Computers and Electrical Engineering 38 (2012) 1073–1087

Contents lists available at SciVerse ScienceDirect

Computers and Electrical Engineering

journal homepage: www.elsevier.com/locate/compeleceng

A framework for establishing trust in the Cloud ☆

Imad M. Abbadi [a,*], Muntaha Alawneh [b]

[a] Department of Computer Science, University of Oxford, United Kingdom
[b] Information Security Group, Royal Holloway, United Kingdom

ARTICLE INFO

Article history:
Available online 25 July 2012

ABSTRACT

Cloud infrastructure is expected to be able to support Internet scale critical applications (e.g. hospital systems and smart grid systems). Critical infrastructure services and organizations alike will not outsource their critical applications to a public Cloud without strong assurances that their requirements will be enforced. Central to this concern is that the user should be provided with evidence of the trustworthiness of the elements of the Cloud without getting involved into infrastructure details. In addition, users should be able to control their outsourced data at public Clouds. Establishing Cloud's trust model is important but the Cloud's infrastructure complexity and dynamism makes it difficult to address. This paper focuses on an important angle in this direction. We start by identifying the related challenges for establishing trust in the Cloud, and then propose a foundation framework which can help in addressing the identified challenges. Our focus is on IaaS Cloud type and on organizations as Cloud users.

1. Introduction

Cloud computing is relatively a new term in mainstream IT, first popularized in 2006 by Amazon's EC2 [1]. It has emerged from commercial requirements and applications [2]. NIST identifies three main types of Cloud provision: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) [3]. IaaS provides the most flexible model for those Cloud users who prefer to have great control over their resources, while SaaS provides the most tightly-focused type, where Cloud providers retain full control over the virtual resources. Establishing trust in Cloud architectures is an important subject that is yet to receive adequate attention from both academia and industry [2,4–6].

There are a number of techniques that enable one party to establish trust in an unknown entity: direct interaction, trust negotiation, reputation, and trust recommendation and propagation. Most of these establish trust based on identity. Trust negotiation, by contrast, establishes trust based on properties. In a Cloud context establishing trust would be based on both identities and properties [7]. This paper does not discuss the properties an attestor requires when establishing trust in Clouds, it neither discusses the collection of such properties. This paper rather is focussed on the provision of a secure and trustworthy environment which assure users that Cloud providers continually enforce their requirements, does not interfere with their application data, and move the control of users' application data from the hands of Cloud providers to the users. The proposed framework considers Cloud properties based on practical understanding of how Clouds work. In our previous work [8] we proposed a framework for establishing trust in Cloud's virtual layer management (i.e. covers the management data of Clouds infrastructure). However, the previous work does not cover the interaction between users and Clouds (i.e. it does not cover the application data of Cloud users). This paper extends our previous work by covering

☆ Reviews processed and proposed for publication to Editor-in-Chief by Guest Editor Dr. Gregorio Martinez.

* Corresponding author.
E-mail addresses: imad.abbadi@cs.ox.ac.uk (I.M. Abbadi), m.alawneh@rhul.ac.uk (M. Alawneh).

0045-7906/$ - see front matter © 2012 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.compeleceng.2012.06.006

applications data and their integration with infrastructure's management data. Combining these together assures organizations that Cloud providers manage their resources based on their defined properties.

