International Journal of Scientific Engineering and Research (IJSER)
www.ijser.in
ISSN (Online): 2347-3878
Volume 2 Issue 2, February 2014

An Approach for Secure Virtual Resource Service Differentiation in a Cloud

P Ramesh Naidu[1], Yerriswamy T[2], Ashwath K[3]

[1]Assistant Professor, Dept. of Computer Science and Engineering
Sri Venkateshwara College of Engineering, Bangalore, India

[2]Assistant Professor, Dept. of Computer Science and Engineering
Sri Venkateshwara College of Engineering, Bangalore, India

[3]Lecturer, Dept. of Computer Science and Engineering
Sri Venkateshwara College of Engineering, Bangalore, India

Abstract: ***The cloud computing infrastructure is hosted in data centers. If a service user orders a cloud service, e.g., a virtual machine in Amazon's EC2, this virtual resource is placed on a physical infrastructure within a data center of the cloud operator. The virtual resource might be moved within the data center from one physical machine to another, e.g., due to maintenance reasons migrating virtual resources to physical machines located in other data centers of the same operator, or to physical machines of other operators automatically is not possible. However, there are some use cases where a flexible placement of virtual resources is needed, e.g., for optimization reasons (reducing costs or latencies when accessing the virtual resource). In cloud networking, virtual resources are moved automatically from one operator's cloud infrastructure to another. Therefore, security checks must also be carried out automatically, in order to assure that an operator's infrastructure follows the service user's demands. In this paper we show an approach for automated security checks. In our approach a service user can define security requirements and a virtual infrastructure provider can describe its security functionality. A service provider moderates the placement of virtual resources, maps the security demands to security functionality, and if needed moves the virtual resources to another virtual infrastructure provider.***

Keywords: cloud, virtual machine, latency, symmetric

1. Introduction

In recent times cloud computing has become more and more popular and is applied for various purposes. Cloud computing itself is in principle an abstraction of the physical infrastructure which is offered as cloud services to service users. The abstraction levels of these cloud services are Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), and Infrastructure-as- a-Service (IaaS). Popular examples are GoogleDocs for SaaS, Google's AppEngine for PaaS, and Amazon's EC2 for IaaS [1][3].

The cloud computing infrastructure is hosted in data centers. If a service user orders a cloud service, e.g., a virtual machine in Amazon's EC2 [3], this virtual resource is placed on a physical infrastructure within a data center of the cloud operator. The virtual resource might be moved within the data center from one physical machine to another, e.g., due to maintenance reasons. A migrating virtual resource to physical machines located in other data centers of the same operator, or to physical machines of other operators automatically is not possible. However, there are some use cases where a flexible placement of virtual resources is needed, e.g., for optimization reasons (reducing costs or latencies when accessing the virtual resource) [3]. The European project SAIL investigates the combined management of cloud computing infrastructures (of different operators) and network infrastructures. This combined management enables the infrastructure service user to optimize various parameters, like costs for the virtual resource, latencies when accessing them. Additionally, this combined management enables cloud and network operators to enhance the work load of their infrastructure, e.g., by adapting pricing or by intelligent placement of virtual resources to reduce network load. Unfortunately, this flexible placement of virtual resources introduces new challenges regarding security. In the cloud computing world the service user checks the security level of a cloud operator manually if security relevant information is published by the operator. Only if the security policies of the service user are followed the service user moves his virtual resource to the cloud operator's infrastructure and it stays there until the costumer removes it manually [4]. In cloud networking, virtual resources are moved automatically from one operator's cloud infrastructure to another. Therefore, security checks must also be carried out automatically, in order to assure that an operator's infrastructure follows the service user's demands. In this paper we show an approach for automated security checks. In our approach a service user can define security requirements and a virtual infrastructure provider can describe its security functionality. A service provider moderates the placement of virtual resources, maps the security demands to security functionality, and if needed moves the virtual resources to another virtual infrastructure provider [1] [2].

2. Roles

We will use the following terminology during the rest of this paper.

- Service User: A service user is a person who is authorized to use the services provided by a service provider, e.g., a private user or an employee of an enterprise. He requests services by the service provider by using a request mechanism [1].

- Service Provider: A service provider provides services to a service user. He is responsible to map the requested services of the service user to a virtual infrastructure provider. Especially, he has to take care of following the security demands of the service user. A service provider can also be at the same time a virtual infrastructure provider [1][2].
- Virtual Infrastructure Provider: A virtual infrastructure provider provides virtual IT infrastructure, where services can be installed on. A service provider uses this virtual infrastructure for implementing and offering his services. Generally, the virtual infrastructure provider owns the hardware, where the virtual infrastructure is running on [1][2].
- Virtual Resource: A virtual resource is a virtual processing, storing, or networking entity that is placed on a physical resource of a virtual infrastructure provider [1].

