IFERP
connecting engineers... developing research

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 8, August 2018

Three Tier Security Architecture for Cloud Networking

[1] Manjunath D R, [2]Shiva Sumant Reddy, [3]Anil Kumar B
[1][2][3] Assistant Professor,Department of computer science, DSATM, Bengaluru.

Abstract: The Cloud Computing calculate the duty to distribute on the resource pool which the massive computers constitute, enables each kind of application system according to need to gain the computation strength, the storage space and all kinds of software service. Cloud computing offers reduced capital expenditure, operational risks, complexity and maintenance, and increased scalability while providing services at different abstraction levels, namely Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), and Infrastructure-as-a-Service (IaaS). However, when networking aspects for distributed clouds are considered, there is little support and the effort is often underestimated. A new approach called cloud networking adds networking functionalities to cloud computing and enables dynamic and flexible placement of virtual resources crossing provider borders. This allows various kinds of optimization, e.g., reducing latency or network load. However, this approach introduces new security challenges. Cloud networking aims at providing on-demand elastic network services to connect existing data centre based cloud infrastructures across wide area networks. This paper presents new the cloud networking Architecture and presents a security architecture that enables a user of cloud networking to define security requirements and enforce them in the cloud networking infrastructure

Keywords: cloud computing, cloud networking, network virtualization, infrastructure as a service, inter-provider Virtual Infrastructure, resource management, cloud network security

I. INTRODUCTION

One of the most appealing aspects of cloud computing is its elasticity, which provides an illusion of infinite, on-demand resources This elasticity provides an attractive environment for highly-scalable multi-tiered applications. However, this can create additional challenges for back-end transactional database systems, which were designed without elasticity in mind. 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).

The vision of Cloud Networking (CLoNe) is to fully realize the potential of networking in the cloud computing paradigm. More specifically, CLoNe aims at providing cloud network services compliant to application requirements in a dynamic and automated way connecting customers to the cloud and connecting different parts of the infrastructure, i.e., geographically distributed data centres. Considering the current state of the technology, this is achievable by enabling the co-existence of legacy and new networks via virtualization of resources and by fully integrating networking services with existing cloud computing services. CLoNe embraces legacy networks by creating an abstraction layer where those network services can be encapsulated. CLoNe can dynamically expand usage of resources integrating performance and fault monitoring for dynamic resource allocation. The CLoNe solution is able to connect private networks and infrastructures together across provider boundaries and technology boundaries. More specifically, the primary objective of building the CLoNe architecture proposed by SAIL is to define roles, responsibilities, interfaces, and a reference model for deploying complex applications over multiple, heterogeneous, multi-operator computing and storage clouds.

Unfortunately, this flexible placement of virtual resources introduces new challenges regarding security [5]. 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. 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.

In the following Section we show how the security functions are added to the cloud network architecture and define functions that are needed to interact between architectural components. Afterwards, we give an overview on related work that is relevant for securing CLoNe. The last Section concludes the work and shows further working directions

II. ROLES AND USE CASES

In this section we introduce the terminology for CLoNe as used in this paper. This consists of roles and actors in this environment. Furthermore, we show example use cases for CLoNe to illustrate these roles and show the basic functionality of CLoNe.

A. ROLES

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

- ***Tenant*** participates in a business relationship with an infrastructure service provider in which the tenant agrees to pay for the provision of virtual infrastructure.
- ***Infrastructure Service User*** accesses a virtual infrastructure service in order to obtain, examine, modify and destroy resources owned by a tenant.
- ***Infrastructure Service Provider*** offers an infrastructure service to tenants that may be accessed by infrastructure service users to obtain, examine, modify and destroy resources.
- ***Administrator or Virtual Infrastructure Provid***er has administrative authority over underlying virtual or physical equipment (the administrative domain) used to implement virtual resources.

B. USE CASE

Cheap Processing and Storage: In this use case we consider a infrastructure 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 infrastructure 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 infrastructure 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 infrastructure service users and virtual infrastructure provider) or diversity in prices for energy (smart grid).

III. CLONE ARCHITECTURE OVERVIEW

This Section describes the CLoNe architecture at a conceptual level. The architecture is organized according to the four layers depicted in Figure 3.1. The resource layer is concerned with virtualization of underlying equipment to implement individual virtual resources. The intra-provider layer deals with organization and coordination of virtual infrastructures within a single infrastructure service provider.

