

Secure Computing in the Cloud

Edited by

Benny Pinkas², Ahmad-Reza Sadeghi¹, and Nigel P. Smart³

¹ TU Darmstadt, DE, ahmad.sadeghi@cased.de

² Bar Ilan University Ramat Gan, IL, benny@pinkas.net

³ University of Bristol, GB, nigel@cs.bris.ac.uk

Abstract

This report documents the program and the outcomes of Dagstuhl Seminar 11491 “Secure Computing in the Cloud”. Cloud Computing offers a lot of benefits for end customers: high-end machines, incredible amounts of storage, high availability and everything available at the touch of a button. In this seminar we concentrate on compute clouds: Clouds, that do not only offer storage but also computations that can be outsourced in form of virtual machines (VMs). Outsourcing computations as well as data to a third party, in this case the cloud provider, are accompanied by the qualms of confiding data to the cloud provider based on blindly trusted service level agreements. The participants of this seminar discuss the involved risks, create threat models as basic assumptions that describe the (un-)trusted entities and present solutions that augment trust in the cloud provider, the integrity and verifiability of computations and data processed in the cloud.

Seminar 04.–09. December, 2011 – www.dagstuhl.de/11491

1998 ACM Subject Classification K.6.5 Security and Protection

Keywords and phrases cloud computing, outsourced computation, verifiability, integrity, confidentiality, trust

Digital Object Identifier 10.4230/DagRep.1.12.1

Edited in cooperation with Stefan Nürnberger


1 Executive Summary

Stefan Nürnberger

Benny Pinka

Ahmad-Reza Sadeghi

Nigel P. Smart

License  Creative Commons BY-NC-ND 3.0 Unported license
© Stefan Nürnberger, Benny Pinkas, Ahmad-Reza Sadeghi, and Nigel P. Smart

Introduction

Cloud computing offers IT resources, including storage, networking, and computing platforms, on an on-demand and pay-as-you-go basis. The high usability of today’s cloud computing platforms makes this rapidly emerging paradigm very attractive for customers who want to instantly and easily provide web-services that are highly available and scalable to the current demands. In the most flexible and general cloud computing model (“*Infrastructure as-a Service*”, *IaaS*), customers are able to run entire Virtual Machines (VMs) inside the Cloud. VM images function as templates from which a virtually unlimited number of VM instances can be instantiated.



Except where otherwise noted, content of this report is licensed under a Creative Commons BY-NC-ND 3.0 Unported license
Secure Computing in the Cloud, *Dagstuhl Reports*, Vol. 1, Issue 12, pp. 1–10
Editors: Benny Pinkas, Ahmad-Reza Sadeghi, and Nigel P. Smart



Dagstuhl Reports
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

Problem Description

Due to virtualisation, limited physical resources are made available for masses. The sharing of these resources and the complex configuration and maintenance of the needed infrastructure is accompanied by security threats [2, 10]. According to the Cloud Security Alliance (CSA), the major inhibitor of a widespread adaptation of cloud computing is the protection of data [4], as data is no longer under the physical control of the owner (in this case the cloud customer). The cloud provider has access to data stored on disks and data transferred through the cloud network. The fact, that the physical hardware of the cloud is shared with other customers, potentially with adversaries, further stresses the need to protect data in order to thwart the lack of physical control over the own data. Moreover, the outsourced computations must be entrusted to the cloud service provider and face the risk of

Sloppy/Lazy provider: A provider that makes mistakes or simplifies computations. The sloppy and lazy provider might compromise the integrity of the result of computations. Verification of results would be a countermeasure here, for example by executing the computations on multiple, independent clouds.

Greedy provider: A provider which reduces security in order to save money. Greedy providers are willing to violate policies for economic reasons, thereby exposing the data to insider or outsider threats.

Malicious Tenant: A cloud customer (tenant) who is deliberately exploits security vulnerabilities to gain access to data or intellectual insight of processes and computations.

The CSA recommends the use of encryption to protect data in transit and data at rest. However, cryptography in the cloud faces two problems:

1. cryptographic keys in a running VM instance are susceptible to run-time attacks like web server exploits, and
2. key provisioning to a VM is not feasible when we assume the cloud provider has access to data and VM images stored on disk.

