2016 9th International Symposium on Computational Intelligence and Design

# A Privacy Filtering and Processing Model in Cloud Computing

Linbo Tao[1], Jianjing Shen[1], Bo Liu[2], Xiaofeng Guo[1]
1.School of Arts and sciences, Information Engineering University, Zhengzhou, China
2.Shenyang Nanchang High School,Shenyang, China
E-mail:taotlb@126.com

***Abstract*—Privacy protection in cloud computing environment has become the key to the rapid development of cloud computing, until now more researches have being placed on preserving methods of privacy, but less on filtering and preserving them efficiently. A two-stages filtering model is designed in this paper to solve the problem. The privacy filtering and processing methods are designed correspondingly. The effect and effectiveness are fully considered too. The dynamic blocking algorithm can effectively improve the difficulty of reverting original data and privacy discovery by statistic. The effectiveness of the model is proved at the end by theoretical proof.**

***Keywords*—Cloud computing. Privacy filtering. Dynamic block. Two-stages. Asymmetry**

## I. Introduction

Data grows at an explosive rate annually in the Internet era, cloud computing provides users with an efficient low-cost service model, this model allows users to develop their information and services without the restriction of computing speed, storage capacity, network speed and other hardware conditions[2]. Cloud computing uses offsite storage, computing migration patterns, this model combines the distributed computing, parallel computing, utility computing, and other network storage, virtualization, load balancing, hot standby redundancy and many other traditional computer and network technology[4][5]. Cloud computing is no longer simply a specific technology, but a service relies on a variety of technologies[1].

Cloud computing greatly reduces its data operational and management cost through storing the mass data on distributed computer[12]. Users only need to follow the actual calculation and the amount of storage they used to make payments on it which called on-demand use[6]. Cloud computing is considered as the next generation of information technology revolution after the Internet[10]. Currently the biggest obstacle to the development of cloud computing is security issues which impeding users to save their data in the cloud, especially their private data[8][9]. For users, architectures and data management process of cloud computing is transparent, data storage is a remote storage mode in cloud environment, so they don't know where their data is stored, how many copies there are and also don't know whether their private information was leaked or misused[7][11].

In this paper, we design a classification filtering method on initial data with different processing methods according to their privacy levels, which lay the foundation for the subsequent processing of privacy data.

## II. Data Classification

Cloud computing is designed to solve the problem of the cost of mass storage. Among the large amount of data storage, the proportion that really impact on users are quite little, most public resources can be shared, only little parts have close relationship with their learning, work, life, finance, experience and other information[15].

The ability to solve privacy protection is still the key affecting cloud computing development[13]. Mr Zhou Shuigeng defines privacy as information of individuals, institutions and other entities who do not want these information to be known by others14]. Here we divide data into tree types called shared data, general privacy and core privacy according to their sensitivity.

1) **Shared data**: Those allows to be shared with others.

2) **General privacy**: Those can make certain influence to their owners.

3) **Core privacy**: Those can make big influence to their owners.

Classification of data occurs mainly in data

2473-3547/16 $31.00 © 2016 IEEE
DOI 10.1109/ISCID.2016.48