New Approach for Information Security in e-Government

Roumen Trifonov, Tasho Tashev, Natalia Toteva

Technical University of Sofia, Bulgaria,

r_trifonov@tu-sofia.bg, t_tashev@tu-sofia.bg, nati_toteva@abv.bg

Abstract—Cloud computing, is a new paradigm for obtaining computing resources and services. In a cloud computing model the resources, such as storage and processing power, as well as services, including software platforms and applications, are dynamically accessed through (most often, public) networks. The cloud’s attributes of scale and flexibility are both a friend and a foe from a security point of view. The massive concentrations of resources and data present are more attractive target to attackers, but cloud-based defences can be more robust, scalable and cost-effective.

Keywords—Information security, risk assessment, vulnerabilities, cloud computing, new technology.

I. INTRODUCTION

Cloud computing, although not a new technology, is a new paradigm for obtaining computing resources and services. In a cloud computing model, the resources, such as storage and processing power, as well as services including software platforms and applications, are dynamically accessed through (most often, public) networks.

The recent draft definition from USA National Institute for Security and technology /NIST/ is perhaps the most comprehensive attempt at outlining the key characteristics of the cloud computing paradigm:

“Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction”.

Cloud computing is an on-demand service model for IT provision, often based on virtualization and distributed computing technologies (figure 1).

The cloud obscures the location of the asset; the only thing the user is concerned with is that the expected asset exists and it works. The essential two characteristics of a cloud environment are that:

- the asset is set up, deployed, or engaged instantly or near-instantly over a network (usually the Internet/Web) without binding to specific physical compute resources, and
- the capacity of the application (supported number of concurrent users, transactions per unit time, amount of storage, etc.) is adjusted automatically as demand fluctuates so that manual sizing and provisioning are eliminated both up-front and over time.

Cloud computing architectures have:

- highly abstracted resources;
- near instant scalability and flexibility;
- near instantaneous provisioning;
- shared resources (hardware, database, memory, etc);

“service on demand”, usually with a “pay as you go” billing system;

Figure 1
• programmatic management (e.g., through WS API), etc.

Many governments are interested in the possibility of using cloud computing to reduce IT costs and increase capabilities [1]. For example, the US Government General Services Administration now offers a portal for cloud computing services [2]. Governments too have serious hurdles to overcome - in terms of public perception of the secure processing of citizens’ personal information in cloud computing infrastructures. On top of this, there are also legal and regulatory obstacles which prevent many e-Government applications from moving to cloud. Nevertheless, the large (primarily economic) benefits of cloud computing forced government (especially in times of crisis) to seek to orient essential part of their activities to it.

The cloud’s attributes of scale and flexibility are both a friend and a foe from a security point of view. The massive concentrations of resources and data present are more attractive target to attackers, but cloud-based defences can be more robust, scalable and cost-effective.

II. MAIN SECURITY BENEFITS OF CLOUD COMPUTING

The first group of benefits are related to the scalability: all kinds of security measures are cheaper when implemented on a larger scale. This includes all kinds of defensive measures such as filtering, patch management, hardening of virtual machine instances and hyper-visors, etc. Other benefits of scale include: multiple locations, edge networks (content delivered or processed closer to its destination), timeliness of response to incidents, threat management, etc.

Other benefits are related to the ability of large cloud providers to offer a standardised, open interface to managed security services providers. This creates a more open and readily available market for security services. It is necessary to mention also the ability of the cloud providers to dynamically reallocate resources for filtering, traffic shaping, authentication, encryption, etc, which has obvious advantages for resilience regarding defensive measures (e.g., against DDoS attacks).

Furthermore, it should be noted that cloud computing (when using virtualisation) can provide dedicated, pay-per-use forensic images of virtual machines which are accessible without taking infrastructure off-line, leading to less downtime for forensic analysis. It can also provide more cost-effective storage for logs allowing more comprehensive logging without compromising performance.

III. THE MAIN SECURITY RISKS OF CLOUD COMPUTING

The first risk is related to the loss of governance - in using cloud infrastructures, the client necessarily cedes control to the cloud provider on a number of issues which may affect security. At the same time, the Service Layer Agreement may not offer a commitment to provide such services on the part of the cloud provider, thus leaving a gap in security defences.

The risk of isolation failure covers the failure of mechanisms separating storage, memory, routing and even reputation between different tenants (e.g., so-called guest-hopping attacks). However it should be considered that attacks on resource isolation mechanisms (e.g., against hyperversors) are still less numerous and much more difficult for an attacker to put in practice compared to attacks on traditional operational systems.