The inter provider layer is concerned with coordination that has to occur between providers where they collaborate to interconnect virtual infrastructures. The service layer renders the virtual infrastructure service itself and accommodates business relationships among the actors.

The colours of the infrastructure service providers and administrative domains represent the same actor operating in each layer. As can be seen from Figure 3.1 not all infrastructure service providers have an administrative domain or appear in the lower layers. The inter-provider and service layers may contain providers whose sole purpose is to coordinate virtual infrastructures implemented by other providers and to cooperate in presenting them as a service for tenants.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 8, August 2018

Non-collaborative infrastructure service providers, such as those that exist today, also fit in this architecture, but would be absent from the inter provider layer. Such providers operate in isolation and do provide service, but do not interact with their peers to coordinate their services. This case is not shown.

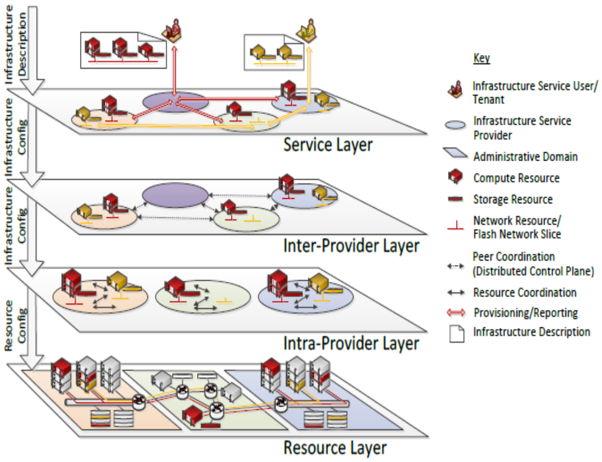

Figure 3.1: CLoNe Architectural overview

Non-collaborative infrastructure service providers, such as those that exist today, also fit in this architecture, but would be absent from the inter provider layer. Such providers operate in isolation and do provide service, but do not interact with their peers to coordinate their services. This case is not shown.

CLoNe also extends the infrastructure service functions to enable collaboration among service providers. This service model is implemented by the service layer.

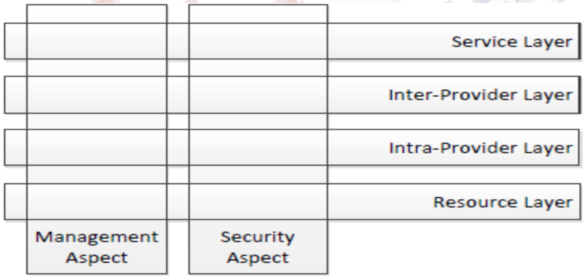

Figure 3.2: Management and security aspects occur in each layer of the architecture

Management and security aspects cut across all layers of the architecture as shown in Figure 3.2.Each intersection between management or security aspects and an architecture layer represents functions implemented in different interfaces or with a different scope of control. The functions come together within each aspect to provide coherent operation of the service. The extensions to the service model, the infrastructure description, the architecture layers, and the management and security aspects are described in the remainder of this chapter. The subsequent chapters describe concrete implementations developed in prototypes of the architecture.

IV .ARCHITECTURAL LAYERS

The layers of the architecture build on each other's functionality from the bottom up. They are described in that order in the following.

A. RESOURCE LAYER

The primary role operating in the resource layer is the administrator. The layer deals with individual control of virtual resources within a single administrative domain. The virtual resources can be individually identified, assigned certain properties, and have runtime status. They may also have links to other virtual resources that are managed separately, for example, a virtual machine might be linked to a virtual network and a storage volume.

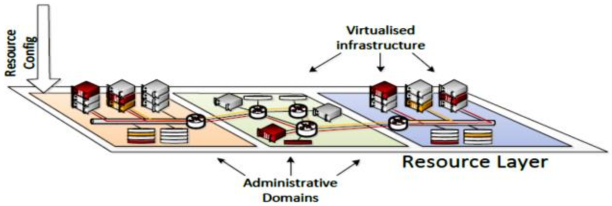

Figure 4.1: The Resource Layer

B. INTRA-PROVIDER LAYER

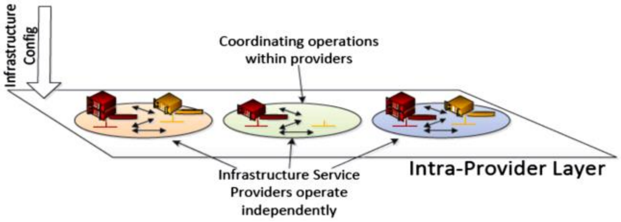
Infrastructure Config
Coordinating operations within providers
Intra-Provider Layer
Infrastructure Service Providers operate independently

Figure 4.2: The Intra-Provider Layer

The primary role in the intra-provider layer is the infrastructure service provider, which also directs actions carried out in the administrator role at the resource layer. The intra-provider layer deals with collective control of multiple virtual resources within a single administrative domain. The links among these virtual resources determine the topology of the infrastructure and constrain their combined management behaviour.

