Contents lists available at ScienceDirect

Computer Standards & Interfaces

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

Towards the design of secure and privacy-oriented information systems in the cloud: Identifying the major concepts

Christos Kalloniatis [a,*], Haralambos Mouratidis [b], Manousakis Vassilis [a], Shareeful Islam [b], Stefanos Gritzalis [c], Evangelia Kavakli [a]

[a] Cultural Informatics Laboratory, Department of Cultural Technology and Communication, University of the Aegean, University Hill, GR81100 Mytilene, Greece
[b] School of Architecture, Computing and Engineering, University of East London, UK
[c] Information and Communication Systems Security Laboratory, Department of Information and Communications Systems Engineering, University of the Aegean, GR83200 Samos, Greece

ARTICLE INFO

Available online 29 December 2013

Keywords:
Security
Privacy
Cloud computing
Security and privacy issues
Concepts
Requirements

ABSTRACT

One of the major research challenges for the successful deployment of cloud services is a clear understanding of security and privacy issues on a cloud environment, since cloud architecture has dissimilarities compared to traditional distributed systems. Such differences might introduce new threats and require a different treatment of security and privacy issues. It is therefore important to understand security and privacy within the context of cloud computing and identify relevant security and privacy properties and threats that will support techniques and methodologies aimed to analyze and design secure cloud based systems.

1 . Introduction

The last few years, a new generation of technology has positively invaded our lives providing a number of capabilities that have made our digital behavior much easier than before. This technology is commonly known as "cloud computing". Various well-known services such as email, instant messaging, and web content management, are among the many applications that can be offered via a cloud environment. Although many of these services and applications were offered, through the internet, before the cloud era; cloud computing environments offer greater degree of scalability, flexibility, and resource pooling thus elevating its use, leading to its great expandability and applicability noted nowadays [1].

While the degree of internet users that enroll and access cloud based services rises dramatically every day, recent surveys reveal the uncertainty and instability of cloud environments. In June 2009, a survey conducted by a document management software company revealed, that 41% of senior IT professionals don't know what cloud computing really is [2]. From the remaining 59% of IT professionals, who stated that they know what cloud computing is, 17% of them understand cloud computing to be internet-based computing while 11% believe it is a combination of internet-based computing, software as a service (SaaS), software on demand, an outsourced or managed service and a hosted software service. The remaining respondents understand cloud computing to be a mixture of the above. One of the innovations that cloud computing introduced and played a key role in its rapid development is the use of virtualization as a way for providing three basic types of services: software, platform and infrastructure. However, most of the recent studies [3–7] have identified a number of security and privacy challenges unique to the cloud. Although, typical security and privacy concerns, such as data protection, unauthorized access, data handling and traceability, are the same as in traditional distributed systems, the solutions required and the requirements introduced by those in a cloud context are very different than those used in traditional systems.

With engineering software systems, it is necessary to identify and model respective security and privacy properties based on the system specific context so that appropriate security and privacy requirements can be identified and analyzed. The elicited security and privacy requirements should be implemented within the system, which should enclose all the necessary measures for dealing with possible security and privacy threats that will cause harm to its assets or users. A number of research efforts [8–11] have already contributed to the area of identifying and analyzing security and privacy requirements for the development of software systems. However, these works have not been developed for cloud based systems. On the other hand, industry-led reports [1,2,12] have been published discussing security and privacy issues within the context of cloud computing. However, most of these reports provide a list of security and/or privacy issues without providing a clear linkage with relevant security and privacy properties and threats. Moreover, they do not explicitly discuss any set of requirements that are essential for analysis and design methodologies to incorporate, to support security and privacy analysis for cloud based systems.

[*] Corresponding author.
E-mail addresses: chkallon@aegean.gr (C. Kalloniatis), haris@uel.ac.uk (H. Mouratidis), ct08081@ct.aegean.gr (M. Vassilis), shareeful@uel.ac.uk (S. Islam), sgritz@aegean.gr (S. Gritzalis), kavakli@ct.aegean.gr (E. Kavakli).

0920-5489/$ – see front matter © 2013 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.csi.2013.12.010

This paper makes a number of contributions. Fig. 1 provides an overview of our contributions. On the one hand, we discuss a number of security and privacy properties that are applicable to the cloud. Our work in that area is based on the highly influential and important report from the Cloud Security Alliance (CSA) [13] and work from an EU report on cloud computing [14]. However, our work introduces a number of security and privacy properties that are not discussed in these reports. On the other hand, we provide a clear linkage between those properties and relevant security and privacy threats. In particular, based on the list of threats published by CSA [3] and Gartner [15], we discuss how each of the security and privacy properties can be linked to specific threats. Finally, we provide a set of requirements that we consider important for any development methodology that supports the analysis and design of security and privacy in the cloud. Although, we do not claim that the list of presented requirements is final (on the contrary we believe it is work in progress), we believe the list provides a good starting point for any developers that would like to consider inclusion of cloud security and privacy analysis in their methodology. As shown in Fig. 1, we start with cloud computing areas and conclude with a list of requirements based on the security and privacy properties, threats and critical areas.

