Chapter 38
Privacy Preservation Based on Separation Sensitive Attributes for Cloud Computing

Feng Xu
Nanjing University of Aeronautics and Astronautics, Collaborative Innovation Center of Novel Software Technology and Industrialization, Nanjing, China

Mingming Su
College of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing, China

Yating Hou
College of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing, China

ABSTRACT

The Cloud computing paradigm can improve the efficiency of distributed computing by sharing resources and data over the Internet. However, the security levels of nodes (or severs) are not the same, thus, sensitive tasks and personal data may be scheduled (or shared) to some unsafe nodes, which can lead to privacy leakage. Traditional privacy preservation technologies focus on the protection of data release and process of communication, but lack protection against disposing sensitive tasks to untrusted computing nodes. Therefore, this article put forwards a protocol based on task-transformation, by which tasks will be transformed into another form in the task manager before they can be scheduled to other nodes. The article describes a privacy preservation algorithm based on separation sensitive attributes from values (SSAV) to realize the task-transformation function. This algorithm separates sensitive attributes in the tasks from their values, which make the malicious nodes cannot comprehend the real meaning of the values even they get the transformed tasks. Analysis and simulation results show that the authors' algorithm is more effective.

DOI: 10.4018/978-1-7998-8954-0.ch038

1. INTRODUCTION

Cloud computing has emerged as an important computing field. It has an innovative Information System (IS) architecture, distinguished from conventional distributed computing, by its focus on virtualized and scalable resources sharing, innovative applications, and, in some cases, high-performance computing orientation (Zissis & Lekkas, 2012; Srinivasamurthy, Liu, Vasilakos, & Xiong, 2013). It can offer many benefits or advantages (Subashini & Kavitha, 2011), like lower costs, fast deployment, pay-for-use, ubiquitous network access, etc. Therefore, the cloud computing technology has been one of the most promising technologies in computing today, and it has been widely used in the Internet. The cloud computing offers some services for processing user data on machines that he does not control and, even more, does not operate. However, because of the computing nodes, which participate in the collaborative distributed computing have the heterogeneous and isolated characteristics, they may trust each other or also may mutual distrust, and even compete with each other. Those dishonest, malicious nodes are motivated to get private information from other nodes and cause loss of some users.

There are many researches about the privacy protection technology in cloud computing. These works mainly focus authentication, authorization, data encryption, resources protection and secure communication (Kaneda, Taura, & Yonezawa, 2003), which can handle the general security problems in cloud computing well. However, it cannot be guaranteed that all the nodes are secure and credible when they disposing sensitive task together. That will probably make malicious nodes gain private information of some other nodes. The reason is that the "honest" nodes, which had passed system verification, have the possibility of view, record and use the private information of other nodes when processing them.

The main contributions of this paper are as follows:

1. We make the first attempt to discuss privacy protection issue for sensitive tasks in cloud computing;
2. In to protect sensitive tasks against leaking information, we present a protocol based on task-transformation. Then we propose a general privacy preservation model based on the protocol, by which we transform sensitive tasks into another form in the Task Manager before scheduling them to nodes;
3. We put forwards a privacy preservation algorithm based on Separation Sensitive Attributes from Values (SSAV) to realize the task-transformation function.

The remainder of this paper is organized as follows. In section 2, the research background is introduced; in the section 3 we present a privacy preservation protocol based on task-transformation; we gives a new privacy preservation algorithm in the section 4; in section 5 we do some simulation experiments and results prove the availability of the new algorithm; finally, in section 6 we give the conclusion and point out the problems which should be resolved in further research.

2. RELATED WORK

In this chapter, we review privacy preservation technologies, especially privacy preservation in cloud computing. These privacy preservation technologies can generally be classified as one of two types: general privacy preservation or privacy preservation in the cloud environment.