At this layer the mapping between the virtual infrastructure and the underlying equipment can be determined. This mapping can take into account group allocation (all or nothing allocation of a collection of virtual resources) and optimal placement (relative placement of virtual resources or use of underlying infrastructure). For example a VM could be placed in a location with optimal network performance relative to a given end user. Some technology selections can be made at this layer. A virtual machine could be executed on a choice of different servers with different memory sizes or chip sets giving different performance trade-offs; a disk volume could be placed on local storage or network attached storage; a network link could be mapped to an isolated VPN tunnel or an open shared network.

C. INTER-PROVIDER LAYER

The correct operation of a virtual resource may depend on the status of resources it is linked to; however, its management subsystem may not have visibility of the linked resource if it is managed by a different subsystem. This level of coordination is outside the scope of the resource layer.

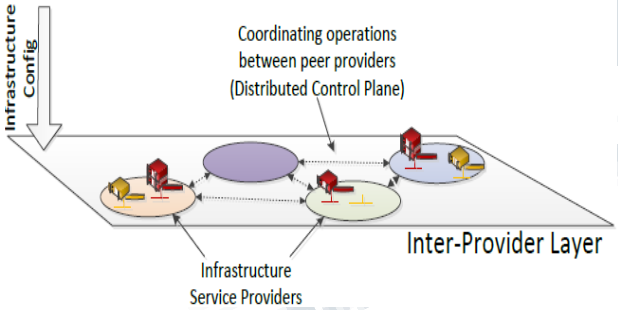

Figure 4.3: The Inter-Provider Layer

The primary role in the inter-provider layer is the infrastructure service provider, with multiple providers interacting across their administrative boundaries as peer groups. The layer deals with collective control of multiple virtual resources across multiple administrative domains. An inter-provider infrastructure is the composition of multiple intra-provider infrastructures. An intra-provider infrastructure may contain virtual resources that have links with virtual resources in other intra-provider infrastructures, thus connecting the virtual infrastructures and determining the topology of the inter-provider infrastructure

Distributed Control Plane

The Distributed Control Plane (DCP) describes a category of protocols, interfaces and control operations within the inter-provider layer that enable two or more infrastructure service providers to interact and exchange information

C. Service Layer

The main roles operating in the service layer are the infrastructure service user and the infrastructure service provider. The tenant also has an important role in this layer as the root of authorization for an infrastructure service user to act.

The CLoNe infrastructure service is implemented by a set of interfaces and functions that enable the creation, monitoring and management of virtual infrastructures, including automatic delegation and collaboration across providers.

Tenant registration

Tenant registration refers to the process of a tenant establishing a business relationship with an infrastructure service provider. This may be an automatic process

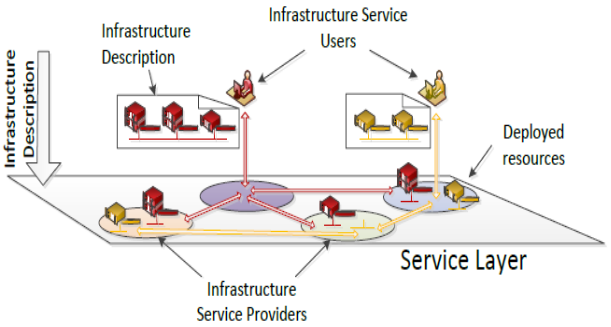

Figure 4.4: The Service Layer

The CLoNe infrastructure service is implemented by a set of interfaces and functions that enable the creation, monitoring and management of virtual infrastructures, including automatic delegation and collaboration across providers.

Tenant registration

Tenant registration refers to the process of a tenant establishing a business relationship with an infrastructure service provider. This may be an automatic process, in which a tenant discovers a provider's capabilities and programmatically registers as a customer. Equally, it may be a manual process.

