Chapter 16
Security Issues of Cloud Computing and an Encryption Approach

Miodrag J. Mihaljević
Mathematical Institute, Serbian Academy of Sciences and Arts, Serbia & Chuo University, Japan

Hideki Imai
Chuo University, Japan

ABSTRACT

The main security and privacy issues of cloud computing as well as the related implications are addressed, and a general framework for achieving the goals is summarized. This chapter basically considers scientific and educational employment of a cloud as a particular instance of a public cloud and its security, and as a potentially specific issue, a request for a heavy minimization of the costs implied by security is pointed out. Consequently, the problem of minimization of the overheads implied by security/privacy mechanisms is addressed. The main security requirements are given as well as the main recommendations, providing a framework for the security management. As a particular issue, data protection is considered and significance of data access control and encryption are discussed. Accordingly, an illustrative approach for achieving lightweight and provable secure encryption is shown. The considered encryption is based on joint employment of cryptographic and coding methods.

INTRODUCTION

On one hand side, cloud computing benefits are very exciting ones, but on the other hand side, security and privacy concerns are also very high. Cloud computing creates a large number of security issues and challenges. These issues range from the required trust in the cloud provider and attacks on cloud interfaces to misusing the cloud services for attacks on other systems. As an introduction regarding cloud computing security and privacy issues, following (Cloud Security Alliance, 2009; Borenstein & Blake, 2011; Ren, Wang, & Wang, 2012; Mell, 2012; Bohli, Gruschka, Jensen, Iacono, & Marnau, 2013; Xiao & Xiao, 2013), we outline several critical security and privacy challenges, point out their importance, and motivate need for further investigation of security solutions.

DOI: 10.4018/978-1-4666-5784-7.ch016

Privacy addresses the confidentiality of data for specific entities, and it carries legal and liability concerns, and should be viewed not only as a technical challenge but also as a legal and ethical concern. Protecting privacy in any computing system is a technical challenge, and in a cloud setting this challenge is complicated by the distributed nature of clouds and the possible lack of user awareness over where data are stored and who has or can have access.

From the security and privacy point of view the following two features of cloud computing appears as the top important ones: data service outsourcing, and computation outsourcing. The main problem that the cloud computing paradigm implicitly contains is that of secure outsourcing of sensitive as well as critical data and processes. When considering using a cloud service, the user must be aware of the fact that all data given to the cloud provider leave the own control and protection sphere. Even more, if deploys data-processing applications to the cloud, a cloud provider gains full control on these processes.

As illustrations of the problems and adequate solutions, note the following. Traditionally, to control the dissemination of privacy-sensitive data, users establish a trusted server to store data locally in clear, and then control that server to check whether requesting users present proper certification before letting them access the data. From a security standpoint, this access control architecture is no longer applicable when we outsource data to the cloud because data users and cloud servers aren't in the same trusted domain: the server might no longer be fully trusted as a reference monitor for defining and enforcing access control policies and managing user details. In the event of either server compromise or potential insider attacks, users' private data might even be exposed. One possible approach to enforce data access without relying on cloud servers could be to encrypt data in a differentiated manner and disclose the corresponding decryption keys only to authorized users. This approach usually suffers from severe performance issues, and doesn't scale, especially when a potentially large number of on-demand users desire fine-grained data access control.

Data encryption before outsourcing is the simplest way to protect data privacy and combat illegal access in the cloud, but encryption also makes deploying traditional data utilization services such as plaintext keyword search over textual data or query over database as a difficult task. The trivial solution of downloading all the data and decrypting data locally is impractical, due to the communications and processing costs. Also, an important issue that arises when outsourcing data service to the cloud is protecting data integrity and long-term storage correctness.

Security and Overheads

Cloud computing requires a lot of security measures in order to avoid heavy impacts if the security is compromised. On the other hand side, each security measure implies certain overhead to the cloud functions, and the cumulative overhead could jeopardize the main functionality. So, although embedding the security into the cloud is necessary and provides benefits to users and cloud system providers, it inevitably increases overhead for both. For users in particular, such overheads could offset the cloud's economical attractions, and might conflict with their reasons for using the cloud in the first place. How to quantitatively explore the trade-offs between security overhead and cloud benefit is another interesting and important problem.

The cumulative overhead appears as the implication of the particular ones among which the main are the following:

- Implementation overheads;
- Power consumption overheads;
- Computational overheads.

These overheads could significantly affect the costs of using cloud computing paradigms.