Seminar Topics

The participants of this seminar were mainly concerned with the privacy of computation or data with respect to the cloud provider. From concrete examples like doctor-patient-confidentiality while processing genomic data at a third party [5, 6], to generic solutions that hide computations that are done at the cloud provider from the cloud provider itself [9]. Additionally, means to verify the result of an outsourced computation with significantly less computational effort than performing the calculation itself [1, 8, 7, 3]. And last, but not least, even outlooks to ad-hoc clouds that are formed by mobile devices on-demand.

References

- 1 M. Atallah, K. Pantazopoulos, J. Rice, and E. Spafford. Secure outsourcing of scientific computations. *Advances in Computers*, 54:216–272, 2001.
- 2 S. Bleikertz, M. Schunter, C.W. Probst, D. Pendarakis, and K. Eriksson. Security Audits of Multi-tier Virtual Infrastructures in Public Infrastructure Clouds. *Proceedings of the 2010 ACM workshop on Cloud computing security workshop*, 2010.
- 3 K. Chung, Y. Kalai, and S. Vadhan. Improved delegation of computation using fully homomorphic encryption. In *CRYPTO'10*, volume 6223, pages 483–501. 2010.
- 4 Cloud Security Alliance (CSA). Top threats to cloud computing, version 1.0. <http://www.cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf>, March 2010.

- 5 M. Franz, B. Deiseroth, K. Hamacher, S. Jha, S. Katzenbeisser, and H. Schröder. Secure computations on real-valued signals. In *IEEE Workshop on Information Forensics and Security (WIFS'10)*. IEEE Press, 2010.
- 6 M. Franz, B. Deiseroth, K. Hamacher, S. Jha, S. Katzenbeisser, and H. Schroder. Towards secure bioinformatics services. In *Financial Cryptography and Data Security: 15th International Conference, FC 2011, Gros Islet, St. Lucia, February 28-March 4, 2011, Revised Selected Papers*, volume 7035, page 276. Springer-Verlag New York Inc, 2012.
- 7 R. Gennaro, C. Gentry, and B. Parno. Non-interactive verifiable computing: outsourcing computation to untrusted workers. In *CRYPTO'10*, volume 6223, pages 465–482. 2010.
- 8 S. Hohenberger and A. Lysyanskaya. How to securely outsource cryptographic computations. In *TCC'05*, volume 3378, pages 264–282, 2005.
- 9 M.O. Rabin. How to exchange secrets by oblivious transfer. Technical report, Technical Report TR-81, Harvard Aiken Computation Laboratory, 1981.
- 10 T. Ristenpart, E. Tromer, H. Shacham, and S. Savage. Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds. In *CCS'09*, pages 199–212, 2009.

2 Table of Contents

Executive Summary

Stefan Nürnberg, Benny Pinkas, Ahmad-Reza Sadeghi, and Nigel P. Smart . . . 1

Overview of Talks

Introduction to cloud security issues
Benny Pinkas 5

Privacy for Genomic Computations
Stefan Katzenbeisser 5

Two New Models for Delegation of Computation
Ben Riva 5

Outsourcing Multi-Party Computation
Seny Kamara 6

Share Conversion and Private Information Retrieval
Yuval Ishai 6

Automatically Optimizing Secure Computation
Florian Kerschbaum 7

A New Approach to Practical Active-Secure Two-Party Computation
Claudio Orlandi 7

Fundamental Issues When Using Crypto in the Cloud
Stefan Nürnberg 8

On “device clouds”
N. Asokan 8

One Cloud for All – Virtual Revolution?
Marc Oliver Pahl 8

Panel Discussions 9

Participants 10

3 Overview of Talks

3.1 Introduction to cloud security issues

Benny Pinkas (Bar-Ilan University – Ramat-Gan, IL)

License © ⓘ ⊖ Creative Commons BY-NC-ND 3.0 Unported license
© Benny Pinkas

The talk serves as an introduction to cloud computing and to the features that make it so appealing. We then discuss several security issues that are new to cloud computing, which are relevant to either storage clouds or compute clouds.