3. Ease of Use

- Traveling business man: In this use case we consider a business man (service user) who has only a lightweight portable device and uses this device to access his virtual machine (service offered by the service provider) which runs in the cloud network [1]. The service user has several security demands on the virtual resource, in order to follow his company's security policies, e.g., that the virtual resource must be located in Europe or Australia and that the access to the data center where the virtual resource resides must be ISO 27001:500 certified. His normal working place is in Europe. In order to reduce latency the service provider demands virtual resource in Europe by a virtual infrastructure provider which has physical resources in Europe that are ISO 27001:500 certified [3].

  When the business man is on a travel in Australia the service provider takes care of moving the business man's virtual resource to Australia in order to keep latency down. Again, the service provider has to take care of choosing a virtual infrastructure provider that has ISO 27001:500 certified physical resources. On another time the business man travels to the USA. In this case the service provider cannot move the virtual machine to the USA because of the security demands of the business man [3].

- Cheap Processing and Storage: In this use case we consider a service user that is interested in cheap processing and storing resources, e.g., a small company that needs from time to time some intensive calculations (e.g., rendering of videos). The service user demands processing power with the constraint that the service is operated in a data center that is ISO 27001:500 certified at the lowest price. In this use case the latency is not really important. For that reason the service provider takes the cheapest virtual infrastructure provider that is ISO 27001:500 certified. If the processing of the task takes longer the service provider may move the task to another virtual infrastructure provider if it becomes the cheapest one. Reasons for diversities in prices of a virtual infrastructure provider might be the current work load(e.g., because of different time zones of service users and virtual infrastructure provider) or diversity in prices for energy (smart grid) [3].

4. Security Challenge and approach

- One challenge in cloud computing is that the service user has some security requirements on the cloud infrastructure which he wants to use, e.g., in the first use case, these security requirements base on security policies of the business man's company. Today, this is done manually in the way that the service user checks some security parameters of a virtual infrastructure provider and compares them with his security requirements. After a positive evaluation the service user moves his data or processes to the virtual infrastructure provider's place. In the case that security parameters of the virtual infrastructure provider change the service user has to check the parameters and security requirements again manually. The same holds if the service user wants to use the cheapest virtual infrastructure provider (see second use case). In this case the service user has to compare prices of different virtual infrastructure providers manually, check the security level of the cheaper virtual infrastructure provider manually before moving the resources, and move the virtual resources manually to the new place [4].
- The cloud networking approach helps to distribute the virtual resources flexible to different virtual infrastructure providers. The service provider takes care of optimization and harmonization of different parameters, e.g., latencies, cost, and network load. In the same way the service provider has to take care of respecting the security requirements of the service users. In the following two subsections, we first show how a service user defines security goals and how these goals are translated into security parameters. On the other hand, we show how a virtual infrastructure provider describes his security functionalities as security parameters. Second, we show the process of implementing the security requirements of a service user into the infrastructure of the virtual infrastructure provider by defining constraints on the resources of a virtual infrastructure provider.

4.1 Extraction of Security Parameters

Figure 3.1 shows the process of extracting security parameters out of security goals of a service user. In a first step the service user defines security goals for his virtual resources, E.g. Confidentiality of stored data and integrity of stored data. The service user expresses these security goals as a security policy, which is more or less a list of security requirements, e.g., containing the statement "data must be stored encrypted" [1]. This security policy is then translated into a list of security parameters. This translation step has two reasons: First, we can define a unique description language for security parameters in order to have means for comparing security requirements of a service user and security mechanisms of virtual infrastructure providers (see next section). Second, we can limit the number of potential security parameters to a list of predefined ones. E.g., a security policy saying "data must be AES encrypted" and a second policy saying "data must be encrypted" can both be described with a security parameter "encryption". This parameter might have the entries "encryption scheme" and "key length". In the first case the policy might results in "encryption scheme == AES, key length == all" and in the second case in "encryption scheme == all, key length == all". The definition of a description language is not part of this paper. Most likely the description language for security parameters will be based on XML (e.g., using VXDL) [2][4].

Using the same security parameters we want to describe the security functionality of a virtual infrastructure provider. Figure 2 shows how the security parameters are extracted from the security mechanisms installed at the virtual infrastructure provider's side. A security service (Confidentiality service) is in this case an abstraction of one or more security mechanisms (e.g., AES encryption with 256 bit key length) [3]. As can be seen in the figure there might be security parameters which do not base on a security mechanisms. This can be the case where no technical mechanism is needed to implement this parameter, e.g., location of the virtual infrastructure provider's side.