Infrastructure Service

The infrastructure service interface is implemented by each infrastructure service provider. Users interact with a single provider to deploy and manage a virtual infrastructure under the authorization of a tenant of that provider. Infrastructure service requests are performed using a high-level description language based on the information model described above

V. 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 use case of Section II if the infrastructure service user wants to use the cheapest virtual infrastructure provider. In this case the infrastructure 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. The cloud networking approach helps to distribute the virtual resources flexibly to different virtual infrastructure providers. The infrastructure service provider takes care of optimization and harmonization of different parameters, e.g., latencies, cost, and network load. In the same way the infrastructure 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 infrastructure 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 infrastructure service user into the infrastructure of the virtual infrastructure provider by defining constraints on the resources of a virtual infrastructure provider.

A. EXTRACTION OF SECURITY PARAMETERS

Figure 5.1 shows the process of extracting security parameters out of security goals of a infrastructure service user. In a first step the Infrastructure service user defines security goals for his virtual resources e.g., confidentiality of stored data and integrity of stored data. The infrastructure service user expresses these security goals as a security policy, which is more or less a list of 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". 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 infrastructure service user and security me chanisms 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 [6,11]). Using the same security parameters we want to describe the security functionality of a virtual infrastructure provider. Figure 5.2 shows how the security parameters are extracted from the security mechanisms installed at the virtual infrastructure provider's or administrator domain 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). 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

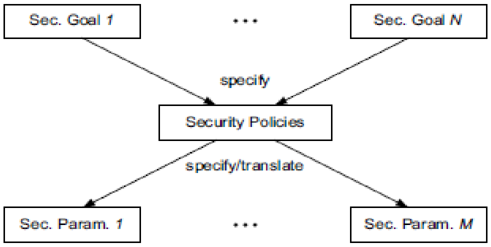

Figure 5.1: Security parameters of Infrastructure Service User

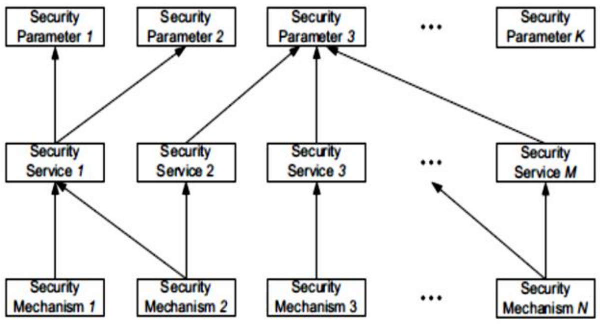

Figure 5.2: Security parameters of Virtual Infrastructure Provider or Administrator domain.

B. VXDL AS A LANGUAGE FOR HIGH-LEVEL GOALS

VXDL is a unifying modelling language for describing virtual infrastructures, which defines a simple grammar for enabling a high-level representation of both the diversity of virtual resources (e.g., nodes, routers, access-points, links, storage) and the constraints attached to them (e.g., capacity and performance attributes, reliability and security levels, geo-location of resources, network topology).

The state of the art with respect to defining elasticity rules and providing for automated scalability [6,11] considers only scaling arrays of virtual machines up and down, according to some metrics. These metrics are usually related to CPU, memory, storage and network activities. Scaling arrays of VMs up and down are only part of the elastic provisioning. Moreover, considering VMs as the granularity unit for scaling virtual infrastructures can lead to a waste of capacity for both user and provider. By considering elasticity on network resources as well as computing resources, the approach extends the state of the art to a more fine-grained mapping of user requests to resource allocation. For the purpose of meeting the challenges of CLoNe, it was identified that VXDL must be ensured to be able to express constraints on the following elements:

Resource capacities: (e.g. CPU, memory, storage, bandwidth configuration).

Scaling virtual elements: the virtual array element also get a interval [MIN, MAX] to specify the limits in terms of elements inside the array.

Latency: the latency attribute also gets a [MIN, MAX] interval but its meaning is slightly different from the other attributes.

Application performance and metrics: by using the TAGS system (a triplet composed of a key, a type and a value), a user can identify metrics that should be monitored during the execution.

