Chapter 58
Data Storage Security Service in Cloud Computing: Challenges and Solutions

Alshaimaa Abo-alian
Ain Shams University, Egypt

Nagwa L. Badr
Ain Shams University, Egypt

Mohamed F. Tolba
Ain Shams University, Egypt

ABSTRACT

Cloud computing is an emerging computing paradigm that is rapidly gaining attention as an alternative to other traditional hosted application models. The cloud environment provides on-demand, elastic and scalable services, moreover, it can provide these services at lower costs. However, this new paradigm poses new security issues and threats because cloud service providers are not in the same trust domain of cloud customers. Furthermore, data owners cannot control the underlying cloud environment. Therefore, new security practices are required to guarantee the availability, integrity, privacy and confidentiality of the outsourced data. This paper highlights the main security challenges of the cloud storage service and introduces some solutions to address those challenges. The proposed solutions present a way to protect the data integrity, privacy and confidentiality by integrating data auditing and access control methods.

INTRODUCTION

Cloud computing can be defined as a type of computing in which dynamically scalable resources (i.e. storage, network, and computing) are provided on demand as a service over the Internet. The service delivery model of cloud computing is the set of services provided by cloud computing that is often referred to as an SPI model, i.e., Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). In a SaaS model, the cloud service providers (CSPs) install and operate application

DOI: 10.4018/978-1-5225-8176-5.ch058

software in the cloud and the cloud users can then access the software from cloud clients. The users do not purchase software, but rather rent it for use on a subscription or pay-per-use model, e.g. Google Docs (Attebury, George, Judd, & Marcum, 2008). The SaaS clients do not manage the cloud infrastructure and platform on which the application is running. In a PaaS model, the CSPs deliver a computing platform which includes the operating system, programming language execution environment, web server and database. Application developers can subsequently develop and run their software solutions on a cloud platform. With PaaS, developers can often build web applications without installing any tools on their computer, and can hereafter deploy those applications without any specialized system administration skills (Tim, Subra, & Shahed, 2009). Examples of PaaS providers are Windows Azure (Chambers, 2013) and Google App Engine (Pandey & Anjali, 2013). The IaaS model provides the infrastructure (i.e., computing power, network and storage resources) to run the applications. Furthermore, it offers a pay-per-use pricing model and the ability to scale the service depending on demand. Examples of IaaS providers are Amazon EC2 (Gonzalez, Border, & Oh, 2013) and Terremark (Srinivasan, 2014).

Cloud services can be deployed in four ways depending upon the clients' requirements. The cloud deployment models are public cloud, private cloud, community cloud and hybrid cloud. In the public cloud (or external cloud), a cloud infrastructure is hosted, operated, and managed by a third party vendor from one or more data centers (Tim, Subra, & Shahed, 2009).The network, computing and storage infrastructure is shared with other organizations. Multiple enterprises can work simultaneously on the infrastructure provided. Users can dynamically provide resources through the internet from an off-site service provider (Bhadauria & Sanyal, 2012). In the private cloud, cloud infrastructure is dedicated to a specific organization and is managed either by the organization itself or third party service provider. This emulates the concept of virtualization and cloud computing on private networks. Infrastructure, in the community cloud, is shared by several organizations for a shared reason and may be managed by themselves or a third party service provider. Infrastructure is located at the premises of a third party. Hybrid cloud consists of two or more different cloud deployment models bound together by standardized technology, which enables data portability between them. With a hybrid cloud, organizations might run non-core applications in a public cloud, while maintaining core applications and sensitive data in-house in a private cloud (Tim, Subra, & Shahed, 2009).

A cloud storage system (CSS) can be considered a network of distributed data centers which typically uses cloud computing technologies like virtualization, and offers some kind of interface for storing data (Borgmann, *et al*., 2012). Data may be redundantly stored at different locations in order to increase its availability. Examples of such basic cloud storage services are Amazon S3 (Berriman, *et al*., 2013) and Rackspace (Garg, Versteeg, & Buyya, 2013). One fundamental advantage of using a CSS is the cost effectiveness, where data owners avoid the initial investment of expensive large equipment purchasing, infrastructure setup, configuration, deployment and frequent maintenance costs (Abo-alian, Badr, & Tolba, 2015). Instead, data owners pay for only the resources they actually use and for only the time they require them. Elasticity is also a key advantage of using a CSS, as storage resources could be allocated dynamically as needed, without human interaction. Scalability is another gain of adopting a CSS because Cloud storage architecture can scale horizontally or vertically, according to demand, i.e., new nodes can be added or dropped as needed. Moreover, a CSS offers more reliability and availability, as data owners can access their data from anywhere and at any time (Abo-alian, Badr, & Tolba, 2016). Furthermore, Cloud service providers use several replicated sites for business continuity and disaster recovery reasons.

Despite the appealing advantages of cloud storage services, they also bring new and challenging security threats towards users outsourced data. Since cloud service providers (CSPs) are separate administrative