3.2 Privacy for Genomic Computations

Stefan Katzenbeisser (TU Darmstadt, DE)

License © ⓘ ⊖ Creative Commons BY-NC-ND 3.0 Unported license
© Stefan Katzenbeisser

Joint work of Katzenbeisser, Stefan; Hamacher, Kay; Franz, Martin; Deiseroth, Björn; Jha, Somesh; Busch, Heike
Main reference M. Franz, B. Deiseroth, K. Hamacher, S. Jha, S. Katzenbeisser, H. Schroder, “Towards secure bioinformatics services,” in Proc. of 15th Int’l Conf. on Financial Cryptography and Data Security (FC’11), Revised Selected Papers, vol. 7035, LNCS, p. 276, Springer, 2012.

We show how privacy of genomic sequences can be protected while they are analyzed using Hidden Markov Models (HMM), which is commonly done in bioinformatics to detect certain non-beneficial patterns in the genome. Besides offering strong privacy guarantees, our solution also allows protecting the intellectual property of the parties involved, which makes the solution viable for implementation of secure bioinformatics services.

In particular, we show how two mutually mistrusting parties can obviously run the forward algorithm in a setup where one party knows a HMM and another party knows a genomic string; while the parties learn whether the model fits the genome, they neither have to disclose the parameterization of the model nor the sequence to each other.

Despite the huge number of arithmetic operations required to solve the problem, we experimentally show that HMMs with sizes of practical importance can obviously be evaluated using computational resources typically found in medical laboratories.

3.3 Two New Models for Delegation of Computation

Ben Riva (Tel Aviv University, IL)

License © ⓘ ⊖ Creative Commons BY-NC-ND 3.0 Unported license
© Ben Riva

Consider a weak client that wishes to delegate computation to an untrusted server and be able to succinctly verify the correctness of the result. We present two new natural relaxations to this model. Specifically:

1. We present a model where the weak client delegates the computation to two or more servers, and is guaranteed to output the correct answer as long as even a single server is honest.


In this model, we show: (1) a 1-round statistically sound protocol for any log-space uniform NC circuit; (2) a very efficient computationally sound protocol for any polynomial computation, with a logarithmic number of rounds.

- Next we present a model with a public offline stage. (That is, the offline stage involves no secret randomness and can be publicly verified separately.)

Here we show two computationally sound protocols for any circuit C , where the client runs in time $\text{poly}(\log(\text{size}(C)), \text{depth}(C))$. The first protocol requires only 1 round of interaction, and its soundness is guaranteed assuming the existence of poly-logarithmic PIR. The second protocol requires $\text{poly}(\log(\text{size}(C)), \text{depth}(C))$ rounds but is much more efficient.

3.4 Outsourcing Multi-Party Computation

Seny Kamara (Microsoft Research – Redmond, US)

License  Creative Commons BY-NC-ND 3.0 Unported license
© Seny Kamara

Joint work of Kamra, Seny; Mohassel, Payman; Raykova, Mariana


We initiate the study of secure multi-party computation (MPC) in a server-aided setting, where the parties have access to a single server that (1) does not have any input to the computation; (2) does not receive any output from the computation; but (3) has a vast (but bounded) amount of computational resources. In this setting, we are concerned with designing protocols that minimize the computation of the parties at the expense of the server.

We develop new definitions of security for this server-aided setting, that generalize the standard simulation-based definitions for MPC, and allow us to formally capture the existence of dishonest but non-colluding participants. This requires us to introduce a formal characterization of non-colluding adversaries that may be of independent interest.

We then design general and special-purpose server-aided MPC protocols that are more efficient (in terms of computation and communication) for the parties than the alternative of running a standard MPC protocol (i.e., without the server). Our main general-purpose protocol provides security when there is at least one honest party with input. We also construct a new and efficient server-aided protocol for private set intersection and give a general transformation from any secure delegated computation scheme to a server-aided two-party protocol.

3.5 Share Conversion and Private Information Retrieval

Yuval Ishai (Technion – Haifa, IL)

License  Creative Commons BY-NC-ND 3.0 Unported license
© Yuval Ishai

Joint work of Beimel, Amos; Ishai, Yuval; Kushilevitz, Eyal; Orlov, Ilan

We suggest a new framework for the construction of information-theoretic private information retrieval (PIR) protocols which relies on a generalized notion of "share conversion" in secret sharing schemes. Our framework unifies previous results in the area and gives rise to new protocols that improve the concrete complexity of PIR even for feasible real-life parameters.


