PpBAC:  
Popularity Based Access Control 
Model for Cloud Computing

Suyel Namasudra, Galgotias University, Uttar Pradesh, India  
Pinki Roy, National Institute of Technology, Silchar, India

ABSTRACT

This article describes how nowadays, cloud computing is one of the advanced areas of Information Technology (IT) sector. Since there are many hackers and malicious users on the internet, it is very important to secure the confidentiality of data in the cloud environment. In recent years, access control has emerged as a challenging issue of cloud computing. Access control method allows data accessing of an authorized user. Existing access control schemes mainly focus on the confidentiality of the data storage. In this article, a novel access control scheme has been proposed for efficient data accessing. The proposed scheme allows reducing the searching cost and accessing time, while providing the data to the user. It also maintains the security of the user’s confidential data.

KEYWORDS
Cloud Service Provider, Data Owner, Decryption, Encryption, Popularity Value

1. INTRODUCTION

In IT sector, cloud computing technology is widely used for the data communication process (Deka & Das, 2014). Cloud computing can be defined as a type of advanced area, where numerous distributed and parallel systems are interconnected. It involves many autonomous technologies like network system, utility computing, distributed processing, web services and hardware virtualization. The term “cloud computing” was first introduced in 1996 for describing a model, where all the desktop applications were running on the cloud. In 2007, cloud computing was accepted by all researchers, when a collaboration was made between Google and IBM. Cloud computing offers reducing IT cost, scalability, business continuity, flexibility and unlimited storage (Deka et al., 2013; Deka & Borah, 2012). It also offers users to use cloud when they demand it, and users need not to worry about the software or hardware in a cloud environment. In the cloud computing environment, the Cloud Service Provider (CSP) entity provides the cloud services. The Data Owner (DO) entity stores his/her data on the cloud environment, and cloud customers or users access files or data using the internet. By using the cloud computing, many business models are developed (Armbrust et al., 2010), which may be described by the term “X as a service (XaaS)”. Here, X may be hardware, platform, etc. With the

DOI: 10.4018/JOEUC.2018100102

Copyright © 2018, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.
gradually growth, cloud environment also faces many difficulties (Vaquero et al., 2011; Namasudra et al., 2017a; Xiao & Xiao, 2013). Data confidentiality, data security and access control are the most challenging issues of cloud computing.

Access control is a procedure, which allows a user to access a data or file from the cloud server (Khan, 2012; Majumder et al., 2014). At the time of accessing data, it is necessary to keep the data contents confidential with respect to the CSP. Traditional Access Control Models (ACM) are usually assume that the DO, CSP and users are in the same communication domain. Nowadays, the DOs store their own file or data on the external domains in the encrypted form since DOs and CSP are not in the same domain. Thus, confidentiality of data can be a critical issue in the cloud server. Cloud computing is fully dependent on the internet. So, it again faces lots of security issues. At the time of accessing a large data there are lots of problems, such as high data accessing time, high searching cost, system overhead, data security, etc. Many secure and efficient ACMs have been developed by many researchers (Chang et al., 2016; Namasudra et al., 2014; Namasudra & Roy, 2016a; Ramachandran & Chang, 2016; Namasudra & Roy, 2016b; Namasudra & Roy, 2017a; Namasudra et al., 2017b; Namasudra et al., 2017c; Devi et al., 2016; Namasudra & Roy, 2015; Namasudra & Roy, 2017b; Namasudra, 2018). For restricting user’s access rights, Zhu et al. (2012) proposed Towards Temporal Access Control (TTAC) model, where the CSP monitors the current time that indicates when users make file or data request. Danwei et al. (2009) proposed Usage Control Based Access Control Model (UCON). This model takes large time for providing a file because of the presence of many modules. Gao et al. (2012) proposed Novel Data Access Control (NDAC) technique for secure data accessing, where the DOs have to be constantly online throughout the entire data transferring process. Attribute Based Access Control (ABAC) model depends on the attributes associated with the users (Yu et al., 2010). Gateway Based Access Control (GBAC) scheme was suggested by Wu et al. (2012) for the collaborative cloud environment. Ferraiolo and Kuhn (1992) suggested Role Based Access Control Model (RBAC), where job role has been used. But, in RBAC, user’s confidential file may face security problems because of many hackers. In RBAC and TTAC, the CSP may have to search the whole database for granting one data, and because of the scattered method of the cloud storage system, maintenance can be very difficult. Therefore, in many cases, the data searching time and the data accessing time may be very high. Implementing a cloud environment with the conventional ACMs can lead a number of problems, such as high data searching time, high data accessing time and high overhead of the system. With a view of all these requirements, a novel ACM has been introduced in this paper, namely Popularity Based Access Control Model for Cloud Computing (PpBAC). In PpBAC, the CSP maintains a popularity value for each large data item that facilitates efficient data accessing. The major contributions of this paper are listed below:

1. In this paper, a novel access control scheme has been proposed based on the popularity value.
2. The proposed scheme maintains a popularity value for each large data item for minimizing many problems: high data accessing time, high data searching time for providing the Public key of the DO (PUODO) and the problem of database maintenance.
3. The proposed scheme can resist many attacks, namely stolen-verifier attack, man-in-the middle attack, phishing attack, masquerade attack and internal attack.

The rest of the paper is organized in different parts. Section 2 reviews the related works. Section 3 highlights the system model and system requirements. The proposed scheme has been presented in section 4. Security analysis of the proposed scheme has been given in section 5. Cloud simulation environments have been discussed in section 6. In section 7, results and discussions of the experiments have been discussed. Performance analysis has been presented in section 8. In section 9, comparisons with the existing schemes have been presented. Finally, conclusions of this paper are given in section 10.
Related Content

A Multifactorial Analysis of the Acceptance of Recommender System for Saudi Universities the Literature Revisited
[www.igi-global.com/chapter/a-multifactorial-analysis-of-the-acceptance-of-recommender-system-for-saudi-universities-the-literature-revisited/173967?camid=4v1a](www.igi-global.com/chapter/a-multifactorial-analysis-of-the-acceptance-of-recommender-system-for-saudi-universities-the-literature-revisited/173967?camid=4v1a)

Family Structure and the Telecommuter’s Quality of Life
[www.igi-global.com/article/family-structure-telecommuter-quality-life/55761?camid=4v1a](www.igi-global.com/article/family-structure-telecommuter-quality-life/55761?camid=4v1a)

Errors in Operational Spreadsheets
[www.igi-global.com/article/errors-operational-spreadsheets/4145?camid=4v1a](www.igi-global.com/article/errors-operational-spreadsheets/4145?camid=4v1a)
Self-Determined Adoption of an ICT System in a Work Organization
Eija Korpelainen, Matti Vartiainen and Mari Kira (2010). Journal of Organizational and
End User Computing (pp. 51-69).
www.igi-global.com/article/self-determined-adoption-ict-system/46969?camid=4v1a