The investment in achieving certification (e.g., industry standard or regulatory requirements) may be put at risk by migration to the cloud if:

- the cloud provider cannot provide evidence of their own compliance with the relevant requirements;
- the cloud provider does not permit audit by the cloud customer.

The cloud computing poses several data protection risks for cloud customers and providers. In some cases, it may be difficult for the cloud customer (in its role as data controller) to effectively check the data handling practices of the cloud provider and thus to be sure that the data is handled in a lawful way. This problem is exacerbated in cases of multiple transfers of data, e.g., between federated clouds. On the other hand, some cloud providers do provide information on their data handling practices. Some also offer certification summaries on their data processing and data security activities and the data controls they have in place.

It is necessary to note that it is often possible for the cloud customer to transfer risk to the cloud provider; however not all risks can be transferred - if a risk leads to the failure of a business, serious damage to reputation or legal implications, it is hard or impossible for any other party to compensate for this damage.

IV. RECOMMENDATIONS AND AREAS FOR FURTHER RESEARCH

Naturally, when we operate with such new technology and face the lack of practical experience, the questions are much more than answers. Here we tried to indicate answers given in some studies in the U.S. and Europe.

1) Some of the challenges to trust present in today’s solutions will be transferred to the cloud environment. First of all, establishing a clear chain
of trust from the client application to the server application - the hardware-software chain of trust needs to be adapted to the cloud environment and provide the capability for remote attestation to allow verification by the clients. At the same time the model needs to allow for performing the equivalent of client safety checks from the cloud rather than through the enterprise network access control. In the future, the trust model needs to be extended to the data, in order to allow it to carry and enforce its access control policy wherever it resides.

Secondly, the defence-in-depth practices employed in protecting data need to be scaled and adapted to protect cloud services. This includes evaluating the current network segmentation models, as well as active and passive controls including intrusion and extrusion detection and anomaly detection. User access control and traffic security mechanisms need to be adapted to work effectively in the cloud environment also.

2) The new challenges posed to the data protection in the cloud environment include:
   • data life-cycle management, i.e. mechanisms to securely create, process, and destroy data residing in the cloud;
   • ensuring integrity of the cloud-based data, including cases when it has to be restored from backups;
   • effective models for managing and enforcing data access policies, regardless of whether the data is stored in the cloud or cached locally on client devices;
   • encrypted data storage that allows cloud-based processing capabilities, including search and indexing.

3) In addition to the technical issues involved in data protection, policy and law enforcement challenges can also benefit from research efforts. Cloud computing models can benefit greatly from the harmonization of data protection, retention, and privacy regulations internationally. This will create an environment in which cloud computing customers will be able to effectively conduct their business globally and obtain their computing services in the most effective and economical fashion.

4) The cloud computing paradigm shift creates new challenges in evaluating the levels of assurance offered and certification standards. Research and industry collaboration is needed to develop guidelines and standards that will allow meaningful and unambiguous evaluation and certification of the assurance of cloud-based services. Standards and methods equivalent to the ISO270XX series are required. At the same time, uniform governance models and best practices will make evaluation and certification easier.

5) In cloud computing, even though many interfaces have been standardized at the software level, which has led to cross-platform interoperability, there has not been any significant standardization activity that has led to proprietary application programming interfaces. This makes it difficult for a customer to move from one cloud computing provider to another and is one of the reasons why many organizations are reluctant to move their services and data to the cloud. Making service and data migration easier, the cloud providers would allow easier migration between the traditional data centre model and the cloud and between different cloud providers.

V. CONCLUSION

The path to secure cloud computing is surely a long one, requiring the participation of a broad set of stakeholders on a global basis. However, we should recognize the progress we are seeing: new cloud security solutions are regularly appearing, enterprises are using new guidance to engage with cloud providers, and a healthy public dialogue over compliance and trust issues has erupted around the world. The most important victory achieved is that security professionals are vigorously engaged in securing the future, rather than simply protecting the present.

REFERENCES


ABOUT THE AUTHORS

Dr. Roumen Trifonov – Department of Computer Systems, Technical University of Sofia, BULGARIA, e-mail: r_trifonov@tu-sofia.bg,
Dr. Tasho Tashev – Dean of English Language Faculty of Engineering, Technical University of Sofia, BULGARIA, e-mail: t_tashev@tu-sofia.bg
Natalia Toteva – PhD student, Department of Electrical Measurement, Technical University of Sofia, BULGARIA, e-mail: nati_toteva@abv.bg