Title: Cloud computing security: The scientific challenge, and a survey of solutions

Author: Mark D. Ryan

PII: S0164-1212(12)00337-8
DOI: http://dx.doi.org/doi:10.1016/j.jss.2012.12.025
Reference: JSS 9077

To appear in:

Received date: 24-9-2012
Accepted date: 7-12-2012

Please cite this article as: Ryan, M.D., Cloud computing security: the scientific challenge, and a survey of solutions, *The Journal of Systems and Software* (2013), http://dx.doi.org/10.1016/j.jss.2012.12.025

Cloud computing security: the scientific challenge, and a survey of solutions

Mark D. Ryan University of Birmingham

January 28, 2013

Abstract

We briefly survey issues in cloud computing security. The fact that data is shared with the cloud service provider is identified as the core scientific problem that separates cloud computing security from other topics in computing security. We survey three current research directions, and evaluate them in terms of a running software-as-a-service example.

What is cloud computing security?

Cloud computing is the idea that data and programs can be stored centrally, in the cloud, and accessed any time from anywhere through thin clients and lightweight mobile devices. This brings many advantages, including data ubiquity, flexibility of access, and resilience. In many ways, it also enhances security: the cloud provider may be able to afford to invest in better and more up-todate security technologies and practices than the data owner can. However, since cloud computing necessarily puts data outside of the control of the data owner, it inevitably introduces security issues too.

Cloud computing security concerns all the aspects of making cloud computing secure. Many of these aspects are not unique to the cloud setting: data is vulnerable to attack irrespective of where it is stored. Therefore, cloud computing security encompasses all the topics of computing security, including the design of security architectures, minimisation of attack surfaces, protection from malware, and enforcement of access control. But there are some aspects of cloud computing security that appear to be specific to that domain [1, 2, 3]:

1 The cloud is typically a shared resource, and other sharers (called tenants) may be attackers.

2 Cloud-based data is usually intentionally widely accessible by potentially insecure protocols and APIs across public networks.

3 Data in the cloud is vulnerable to being lost (e.g., accidentally deleted) or incorrectly modified by the cloud provider.