In a nutshell, we use the following two-step approach:

- (1) apply share conversion to get a low-communication secure multiparty computation protocol P for a nontrivial class F of low-depth circuits;
- (2) use a lower bound on the VC dimension of F (a combinatorial measure of dimension) to get a good PIR protocol from P .

Our framework reduces the task of designing good PIR protocols to that of finding powerful forms of share conversion which support circuit classes of a high VC dimension.

3.6 Automatically Optimizing Secure Computation

Florian Kerschbaum (TU Dresden, DE)

License  Creative Commons BY-NC-ND 3.0 Unported license
© Florian Kerschbaum

Main reference F. Kerschbaum, “Automatically Optimizing Secure Computation,” in Proc. of the 18th ACM Conf. on Computer and Communications Security (CCS’11), pp. 703–714, ACM.

URL <http://dx.doi.org/10.1145/2046707.2046786>

On the one hand, compilers for secure computation protocols, such as FairPlay or FairPlayMP, have significantly simplified the development of such protocols. On the other hand, optimized protocols with high performance for special problems demand manual development and security verification.

The question considered in this paper is: Can we construct a compiler that produces optimized protocols? We present an optimization technique based on logic inference about what is known from input and output.

Using the example of median computation we can show that our program analysis and rewriting technique translates a FairPlay program into an equivalent – in functionality and security – program that corresponds to the protocol by Aggarwal et al. Nevertheless our technique is general and can be applied to optimize a wide variety of secure computation protocols.

3.7 A New Approach to Practical Active-Secure Two-Party Computation

Claudio Orlandi (Bar-Ilan University – Ramat-Gan, IL)

License  Creative Commons BY-NC-ND 3.0 Unported license
© Claudio Orlandi

Joint work of Nielsen, Jesper; Nordholt, Peter; Orlandi, Claudio; Sheshank, Sai

Main reference J. Nielsen, P. Nordholt, C. Orlandi, S. Sheshank, “A New Approach to Practical Active-Secure Two-Party Computation,” Cryptology ePrint Archive: Report 2011/091, 2011.


URL <http://eprint.iacr.org/2011/091>

We propose a new approach to practical two-party computation secure against an active adversary. All prior practical protocols were based on Yao’s protocol. We use an OT-based approach and get efficiency via OT extension.

To get a practical protocol we introduce a number of novel techniques for relating the outputs and inputs of OTs in a larger computation. We also report on an implementation of this approach, that shows that our protocol is more efficient than any previous one: As an example, evaluating a Boolean circuit of 34000 gates (oblivious AES encryption) takes less than 2 seconds using our protocol.

3.8 Fundamental Issues When Using Crypto in the Cloud

Stefan Nürnberger (TU Darmstadt, DE)


License  Creative Commons BY-NC-ND 3.0 Unported license
© Stefan Nürnberger

Traditionally, Smartcards or HSMs can be used in untrusted environments. However, a natural adaptation from cryptography used on physical machines to virtual machines used in the cloud is not possible due to a lack of securely storing a cryptographic key. Currently, there is no secure means to authenticate a running virtual machine (VM) or to put a key in the VM image before it gets started. Additionally, when a customer's VM is exposed to the Internet (e.g. to provide web services) it is susceptible to attacks and cryptographic keys might be compromised.

We propose an architecture that incorporates a component (CryptoProxy) that securely wraps high-value secret keys of the cloud customer and only exposes them as cryptographic primitives to the customer's VM or to transparently protect resources the VM uses. For instance, this can be authentication or encryption of data or even of a VM image. Keys can be provisioned from outside the cloud to the CryptoProxy over a trusted channel. Our architecture allows to authenticate running VM instances, protect cryptographic keys and acts as a trust anchor that can audit key usage.

