

Chapter 64

Data Integrity in Mobile Cloud Computing

Abhishek Majumder
Tripura University, India

Samir Nath
Tripura University, India

Avijit Das
Tripura University, India

ABSTRACT

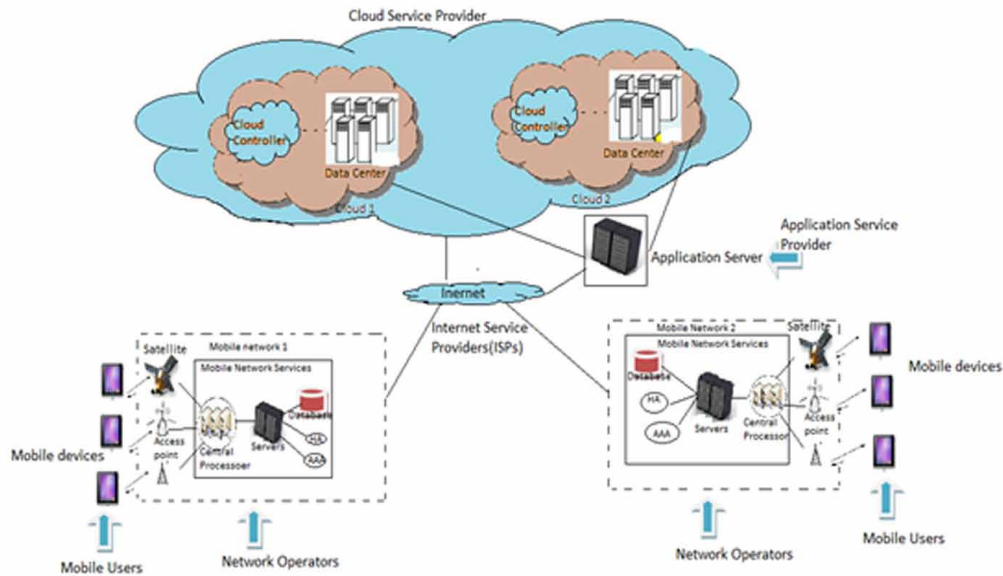
With the help of cloud computing Mobile Cloud Computing (MCC) overcomes the limitations of a mobile device such as security, performance and environment. But, security of the data stored in the cloud is a very challenging issue. Since the cloud cannot be fully trusted, data stored in the cloud is not fully secured. Integrity of the stored data is very important for the data owner. Therefore, it is a big problem to maintain the integrity of the data stored in the cloud environment. This chapter discusses existing schemes for data integrity in the mobile cloud environment. In this chapter a scheme has been proposed for enhancing data integrity in Mobile Cloud Environment. To make integrity checking fast the size of the data file is used. It has also been shown that how fast the integrity loss can be detected if the file size is considered. Finally, the proposed scheme is compared with some of the existing scheme.

INTRODUCTION

The data storage and processing has been shifted to the centralized and powerful systems located inside the cloud from the mobile devices because of the platform provided by the Mobile cloud computing (MCC). MCC (Dinh, 2013, Chetan et al., 2010; Gupta et al., 2012; Mane et al., 2013) offers an infrastructure where data processing and storage is performed outside the mobile device. By this way, the services of MCC can be provided not only to the smart phone users but also to much wide range of mobile users. An example of MCC is shown in Figure 1.

DOI: 10.4018/978-1-5225-8176-5.ch064

Figure 1. Mobile cloud computing architecture



In MCC Mobile Client gets relieved from the burden of computation and storage because most of their data files are put into the cloud. But it gives rise to some new problems and challenges. The owners of the data are often worried about the integrity of the data stored in the cloud because, when the data is stored, owners do not have full control over the data. The cloud cannot be fully trusted; therefore, the data stored in the cloud is not fully secured. CSP can be dishonest and can disclose or manipulate the stored information. This kind of activities will not be acceptable to data owner. Mishaps such as tempering and information disclosure can take place with the data while residing in the cloud. So, data confidentiality and security is very important for the owner. If data is altered by any unauthorized person, the integrity of the data gets severely damaged. Therefore, for the clients it is very vital to guarantee that their data is correctly maintained and stored in the cloud. So, maintaining the integrity of the user data is a challenging issue in mobile cloud environment.

The main objective of this chapter is to design a mechanism to ensure the data integrity as well as the confidentiality of the user's data stored in cloud in MCC environment. In this scheme the objective is to make the data secret not just from the cloud service provider (CSP) but also from trusted third party (TPA). Secondly, to build a simple and efficient mechanism through which the resource constrained mobile device can also be benefited by offloading most of the tasks like encryption, decryption and integrity verification tasks to the TPA.

MOBILE CLOUD COMPUTING

In today's world, handheld devices such as, smart phone, tablet PCs have emerged as an integral part of human life as they are very convenient and effective tools for communication at any place and at

26 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:
www.igi-global.com/chapter/data-integrity-in-mobile-cloud-computing/224631

Related Content

Cloud-Based Adaptable Energy-Efficient Medium-Access Control Protocol for Healthcare Analysis

M. J. Carmel Mary Belinda, E. Kannanand M. Hemanth Chakravarthy (2019). *Novel Practices and Trends in Grid and Cloud Computing* (pp. 215-233).

www.irma-international.org/chapter/cloud-based-adaptable-energy-efficient-medium-access-control-protocol-for-healthcare-analysis/230640

FogLearn: Leveraging Fog-Based Machine Learning for Smart System Big Data Analytics

Rabindra K. Barik, Rojalina Priyadarshini, Harishchandra Dubey, Vinay Kumarand Kunal Mankodiya (2018). *International Journal of Fog Computing* (pp. 15-34).

www.irma-international.org/article/foglearn/198410

Smart Vehicles for Traffic Management and Systems Using Cloud Computing

Ashish Thomas, Gaurav Singaland Riti Kushwaha (2018). *Vehicular Cloud Computing for Traffic Management and Systems* (pp. 178-199).

www.irma-international.org/chapter/smart-vehicles-for-traffic-management-and-systems-using-cloud-computing/206615

Multi-Aspect DDOS Detection System for Securing Cloud Network

Pourya Shamsolmoali, Masoumeh Zareapoorand M.Afshar Alam (2019). *Cloud Security: Concepts, Methodologies, Tools, and Applications* (pp. 1952-1983).

www.irma-international.org/chapter/multi-aspect-ddos-detection-system-for-securing-cloud-network/224666

Fog Computing Architecture, Applications and Security Issues

Rahul Newareand Urmila Shrawankar (2020). *International Journal of Fog Computing* (pp. 75-105).

www.irma-international.org/article/fog-computing-architecture-applications-and-security-issues/245711