Chapter 8

Hardware-Based Security for Ensuring Data Privacy in the Cloud

Wassim Itani
American University of Beirut, Lebanon

Ayman Kayssi
American University of Beirut, Lebanon

Ali Chehab
American University of Beirut, Lebanon

ABSTRACT

In this chapter, the authors present a set of hardware-based security mechanisms for ensuring the privacy, integrity, and legal compliance of customer data as it is stored and processed in the cloud. The presented security system leverages the tamper-proof capabilities of cryptographic coprocessors to establish a secure execution domain in the computing cloud that is physically and logically protected from unauthorized access. The main design goal is to maximize users’ control in managing the various aspects related to the privacy of sensitive data by implementing user-configurable software protection and data privacy categorization mechanisms. Moreover, the proposed system provides a privacy feedback protocol to inform users of the different privacy operations applied on their data and to make them aware of any data leaks or risks that may jeopardize the confidentiality of their sensitive information. Providing a secure privacy feedback protocol increases the users’ trust in the cloud computing services, relieves their privacy concerns, and supports a set of accountable auditing services required to achieve legal compliance and certification.

DOI: 10.4018/978-1-4666-2125-1.ch008
Hardware-Based Security for Ensuring Data Privacy in the Cloud

INTRODUCTION

Cloud computing has achieved unprecedented success and adoption in the last few years. This evolutionary computing model relies on the great advancements in virtualization technologies, commodity hardware, processor design, and most importantly Internet communication networks to provide compelling services to enterprises and individuals.

In spite of all the advantages delivered by cloud computing, several challenges are hindering the migration of customer software and data into the cloud. On top of the list is the security and privacy concerns arising from the storage and processing of sensitive data on remote machines that are not owned, or even managed by the customers themselves. With cloud computing, all the customer can see is a virtual infrastructure built on top of possibly non-trusted physical hardware or operating environments. Thus, customers’ fear of sensitive data leakage, misuse, or regulatory incompliance is real and justifiable as long as cloud services are not designed with security in mind (Pearson, 2009). We believe that data privacy should be provided to cloud customers as a service with minimal additional cost. Moreover, we believe that the cloud privacy model should be configurable and user-centric. That is the cloud customer should be able to flexibly control and manage the different privacy mechanisms necessary to protect sensitive data and achieve legal compliance. Customers should be made aware through a secure privacy auditing process of all the operations carried out to secure the storage and processing of their sensitive information. This fact will become more pressing with the expansion of the cloud computing infrastructure where the need will arise for a comprehensive security model that targets the strictest privacy requirements of a wide set of cloud applications and services.

Hardware-based security protocols are believed to be the natural trend that the cloud computing market will follow in the coming years to resolve the different data privacy and integrity challenges hampering the adoption of cloud computing, particularly in healthcare and financial applications. This fact is corroborated by a set of signals received from the IT industry itself:

1. The considerable advancement in physical security mechanisms and packaging technology and the assortment of secure applications that can be implemented on top of physically-secure cryptographic coprocessors.
2. The availability of a set of successful cryptographic coprocessor implementations meeting the strictest FIPS 140 security standards (Dyer et al., 2001).
3. The emergence of general-purpose open-source cryptographic coprocessor designs that provide competitive performance and higher functionality compared to commercial products at one to two orders of magnitude lower cost.
4. The proposed work of the Trusted Computing Group for developing a set of cloud security services and protocols based on their Trusted Platform Module (TPM) (Bajikar, 2002).

In this chapter, we present, PasS (Privacy as a Service), a set of hardware-based security mechanisms for ensuring the privacy, integrity, and legal compliance of customer data as it is stored and processed in the cloud. PasS leverages the tamper-proof capabilities of cryptographic coprocessors to establish a secure execution domain in the computing cloud that is physically and logically protected from unauthorized access. The main design goal is to maximize users’ control in managing the various aspects related to the privacy of sensitive data by implementing user-configurable software protection and data privacy categorization mechanisms. Moreover, the presented security system provides a privacy feedback protocol to inform users of the different
22 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the product's webpage:

www.igi-global.com/chapter/hardware-based-security-ensuring-data/70044?camid=4v1


Recommend this product to your librarian:

www.igi-global.com/e-resources/library-recommendation/?id=1

Related Content

Location-Based Services
www.igi-global.com/chapter/location-based-services/43982?camid=4v1a

Optimal Compensation for Hierarchical Web Services Compositions Under Restricted Visibility
www.igi-global.com/article/optimal-compensation-hierarchical-web-services/58908?camid=4v1a

A Review of Service Frameworks Analyzing Strategic Repositioning: The Case of Bank Services
www.igi-global.com/article/review-service-frameworks-analyzing-strategic/50565?camid=4v1a

Hybridization of SOM and PSO for Detecting Fraud in Credit Card
www.igi-global.com/article/hybridization-of-som-and-pso-for-detecting-fraud-in-credit-card/182657?camid=4v1a