3.9 On “device clouds”


N. Asokan (NOKIA Research Center – Helsinki, FI)

License  Creative Commons BY-NC-ND 3.0 Unported license
© N. Asokan

Although local networking technologies like Bluetooth and WiFi have been common for over a decade, they have not led to local ad-hoc device-to-device networking. Several recent developments on energy-efficient and fast device-to-device connections may change this in the near future. This may make it possible to realize a different type of “cloud” consisting of devices (probably of other users) nearby. There are several interesting use cases that make the use of local device cloud interesting from efficiency or privacy points of view. But they also lead to several security and privacy concerns.

3.10 One Cloud for All – Virtual Revolution?

Marc Oliver Pahl (TU München, DE)

License  Creative Commons BY-NC-ND 3.0 Unported license
© Marc Oliver Pahl

A Vision: Computation and storage are ambient resources that can be used by everyone at any place at any time.

With virtualisation every computing and storage resource can be used by everyone. Devices with wireless access are always connected to the cloud and can augment reality. The data of the users is spread everywhere. The dissemination is not controllable and this is also not wanted as the system is autonomous.

How can we have privacy in this vision?

Some thoughts on the example of automated functionality in and across buildings.

4 Panel Discussions

Two cloud security related seminars took place simultaneously at Schloss Dagstuhl from December 4 to December 9, 2011. This Seminar focused on the verifiability, auditability and confidentiality of computation and data, whereas seminar *11492 Secure Architectures in the Cloud* discussed architectures for verification of computations and configurations, as well as customisability of cloud security and privacy. The joint panel discussion featured the panellists Radu Sion, Martijn Warnier, and Marianne Winslett (11492), as well as Ari Juels, Ahmad Sadeghi and Nigel Smart (11491).

Topics of the panel discussion included, but were not limited to, the following. The panel discussed the “big question” whether small or medium-sized enterprises are more secure in the cloud or using their own systems. Naturally, no answer was found. Here as well, an estimation of the security of cloud providers compared to the security of local infrastructures is essential. For this purpose, self-regulatory or government-initiated penetration testing agencies were suggested in order to assess different cloud infrastructures in an objective fashion.

We discussed the security consequences of providing complete infrastructure-as-a-service (IaaS) images in an App-Store like fashion for clouds. This raises security concerns both for the users of such images (potentially malicious software pre-installed) and for the providers of the images (full erasure of sensitive, private data from the images). Consequently, automated checks are needed to address these problems – with some technical details still being challenging.

Other topics included the efficient verifiability of outsourced computation in the general setting that the cloud provider is not fully trusted. Moreover, the internet-of-things was also a topic. That includes car-to-X communication as well as device clouds. The latter allows the creation of ad-hoc clouds, e.g. for the purpose of sharing an internet connection with people who are travelling in order to save roaming fees.

Further, we discussed the possibility of buying insurance for the data stored in the cloud. This, however, requires precise definitions of (a) the coverage of the insurance (data loss, leakage or corruption) and (b) how to assess whether such an event has indeed occurred.

Participants

- N. Asokan
NOKIA Research Center –
Helsinki, FI
- Maxime Augier
EPFL – Lausanne, CH
- Amir Herzberg
Bar-Ilan Univ. – Ramat-Gan, IL
- Yuval Ishai
Technion – Haifa, IL
- Ari Juels
RSA Laboratories – Bedford, US
- Seny Kamara
Microsoft Res. – Redmond, US
- Stefan Katzenbeisser
TU Darmstadt, DE
- Florian Kerschbaum
TU Dresden, DE
- Thilo Mie
KIT – Karlsruhe Institute of
Technology, DE
- Stefan Nürnberger
TU Darmstadt, DE
- Claudio Orlandi
Bar-Ilan Univ. – Ramat-Gan, IL
- Marc Oliver Pahl
TU München, DE
- Alain Patey
Morpho, SAFRAN Group, FR
- Benny Pinkas
Bar-Ilan Univ. – Ramat-Gan, IL
- Ben Riva
Tel Aviv University, IL
- Ahmad-Reza Sadeghi
TU Darmstadt, DE
- Nigel P. Smart
University of Bristol, GB
- Francois-Xavier Standaert
Université Catholique de
Louvain, BE
- Eran Tromer
Tel Aviv University, IL