As result we now have security parameters on service user's side describing his security requirement. On the other side we have security parameters describing the security functionality of a virtual infrastructure provider.

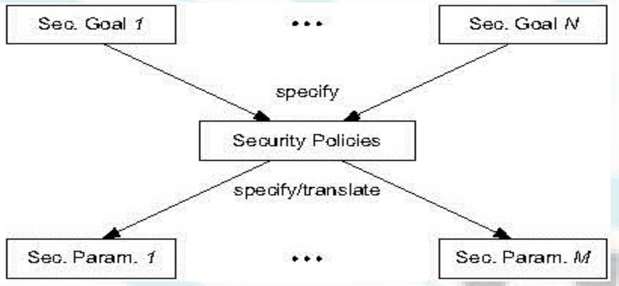

Figure 3.1: Security parameter of Service User

4.2 Approach

In the previous Section we have seen how the security parameters are extracted from the service user and from the virtual infrastructure provider. The virtual infrastructure provider needs to commit his list of security parameters de- scribing his security functionality to the service provider. The service provider stores for each virtual infrastructure provider he has contact to such a list of security parameters [1] [2]. Besides this, he also stores additional information on functionalities and available resources which is not part of this paper.

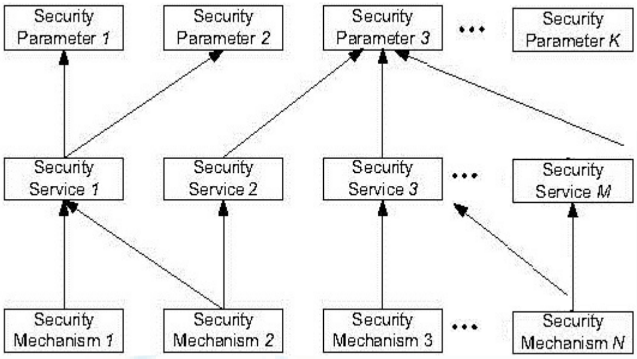

Figure 3.2: Security parameters of virtual infrastructure providers

When a service user wants to have a virtual resource, e.g., cheap storage, he sends a request to the service provider (see second use case in Section II-B). Together with the request for virtual resources he sends a list of security parameters which needs to be followed. In the next step the service provider compares these security parameters with the security parameters of virtual infrastructure providers. If a virtual infrastructure provider has at least the security functionality as requested through the security parameters by the service user the service provider might invoke virtual resources at this virtual infrastructure provider. The decision on where to place virtual resources also depends on other parameters, e.g., price, which is not part of this paper.

After the service provider has chosen a virtual infrastructure provider that fulfils the security requirements (described as security parameters) of the service user he translates the security parameters to resource constraints for the virtual infrastructure provider. This step is needed because the service user does not need all security functionalities of the virtual infrastructure provider (e.g., only AES encryption with 256 bit key length and no DES encryption) [2]. Based on these resource constraints the virtual infrastructure provider invokes security services and mechanisms (AES encryption with 256 bit key length) for virtual resources.

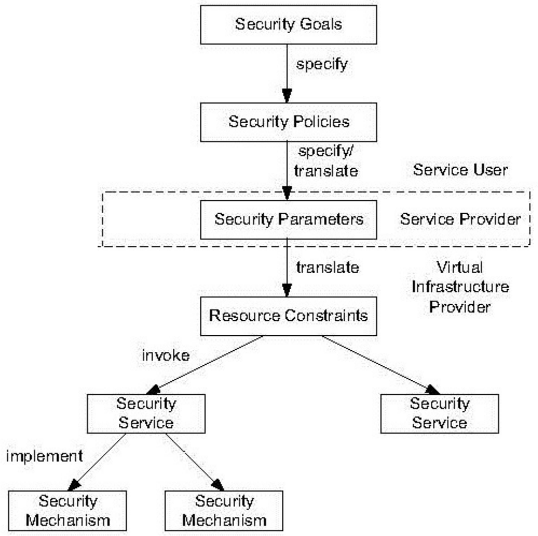

Figure 3.2.2: Security Approach

5. Architecture and Functions

The architecture and functions between the architectural elements are shown in Figure 4. This architecture consists of three functional entities: the service user, the service provider, and the virtual infrastructure provider.

