


# Chapter 11

## Enhance Data Security and Privacy in Cloud

**Hicham Amellal**

 <https://orcid.org/0000-0002-7344-3246>

*University Mohamed V, Morocco*

**Abdelmajid Meslouhi**

*University Mohamed V, Morocco*

**Abderahim El Allati**

*Abdelmalek Essaadi University, Morocco*

**Annas El Haddadi**

*ENSA El-Hoceima, Morocco*

### ABSTRACT

*With the advancement of communication and information technology, the internet has become used as a platform for computing and not only a way of communications networks. Accordingly, the large spread of cloud computing led to the emergence of different privacy implications and data security complexities. In order to enhance data security in the cloud, the authors propose in this chapter the use of an encryption box, which includes different cryptosystems. In fact, this step gives the user the opportunities to encrypt data with an unknown algorithm and makes a private key before the storage of data in the host company servers. Moreover, to manage the encryption database, the authors propose a quantum approach in search based on Grover's algorithm.*

### INTRODUCTION

In general terms, the cloud computing refers to the ability to access and manipulate, the stored data and the computer applications run somewhere else's in the servers of the host companies via the internet, using any internet-enabled platform, including smart phones. The cloud computing is used by companies in all industries and for different services this includes: Web-based email services such as Yahoo and

DOI: 10.4018/978-1-5225-9742-1.ch011

Microsoft Hotmail, Photo storing services such as Google's Picasa, spreadsheet applications such as Zoho, online computer backup services such as Mozy, Applications associated with social networking sites such as Facebook and much others. This technology, allows companies to buy IT resources as a service, in the same way that they consume electricity, instead of having to build and maintain internal IT infrastructures (Gupta & Agrawal, 2016; Papazoglou & van der Heuvel, 2007). Also, the cloud computing offers several advantages and benefits for users such as self-service provisioning which allows users to access any on-demand computing resource, elasticity offers the opportunity to increase or decrease the consumption of resources according to the needs of the company and pay per use allows companies to pay only for the resources consumed (Papazoglou & van der Heuvel, 2007). At the same time, the cloud is a multifaceted challenge includes technical and laws, obstacles this includes trust the operators, the question of intellectual property. Therefore, we must be found the achievement of a balanced relationship that guarantees the user rights and the economic return of the company. Recently, the scandal Facebook-Cambridge Analytica showed how the host companies reckless the user privacy. Therefore, the user in his relationship with the company has been always in a weak position, because he cannot verify compliance with the security mechanisms declared as security requirements. Accordingly, the cloud is represented a black box for the user. In order to give the users more control of data and more trust we propose in this paper to protect the privacy in the cloud via encryption box which includes different classical cryptosystems (Amellal et al., 2018; Armbrust et al., 2009).

The paper is organized as follows: In Sec. II, The complexities of privacy in cloud computing. In Sec. III, Cloud computing services. In Sec. IV, our proposition to protect data and privacy in cloud. Finally, conclusion is drawn in the last section.

## **THE COMPLEXITIES OF PRIVACY IN CLOUD COMPUTING**

The privacy implications of cloud computing services introduce a number of unidentified parameters in the management, which makes the relation between the service providers and users are unclear. When customers store their data on host companies' servers, they lose a degree of control over their sensitive information. Accordingly, the responsibility of data security against all menaces including hackers and internal data breaches then falls into the hands of the hosting company rather than the individual user. Moreover, different companies could even readily sale the user's sensitive information with marketing firms. Therefore, there is a big risk in putting our data in someone else's hands (Taylor & Francis, 2018). Therefore; many internet users believe that the safest approach is to maintain sensitive information under your own control. One of the problems with cloud computing is that technology is frequently light years ahead of the law. There are many questions about privacy that need to be answered such as:

- Who are the interferers in cloud computing?
- Does the user or cloud computing own the data?
- What are their limits, roles and responsibilities?
- Can the host deny a user access to their own data?
- Where is the data reserved?
- How is the data replicated?
- What are the relevant legal rules for data processing?
- How will the host companies meet the expected level of data security and privacy?

14 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/enhance-data-security-and-privacy-in-cloud/234814](http://www.igi-global.com/chapter/enhance-data-security-and-privacy-in-cloud/234814)

## Related Content

---

### NERC CIP Standards: Review, Compliance, and Training

Guillermo A. Francia III and Eman El-Sheikh (2022). *Global Perspectives on Information Security Regulations: Compliance, Controls, and Assurance* (pp. 48-71).

[www.irma-international.org/chapter/nerc-cip-standards/302386](http://www.irma-international.org/chapter/nerc-cip-standards/302386)

### Leveraging UML for Access Control Engineering in a Collaboration on Duty and Adaptive Workflow Model that Extends NIST RBAC

Solomon Berhe, Steven A. Demurjian, Jaime Pavlich-Mariscal, Rishi Kanth Saripalle and Alberto De la Rosa Algarín (2016). *Innovative Solutions for Access Control Management* (pp. 96-124).

[www.irma-international.org/chapter/leveraging-uml-for-access-control-engineering-in-a-collaboration-on-duty-and-adaptive-workflow-model-that-extends-nist-rbac/152959](http://www.irma-international.org/chapter/leveraging-uml-for-access-control-engineering-in-a-collaboration-on-duty-and-adaptive-workflow-model-that-extends-nist-rbac/152959)

### A More Secure Image Hiding Scheme Using Pixel Adjustment and Genetic Algorithm

Omar Banimelhem, Lo'ai Tawalbeh, Moad Mowafi and Mohammed Al-Batati (2013). *International Journal of Information Security and Privacy* (pp. 1-15).

[www.irma-international.org/article/a-more-secure-image-hiding-scheme-using-pixel-adjustment-and-genetic-algorithm/95139](http://www.irma-international.org/article/a-more-secure-image-hiding-scheme-using-pixel-adjustment-and-genetic-algorithm/95139)

### Encryption of Analog and Digital signals through Synchronized Chaotic Systems

Kehui Sun (2011). *Chaos Synchronization and Cryptography for Secure Communications: Applications for Encryption* (pp. 415-438).

[www.irma-international.org/chapter/encryption-analog-digital-signals-through/43310](http://www.irma-international.org/chapter/encryption-analog-digital-signals-through/43310)

### Assessing HIPAA Compliance of Open Source Electronic Health Record Applications

Hossain Shahriar, Hisham M. Haddad and Maryam Farhadi (2021). *International Journal of Information Security and Privacy* (pp. 181-195).

[www.irma-international.org/article/assessing-hipaa-compliance-of-open-source-electronic-health-record-applications/276390](http://www.irma-international.org/article/assessing-hipaa-compliance-of-open-source-electronic-health-record-applications/276390)