D. APPROACH

In the previous Section we have seen how the security parameters are extracted from the infrastructure service User and from the virtual infrastructure provider. The virtual infrastructure provider needs to commit his list of security parameters describing his security functionality to the infrastructure service provider. The infrastructure service provider stores for each virtual infrastructure provider he has contact to such a list of security parameters. Besides this, he also stores additional information on functionalities and available resources which is not part of this paper. When a infrastructure service user wants to have a virtual resource, e.g., cheap storage, he sends a request to the infrastructure service provider. Together with the request for virtual resources he sends a list of security parameters which needs to be followed. In the next step the infrastructure service provider compares these security parameters with the security

A. Infrastructure Service User Functions

Request Virtual Resources This request contains overall goals, e.g., type of resource, amount, and optimization parameters (e.g., latency demands and price), and the security goals.

B.Infrastructure Service Provider Functions

Request Virtual Resources The infrastructure service provider has also a function for requesting virtual resources. This function requests virtual resources from a virtual infrastructure provider. However, before sending the request to a virtual infrastructure provider the infrastructure service provider maps the security parameters of the infrastructure 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 infrastructure 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 Deliver Virtual Resources After receiving the access to the virtual resources from the virtual infrastructure provider the infrastructure service provider forwards the access to the infrastructure service user.

Details on access control are not part of this paper and will follow in future work.

C. Virtual Infrastructure Provider Functions

Offer Virtual Resources and Security Functionality The virtual infrastructure offers his virtual resources and security functionality to the infrastructure service provider. How the virtual resources are offered is not part of this paper. The security functionalities are described as security parameters.

Invoke Virtual Resources and Security Functionalities When the virtual infrastructure provider receives a request for virtual resources from security parameters of the infrastructure service user. parameters of virtual infrastructure providers. If a virtual infrastructure provider has at least the security functionality as requested through the security parameters by the infrastructure service user the infrastructure 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 infrastructure 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). Based on these resource constraints the virtual infrastructure provider invokes security services and mechanisms (AES encryption with 256 bit key length) for virtual resources.

VI. SECURITY ARCHITECTURE AND FUNCTIONS

This section describes the CLoNe security architecture which integrates the security requirements and goals described above the security architecture provides quantifiable security levels within the CLoNe infrastructure. This ensures that all the CLoNe entities obtain a better view of real-time security levels of the service provisioning infrastructure. The security goal translation function forms the backbone of the CLoNe security architecture. The architecture and functions between the architectural elements are shown in Figure 6.1 and the interaction between security functions is shown in Figure 6.2. This architecture consists of three functional entities: the infrastructure service user, the infrastructure service provider, and the virtual infrastructure provider. The figure shows the different functions which are used to interact between these entities. We classify the functions by the caller a infrastructure service provider he invokes the virtual resources and activates the requested security functionalities (see request function of service provider).

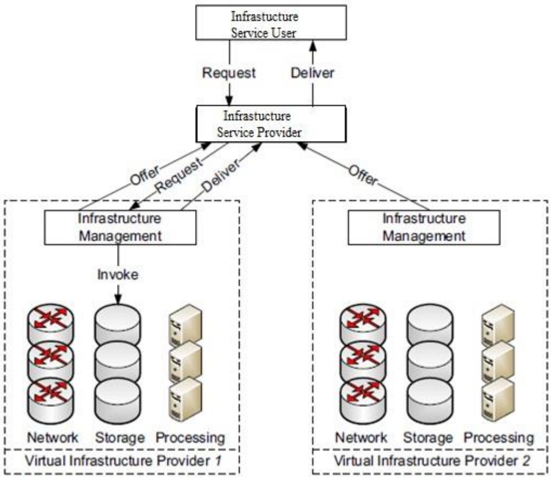
Infrastucture Service User
Request
Deliver
Infrastucture Service Provider
Offer
Request
Deliver
Offer
Infrastructure Management
Invoke
Infrastructure Management
Network
Storage
Processing
Virtual Infrastructure Provider 1
Network
Storage
Processing
Virtual Infrastructure Provider 2

Figure 6.1: CLoNe Security Architecture

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 infrastructure service provider.