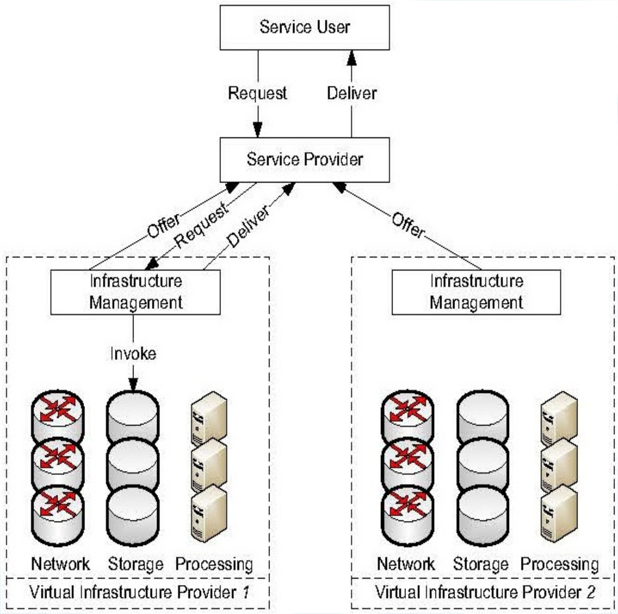

Figure 4: Architecture and Security functions

The figure shows the different functions which are used to interact between these entities. We classify the functions by the caller

5.1 Service User Functions

- Request Virtual Resources: In this simplified architecture the only function a service user can call is a request for virtual resources from the service provider. This request contains overall goals, e.g., type of resource, amount, and optimization parameters (e.g., latency demands and price), and the security goals. The security goals are transmitted in form of security parameters. The translation of security goals to security parameters will be performed at the service user side [3][4]. The translation step can be assisted by translation tools.

5.2. Service Provider Functions

- Request Virtual Resources. The service provider has also a function for requesting virtual resources. This function re- quests virtual resources from a virtual infrastructure provider. However, before sending the request to a virtual infrastructure provider the service provider maps the security parameters of the service user to the security parameters of a virtual infrastructure provider. Only if the virtual infrastructure provider provides the security functionality to fulfil the security demands of the service user the service provider is allowed to request the resources here. The request contains the same overall goals as the request function from the service user and additional security constraints which base on the security parameters of the service user [2][3].
- Deliver Virtual Resources After receiving the access to the virtual resources from the virtual infrastructure provide the service provider forwards the access to the service user. Details on access control are not part of this paper and will follow in future work [1].

5.3 Virtual Infrastructure Provider Functions

- Offers Virtual Resources and Service Functionality. The virtual infrastructure offers his virtual resources and security functionality to the service provider. How the virtual resources are offered is not part of this paper. The security functionalities are described as security parameters (see Section III-A) [1].
- Invoke Virtual Resources and Security Functionalities When the virtual infrastructure provider receives a request for virtual resources from a service provider he invokes the virtual resources and activates the requested security functionalities (see request function of service provider) [1].
- Deliver Virtual Resources After having invoked the virtual resources and security functionalities the virtual infrastructure provider sends the access to the virtual resources to the service provider [2].

6. Conclusion

We presented a security architecture for cloud networking. This architecture helps in preserving the security goals of service users while at the same time benefiting from the flexible and dynamic placement of virtual resources at different virtual infrastructure providers. Key concepts of this architecture are the definition of unique security parameters for expressing security requirements and security functionality, the translation of security parameters in security constraints, and the management of service users and virtual infrastructure providers by service providers.

7. Future Enhancement

As further steps we plan to include the security functionality in the SAIL prototype. We plan to extend the architecture by auditing techniques so that a service user and a service provider are able to verify that a security constraint is followed by a virtual infrastructure provider. Furthermore, we plan to establish access control mechanisms for accessing virtual re- sources and making the flexible nature of the cloud networking infrastructure transparent for the service user.

References

[1] http://docs.google.com
[2] http://code.google.com/appengine
[3] http://aws.amazon.com/ec2/
[4] http://www.sail-project.eu/ss

Author Profile

P Ramesh Naidu received the B.E and M.Tech degree in Computer Science and Engineering from JNTU, Hyderabad. He is having a work experience of 8 years in Teaching and 1year in Industry. SCJP Certified by Sun Microsystems.

Yerriswamy T received B.E degree in Computer Science & Engineering and M. Tech degree in Computer Networks and Engineering from VTU, Belgaum. Having work experience of 5years in teaching.

Ashwath K received B.E degree in Computer Science & Engineering from VTU Belgaum and M.S degree in Embedded Systems from Manipal University, Manipal. Having work experience of 1year in teaching and 1year in industry.