1.1. Organization requirements

Organizations when outsourcing their applications (or part of their applications) using IaaS Cloud type would typically do the following (as discussed in [4,9]): The organization must first decide on the application that will be outsourced to the Cloud. The application nature, organization policy, and legislation factors would play an important role in such a decision. After the organization decides on the applications to be outsourced, it defines the following application requirements (we refer to as *User Properties*): (I) **Technical requirements** — Organization enterprise architects provide an architecture for the outsourced infrastructure based on application requirements. This includes VMs, storage and network specifications. Enterprise architects could also provide the properties of outsourced applications, e.g. DBMS instances that require high availability with no single point of failure. Realizing these would enable Cloud providers to identify the best resources that can meet user requirements [9]. (II) **Service Level Agreement (SLA)** — SLA specifies quality control measures and other legal and operational requirements. (III) **User-centric security and privacy requirements** — An example of these includes users need stringent assurance that their data is not being abused or leaked. Finally, the organization provides these properties to the Cloud via a set of APIs. The APIs are supplied by the Cloud provider, which then creates virtual resources considering the provided user properties. Cloud provider manages the organizational outsourced resources based on the agreed user properties. In turn the organization pay Cloud provider on a pay-per-use model.

Current Cloud providers have full control over all hosted services in their infrastructure; e.g. Cloud provider controls who can access VMs (e.g. internal Cloud employees, contractors) and where user data can be hosted [10,2]. Cloud users have very limited control over the deployment of their services, have no control over the exact location of the provided services, and have no option but to trust Cloud provider to uphold the guarantees provided in the SLA.

1.2. Organization of the paper

This paper is organized as follows. Section 2 discusses the related work. Section 3 outlines Cloud taxonomy and management. Section 4 identifies the paper's main objectives and the framework requirements. Section 5 identifies devices hardware properties. Section 6 discusses the dynamic domain concept, and then proposes the Cloud framework architecture. Section 7 defines and discusses the framework software agents. Section 8 proposes the scheme workflow. Section 9 analyses the proposed scheme framework. We conclude the paper in Section 10. Finally, Appendix A presents our prototype.

2. Related work

Many research on Cloud mainly focuses on independent structural components. Research in Cloud's structural components and their security existed long-time ago before the term 'Cloud Computing' and are well established research areas; however, such areas still have unresolved problems which are inherited to the Cloud [4,11]. The issue of establishing trust in the Cloud has been discussed by many authors. Much of the discussion has been centered around reasons to "trust the Cloud" or not to. Khan and Malluhi [12] discusses factors that affect consumer's trust in the Cloud and some of the emerging technologies that could be used to establish trust in the Cloud including enabling more jurisdiction over the consumers' data through provision of remote access control, transparency in the security capabilities of the providers, independent certification of Cloud services for security properties and capabilities and the use of private enclaves. The issue with jurisdiction is echoed by Hay et al. [13], who further suggest some technical mechanisms including encrypted communication channels and computation on encrypted data as ways of addressing some of the trust challenges. Schiffman et al. [14] propose the use of hardware-based attestation mechanisms to improve transparency into the enforcement of critical security properties. Ryan et al. [15] discuss the importance of accountability and provenance in providing trustworthy Cloud infrastructure. Accountability, and more generally provenance in Clouds, are a key to establish trustworthy Cloud. Our paper establishes the secure foundation which can be utilized by other frameworks (e.g. Cloud provence mechanism) to establish trustworthy Clouds. Takabi et al. [16] discusses the importance of establishing secure and trusted Cloud computing. They also raise several questions concerning the way a trust could possibly be established considering Cloud dynamic nature and suggested the use of "delegation primitives" [17] without discussing any details of how this could establish trust in Clouds.

Some researchers proposed the usage of a TPM (TPM is discussed in Section 5) to establish trust in Clouds and to provide remote attestation [14,18,19]. The work in [18] establishes trust between Cloud entities based on their dynamic behavior which is not accurate and might affect Cloud availability and resilience. For example, entities at the physical layer forming a collaborating domain do not communicate frequently, and sometimes never communicate directly. If a physical domain fails then all its hosted resources must start-up immediately at another physical domain. Establishing a chain of trust at this stage affects the timing of service recovery. The work of [14,19] provide remote attestation for either the entire Cloud infrastructure or for the physical resources hosting VMs. However, we argue that it is not practical to attest to the entire Cloud infrastructure considering its enormous resources, neither it is practical to attest to a specific set of physical resources considering the dynamic nature of Clouds where VMs can move between different physical resources.