proposed the feasible access control model called role-based access control (RBAC) [1]. It simplifies authorization and administration because a security administrator needs only to revoke and assign the new appropriate role memberships if a user changes her job function. Various improved RBAC models have been proposed and been widely used in practice. Zhang and Parashar extended the RBAC model to support context information called context-aware dynamic access control scheme [2]. In [2], a user is assigned with access credentials based on her roles (i.e., a set of attributes) and context information. The resource maintains a set of roles and assign a potential role with certain permissions to the user.

Similar works have been proposed based on temporal condition called a temporal RBAC in [4] and based on wider range of event and environmental conditions called event-based RBAC in [3]. In [3,4], the event was defined as measurable, dynamic context variables that can influence access decisions besides the location and time variables. In [17], both the spatial and temporal attributes were exploited to support patient-centric access control scheme in e-healthcare. All these works successfully extend the RBAC model to enforce the context information for access control. However, the central architecture of RBAC is not suitable for today's mobile environment since the data and users are not restricted to be in the same environment i.e., outsourcing the data to cloud and usage of smart devices.

Mobile RBAC system which enforces spatially-aware (location) RBAC policies is proposed in [6]. In [6], an object is equipped with a near field communication (NFC) receiver and the user has an NFC enabled handset. Thus, the users can access certain resources by exchanging credentials using NFC protocols. The NFC receiver verifies the location of the user, but also restrains the range of the implementation since the user has to access the resource by going to an access point.

Hasen and Oleshchuk presented an extended version of RBAC model for mobile systems [5]. They extended the RBAC model by introducing the notion of environmental roles in order to control permission sets by activation and/or deactivation of roles based on spatial information. The main difference in their work with others' is that the availability of permission sets depend on spatial information within the same active role. Permissions are dynamically assigned to the role dependent on location. Thus, it reduces the number of roles that needs to be specified within the system.

In [7], the authors presented a more complex location-aware RBAC model. There are two kinds of associations roles are possible with locations: the role can only be assigned to a user when he is in certain designated locations and some roles can only be activated in some specific locations. Both of the works in [5,7] incorporate the spatial-temporal information in the RBAC model, but they do not consider other important contextual attributes which are important in today's mobile environment.

It should be noted that the works discussed so far have not focused on the data confidentiality. These works assumed that the storage server is secure, hence the data stored in the server is not encrypted. As said in the introduction, these traditional access control techniques are not suitable for the current unified communications network. Let us now discuss the existing access control techniques where the data is stored in the encrypted format.

Hsien-Chou and Yun-Hsiang proposed a location-based data encryption technique using static locations [19]. In this work, each static location contains pre-determined longitude and latitude coordinates. The concept of "geoencryption" or "location-based encryption" was developed to use in digital film distribution by Scott and Denning [18]. Al-Ibrahim et al. presented a geoencryption protocol by restricting the decryption of a message to a particular location and time period [20]. The encryption in this work is similar to [19] where the locations were static which means those are pre-defined in the system.

Vijayalakshmi and Palanivelu proposed a secure localization using elliptic curve cryptography (ECC) in wireless sensor networks, where determining the physical positions of sensors is a fundamental and crucial problem for the wireless sensor network operation [21]. In [21], the location based authentication scheme was built based on the identity-based cryptography using ECC and ECC key exchange. Karimi and Kalantari [22] presented a geoencryption protocol which allows the mobile nodes to communicate with each other by restriction when decoding a message in the specific location and time period. Similar technique was applied for mobile devices in [23].

In [8], an access control framework is proposed using IEEE 802.11 protocol, whereby the access to a wireless local area network (WLAN)