Computers and Electrical Engineering 000 (2016) 1–12

Contents lists available at ScienceDirect

Computers and Electrical Engineering

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

Achieving reliable and secure services in cloud computing environments

Qin Liu[a], Guojun Wang[b,*], Xuhui Liu[a], Tao Peng[c], Jie Wu[d]

[a] College of Computer Science and Electronic Engineering, Hunan University, Changsha, Hunan Province, 410082, PR China
[b] School of Computer Science and Educational Software, Guangzhou University, Guangzhou, Guangdong Province, 510006, PR China
[c] School of Information Science and Engineering, Central South University, Changsha, Hunan Province, 410083, P R China
[d] Department of Computer and Information Sciences, Temple University, Philadelphia, PA 19122, USA

ARTICLE INFO

Article history:
Received 21 April 2016
Revised 7 October 2016
Accepted 7 October 2016
Available online xxx

Keywords:
Cloud computing
Reliability
Security
Comprehensive transmission model
Two-phase resource sharing protocol

ABSTRACT

In cloud computing environments, resources stored on the cloud servers are transmitted in the form of data flow to the clients via networks. Due to the real-time and ubiquitous requirements of cloud computing services, how to design a sophisticated transmission model to ensure service reliability and security becomes a key problem. In this paper, we first propose a Comprehensive Transmission (CT) model, by combining the Client/Server (C/S) mode and the Peer-to-Peer (P2P) mode for reliable data transmission. Then, we design a Two-Phase Resource Sharing (TPRS) protocol, which mainly consists of a pre-filtering phase and a verification phase, to *efficiently* and *privately* achieve *authorized resource sharing* in the CT model. Extensive experiments have been conducted on the synthetic data set to verify the feasibility of our protocol.

1. Introduction

Cloud computing as a promising computing paradigm, allows users to enjoy user-controlled services transparently and seamlessly. In cloud computing, everything is a service (XaaS). That is, computer resources (e.g., hardware, software, and data) are delivered as services that can be subscribed and unsubscribed by customers over the Internet in a pay-as-you-go fashion. In the NIST cloud definition framework [1], cloud computing offers three kinds of service models, i.e., Software as a Service (SaaS) that allows the cloud customers to control only application configurations, Platform as a Service (PaaS) that allows the cloud customers to control the hosting environments, and Infrastructure as a Service (IaaS) that allows the cloud customers to control everything except the hardware infrastructure.

Fig. 1 shows a typical cloud computing environment, where all of the resources stored on the cloud servers will be transmitted in the form of data flow to the clients. The users can access any desired resources on demand, anytime and anywhere, using various kinds of devices connected to the Internet. Cloud computing, as an evolved paradigm of distributed computing, parallel computing, grid computing, and utility computing, has a lot of merits such as fast deployment, pay-for-use, high availability, high scalability, rapid elasticity, low costs, and so on. However, its unique features bring new challenges to service reliability [2,3].

* Corresponding author.
E-mail address: csgjwang@gmail.com (G. Wang).

http://dx.doi.org/10.1016/j.compeleceng.2016.10.005
0045-7906/

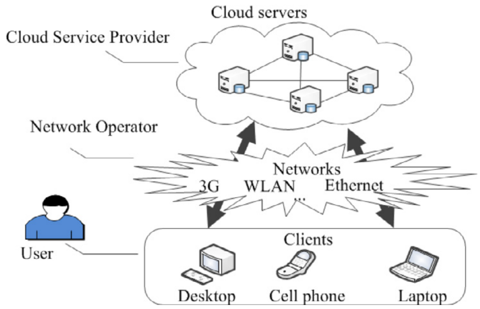

Fig. 1. A typical cloud environment. The clients held by the user are network-connected devices such as cell phones and laptops; the cloud servers maintained by the Cloud Service Provider (CSP) are regular personal computers; and the networks managed by the Network Operator support various kinds of network access methods, e.g., WLAN, 4G, etc.

First of all, cloud computing requires high real-time services. In cloud computing environments, resources are dynamically scheduled over networks in a block-streaming way. The delay or lack of a single block during data transmission will cause the failure of the service delivery. Secondly, cloud computing requires ubiquitous services. The users are promised to enjoy services at anytime and at any place using any type of device. In certain circumstances, the time delay for data transmission between the cloud servers and the clients may be intolerant. Such examples include the cloud servers becoming overloaded or the clients having low-speed Internet access. To ensure the quality of the service, an alternative solution is to establish a peer-to-peer connection between nearby clients for direct data transferring.

In this paper, we propose a Comprehensive Transmission (CT) model to ensure service reliability in cloud environments. The CT model, which combines the Client/Server (C/S) mode and the Peer-to-Peer (P2P) mode for data transmission, allows the clients to access resources from the cloud servers in the C/S mode or other clients in the P2P mode. The CT model makes full use of the advantages of both modes: On one hand, the centralized resource management in C/S mode is in favor of access control and system security; On the other hand, P2P resource sharing can reduce the workload on the cloud servers, which mitigates the risk of a single point of failure [4–6].

However, different users have different access rights for various resources in cloud computing environments. Although the C/S mode can easily achieve fine-grained access control under the cloud servers' centralized control, *efficiently* and *privately* achieving *authorized resource sharing* in the P2P mode becomes a problem. For efficiency, we should ensure that a client can quickly find appropriate resources. For privacy, we should protect the privacy of a client while searching resources (i.e., which resources it is authorized to access). For authorized resource sharing, we should ensure that a client can access resources only after obtaining authorization from the cloud servers.

To this end, we design a Two-Phase Resource Sharing (TPRS) protocol, which mainly consists of a pre-filtering phase and a verification phase. In the TPRS protocol, the clients are further classified as *requesters* and *providers* for certain resources. The pre-filtering phase applies the Secure Dot-Product (SDP) protocol [7] to let a requester *efficiently* and *privately* find *candidate* providers. Then, the verification phase applies the Fuzzy Vault (FV) [8] and Attribute-Based Encryption (ABE) [9] techniques to let each party *privately* verify the authenticity of the results in the pre-filtering phase for authorized resource sharing. The main contributions of our work are as follows:

- To achieve reliable and secure services in cloud computing environments, we propose a CT model by combining the C/S mode and the P2P mode for data transmission.
- We are among the first to consider the problem of efficient, private, and authorized resource sharing in cloud computing environments. We design a TPRS protocol, which consists of a pre-filtering phase and a verification phase.
- Extensive experiments have been conducted on the synthetic data set to verify the feasibility and effectiveness of the proposed protocol.

Paper organization. We provide our models and definitions in Section 2 before introducing technique preliminaries in Section 3. We present the pre-filtering phase in Section 4 before illustrating the verification phase in Section 5. Then, we analyze the security of the proposed protocol in Section 6. After providing an evaluation in Section 7, we introduce related works in Section 8. Finally, we conclude this paper in Section 9.

2. Models and definitions

2.1. Comprehensive transmission model

The CT model mainly consists of two kinds of entities: the cloud servers and the clients, as shown in Fig. 2. In the CT model, we mainly consider wireless networks, where many Access Points (APs) are deployed for data transmission. We assume that the clients close to an AP form a *group*.