Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 97 (2016) 126 – 130

Procedia Computer Science

CLOUD FORWARD: From Distributed to Complete Computing, CF2016, 18-20 October 2016, Madrid, Spain

Client-side encryption for privacy-sensitive applications on the cloud

Stefano M P C Souza[a,*], Ricardo S Puttini[a]

[a] *Universidade de Brasília, Brasília-DF 70910-900, Brazil*

Abstract

There are important concerns when trusting sensitive information to the cloud. Health and financial records, for instance, suffer strict legal restrictions to data escrow. Organizations holding such information need to assure end-users and authorities that a third party will never access restricted data. Client-side encryption is a common solution in literature. Most works fail, however, to reason the impact of security solutions on performance and usability. Homomorphic and order preserving encryption systems can mitigate such negative impacts, as they allow the computation of regular searches over encrypted records on the cloud, while preserving information confidentiality and the privacy if end-users.

Peer-review under responsibility of organizing committee of the international conference on cloud forward: From Distributed to Complete Computing

Keywords: Cloud computing; security; privacy; client-side encryption; homomorphic encryption

1. Introduction

Cloud computing is a business model by which pooled computational resources are provisioned, on demand and with rapid elasticity, through a broadband network, in the form of a metered service[1]. The main economic appeal of such services is that consumers are able to turn huge capital costs into a smaller and more flexible operational defrayal, pushing concerns with ownership and maintenance of the underlying infrastructure supporting their computing and communication systems to the service provider[2].

To reason the security of assets on the cloud, one must select a stakeholders' perspective or needs. Providers need to efficiently charge for any access to cloud resources. Consumers need assurances about the control over their assets, stability of services and predictability in business conditions. End-users need privacy; they need accurate information and a good sense of control on who has access to their private information[3]. No realistic security solution can be designed to respond to all needs at once.

Also, there are different service models and contract options that render different levels of control and responsibility over systems security to cloud consumers and providers. Infrastructure-as-a-Service consumers control VMs (virtual machines), operational systems, libraries and network configuration, and, thus, are able to implement sophisticated

* Corresponding author. Tel.: +55-61-982623011.
E-mail address: stefano@stm.gov.br

Peer-review under responsibility of organizing committee of the international conference on cloud forward: From Distributed to Complete Computing
doi:10.1016/j.procs.2016.08.289

security techniques, such as VM nesting, memory and processes taint analysis[4]. The same is not true to Platform-as-a-Service or Software-as-a-Service consumers.

There is an important trade-off here: the higher the complexity of cloud services, the lesser the flexibility and effective control over the assets for the consumer and, therefore, the greater the importance of the provider in information security. In most cases, the provider, as a larger organization, with access to cutting edge technology and highly qualified personnel, will be in a better position to deal with security. Consumers, therefore, are better off pushing security concerns and costs to the provider. In some cases, however, consumers are bound by law to guarantee themselves the integrity, confidentiality and privacy of information they hold.

Health care providers, for instance, are held responsible for the security of health records and their patient's privacy. That is, records under their guard cannot be disclosed to any third parties, and, in the case that they are, cannot be used to identify a person. Such restrictions do not only apply to those records comprising health information, but also those that reveal the payment for the provision of any kind of health services. A hospital manager cannot simply respond to government officials saying that the cloud provider is HIPAA[a] compliant and, therefore, he could share the escrow of the Electronic Health Records under his responsibility. The credit card operator, in the same way, cannot share a card holder's payment history on the grounds that the provider is PCI[b] compliant.

The provider will always have privileged access to every part of his service infrastructure, and a curious provider could misuse the virtualization and provisioning basic software stack to capitalize on eventual access to consumer data. The '2015 Information Security Breaches Survey'[5], a comprehensive study from the UK's government, shows that 75% of large corporations in the country had security events related to internal personnel in that year. Despite the solid security and audit processes usually in place, large cloud providers are still vulnerable to the 'insider threat', thus cloud consumers are always at risk of leakage of data transported, processed or stored on the cloud.

Hence, with little control over environment configuration and the resulting security of processes, and little or no access to credible auditing tools, the average consumer can only control what is delivered to the cloud. That makes client-side encryption an important topic. The intuition is that, if every piece of data is encrypted at client-side in a way that even an attacker with enormous computing power cannot break information confidentiality, or end-user's privacy, then the use of a cloud service does not impact information escrow policies[6].

For simple reading and writing to the cloud, the best fit is a fast, well tested and standardized symmetric encryption system. Along with the system used for storage, homomorphic and OPE (order-preserving encryption) systems can be used to provide search indexes and anonymous aggregate information – such as modes, means and other measures of central tendency. A careful combination of different schemes, each enabling a specific computation or feature, can be used to perform regular searches and the most commonly needed operations over the encrypted data on the cloud, revealing no relevant information to an eventual eavesdropper.

2. Related work

There is an intense work, both in industry and academia, to formulate practical solutions with reasonable security for cloud applications. Some works present ways to enhance the auditability of the cloud service software[7]. The strongest trend, however, is to assume the cloud is unsafe and propose a form of secure delegation of computation. Secure multi-party computation protocols have been around for over thirty years now: some with provable security in the semi-honest setting, which fits the cloud scenario. Nevertheless, there are still very few efficient and broadly applicable implementations[8].

Client-side encryption, using homomorphic cryptography, may represent a simpler alternative. The non-interactive nature of homomorphic encryption solutions results in more efficient systems, not bound by network latency nor by the client's thin hardware. Also, there are already many practical applications in literature. The system of Chase and Lauter, for instance, uses an anonymous credentials system, in the form of cryptographic tokens, to allow the exchange of data or endorsement messages between different agents in the health care industry, disclosing no information other than the strictly necessary for that single interaction[9].

[a] Health Insurance Portability and Accountability Act, a US law enforcing standards for electronic health record transactions
[b] Payment Card Industry Data Security Standard, a information security standard for credit cards and payment accounts