Indonesian Journal of Electrical Engineering and Computer Science
Vol. 2, No. 2, May 2016, pp. 452 ~ 460
DOI: 10.11591/ijeecs.v2.i2.pp452-460

Ensuring Data Integrity Scheme Based on Digital Signature and Iris Features in Cloud

[1]Salah H Refish*, [2]Zaid Ameen Abdul jabbar, [3]Zaid Alaa Hussien
[4]Thair A Kadhim, [2]Ali A Yassin, [2]Mohammed Abdulridha Hussain, [5]Salam Waley
[1]Huazhong University of Science and Technology, Wuhan, China
[2]University of Basrah, Basrah, Iraq
[3]Southern Technical University, Basrah, Iraq
[4]Directorate of Education-Babylon, Iraq
[5]University of Technology, Baghdad, Iraq
*Corresponding author, e-mail: manatheraa@yahoo.com

Abstract

Cloud computing is a novel paradigm that allows users to remotely access their data through web- based tools and applications. Later, the users do not have the ability to monitor or arrange their data. In this case, many security challenges have been raised. One of these challenges is data integrity. Contentiously, the user cannot access his data directly and he could not know whether his data is modified or not. Therefore, the cloud service provider should provide efficient ways for the user to ascertain whether the integrity of his data is protected or compromised. In this paper, we focus on the problem of ensuring the integrity of data stored in the cloud. Additionally, we propose a method which combines biometric and cryptography techniques in a cost-effective manner for data owners to gain trust in the cloud. We present efficient and secure integrity based on the iris feature extraction and digital signature. Iris recognition has become a new, emergent approach to individual identification in the last decade. It is one of the most accurate identity verification systems. This technique gives the cloud user more confidence in detecting any block that has been changed. Additionally, our proposed scheme employs user's iris features to secure and integrate data in a manner difficult for any internal or external unauthorized entity to take or compromise it. Iris recognition is an internal organ that is well protected against damage and wear by a highly transparent and sensitive membrane. Extensive security and performance analysis show that our proposed scheme is highly efficient and provably secure.

Keywords*: Cloud computing; data integrity; iris features; digital signature*

1. Introduction

There are many beneficial characteristics of cloud computing, such as being on-demand self- service, broad network access, resource pooling, rapid elasticity, and measured service [1]. Conversely, there exist many security challenges [2, 3]. Cloud storage which is supplied by the cloud server and provided to the cloud users as a service is considered one of these challenges. On the one hand, cloud infrastructures are more powerful and reliable than personal computing devices, although internal and external threats to data integrity still exist. On the other hand, there exist various incentives for the cloud service provider (CSP) to behave dishonorably towards cloud users, such as financial reasons or reputation. All these issues arise because once the cloud users outsource their data to the CSP they no longer have possession of a local copy of their data. At the same time, cloud users lose the ability to monitor and control their data in the cloud, so it can be easily corrupted, modified, or deleted due to hardware failure or human errors.

Thus, protecting the integrity of data is highly essential and security challenge in the cloud. Additionally, the data stored in the cloud is not only accessed but also frequently updated by cloud user, including insertion, deletion, modification etc. Thus, it is imperative to support the dynamic features of cloud storage. The process of saving data in the remotely located cloud servers is called cloud storage [4].Cloud users can upload their data to the cloud and can access these data anytime and anywhere. There are key characteristics that make cloud storage better than traditional storage. These characteristics are (1) performance: with this

Received January 5, 2016; Revised April 18, 2016; Accepted May 1, 2016