Section 2 provides a brief overview of the basic cloud computing characteristics. In Section 3, the most critical cloud computing areas are presented along with security and privacy threats. In Section 4, the major security and privacy properties are discussed and a clear linkage is provided between issues, threats and properties. Moreover, a set of requirements is presented for methodologies based on the linkage of issues, threats and properties in Section 5. Section 6 presents related work both on software engineering methods both in the fields of traditional as well as cloud oriented systems. Finally, Section 7 presents areas for future work and concludes the paper.

2 . Cloud computing main characteristics

Cloud computing is the delivery of computing and storage capacity as a service [12] to a community of end-recipients. Cloud computing entrusts services with a user's data, software and computation over a network, following a logical diagram as shown in Fig. 2. Cloud computing providers offer their services according to three fundamental models [16–18]: a) Infrastructure as a Service (IaaS), where users rent the use of servers provided by one or more cloud providers; b) Platform as a Service (PaaS), where users rent the use of servers and the system software to use in them; and c) Software as a Service (SaaS), where users rent also the application software and databases. In the cloud, IaaS is the most basic and each higher model abstracts from the details of the lower models as it is graphically shown in Fig. 3.

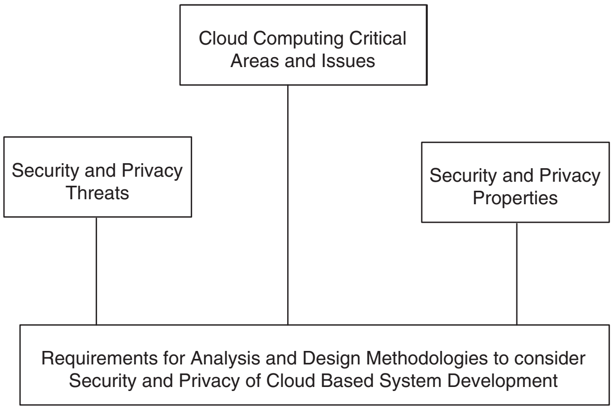
Cloud Computing Critical Areas and Issues
Security and Privacy Threats
Security and Privacy Properties
Requirements for Analysis and Design Methodologies to consider Security and Privacy of Cloud Based System Development

Fig. 1. Overview of the contribution.

Cloud computing provides the following characteristics:

a) *Agility*, which improves users' ability to re-provision technological infrastructure resources;
b) *Cost*, which is reduced since infrastructure is typically provided by a third party and does not need to be purchased for one-time or infrequent intensive computing tasks. Also the cost of IT skills is lowered since in-house implementation is avoided [19];
c) *Virtualization*, which is the basic technology used in cloud environments allows servers and storage devices to be shared thus increasing utilization. Applications are usually being migrated from one server to another depending on the capacity and usage of the cloud providers' infrastructure;
d) *Multi-tenancy*, which enables the sharing of resources and cost across a large pool of users allowing centralization of infrastructure, increment of peak-load capacity and systems' utilization and efficiency improvement [20];
e) *Reliability*, which is improved if multiple redundant sites are used, which makes well-designed cloud computing suitable for business continuity and disaster recovery [21];
f) *Scalability* and *elasticity*, which support the on-demand provisioning of resources on a fine-grained self-service basis near real-time without users having to engineer for peak loads [22,23];
g) *Device and location independence*, which support users to access cloud services from any place through a web-browser regardless of the device they are using or the location they are accessing the service from [24]; and
h) *Maintenance*, which is easier since there is no software installation on each user's machine and the services' sources are managed and updated from a single third party.

It is worth mentioning, that although the combination of the above characteristics is what provides the various advantages of cloud computing, it is the same combination that introduces new security and privacy challenges and requires different solutions. The following section provides an analysis of the critical areas and major threats that exist in cloud environments.

3 . Critical areas and threats of cloud computing

Building new services in the cloud or even adopting cloud computing into existing business context in general is a complex decision involving many factors. Enterprises and organizations have to make their choices related to services and deployment models as well as to adjust their operational procedures into a cloud oriented scheme combined with a comprehensive risk assessment practice resulting from their needs. In doing so, it is important to have a clear understanding of the critical areas, with respect to security and privacy, of a cloud computing solution. This section provides an overview of the critical areas of cloud computing and security and privacy threats that can affect the cloud based system context.

3.1. Critical areas of cloud computing

We performed a systematic review [25] of the literature, which started by identifying studies that consider cloud computing areas, alongside security and privacy as domain specific key words. We focused on areas that are important to cloud based systems, such as virtualization, interoperability, regulatory compliance, and identity management. We followed these key words to specifically search the literature. We also identified relevant literature from major research databases such as Elsevier, IEEE Xplore, SpringerLink, ACM Digital Library, and Google scholar. We considered only peer-reviewed papers and considered citations and place of publication of individual papers as