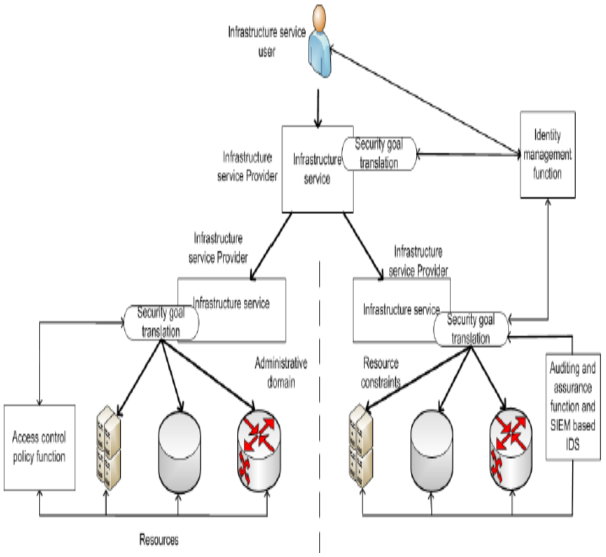
Infrastructure service user
Infrastructure service Provider
Infrastructure service
Security goal translation
Identity management function
Infrastructure service Provider
Infrastructure service Provider
Infrastructure service
Security goal translation
Infrastructure service
Security goal translation
Administrative domain
Resource constraints
Access control policy function
Auditing and assurance function and SIEM based IDS
Resources

Figure 6.2: Interaction between Security Functions

D. Utilization

We show the utilization of the security architecture and its functions by applying it to the second use case Section where a infrastructure service user is interested in cheap processing and storing resources. In a first step the virtual infrastructure providers VP1 and VP2 offer virtual resources and security functionality to a infrastructure service provider (see Figure 4). VP1 offers storage resources and provides AES encryption with maximum key length of 256 bit as security functionality (security parameter). VP2 also offers storage resources and provides DES encryption with 56 bit key length as security functionality. The infrastructure service user SU sends a request for virtual resources to the infrastructure service provider. SU asks for 100GB of storage that is AES-encrypted with at least 128 bit key length (security parameter). The infrastructure service provider now detects that only VP1 offers the adequate encryption for the request of SU. For that reason the infrastructure service provider sends a request to VP1 for 100GB of storage that is AES encrypted with 128 bit key length (resource constraint).

VP1 invokes the virtual resource by allocating 100GB of storage, encrypting the storage with AES and 128 bit key length, and delivering the access to the virtual resource to the infrastructure service provider. The infrastructure service providers forward the access to SU.

VII. CONCLUSIONS

In this paper 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 or 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.

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 resources and making the flexible nature of the cloud networking infrastructure transparent for the service user.

Additionally, the ability to deploy services across and within networks, as a way to take advantage of network proximity to customers and their (potentially mobile) end users, is developing as a means to support on- demand services from bulk-data transfer, to streaming media and on-line gaming. It is clear that the concepts and mechanism developed in the CLoNe architecture enable real business needs of cloud computing to be met in the on-going evolution of the Internet

REFERENCES

[1] "Google Docs," July 2011. [Online]. Available: http: //docs. google .com

[2] "Google App Engine, "July 2011. [Online]. Available: http://code.google.com/appengine/

[3] "Amazon Virtual Private Cloud," July 2011. [Online]. Available: http :// aws. amazon. com ec2 /

[4] The SAIL project web site. http://www.sail-project.eu/.

[5] Volker Fusenig and Ayush Sharma. Security architecture for cloud networking. In Computing,Networking and Communications (ICNC), 2012 International Conference on, pages 45-49, 30 2012-feb. 2 2012.

[6] G. P. Koslovski and P. V.-B. Primet, "Vxdl: Virtual resources and interconnection networks description language," Engineering, pp.138–154, 2009. [Online]. Available: http:// www. springerlink. com/index/N131016226414516.pdf

[7] A. Streitberger, W. Ruppel, "Cloud computing security protection goals, taxonomy, market review," Institute for Secure Information Technology SIT, Tech. Rep., 2010.

[8] S. D. C. d. Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, G. Pelosi, and P. Samarati,

"Encryption-based policy enforcement for cloud storage,"in Proceedings of the 2010 IEEE 30th International Conferenceon Distributed Computing Systems Workshops, ser. ICDCSW '10.Washington, DC, USA: IEEE Computer Society, 2010, pp. 42–51. [Online]. Available: http: // dx. doi. org/ 10.1109 /ICDCSW. 2010.35

[9] CloudAudit, June 2012. http://cloudaudit.org/

[10] "Intel virtualization," July 2011. [Online]. Available: http://www.intel. com/ technology/ virtualization/

[11] Guilherme Koslovski, Pascale Vicat-Blanc Primet, and Andrea Schwertner Char~ao. VXDL:Virtual Resources and Interconnection Networks Description Language. In The Second International Conference on Networks for Grid Applications (GridNets 2008), Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering,Beijing, China, Oct. 2008. Springer Berlin Heidelberg.

[12] "AMD Virtualization (AMD-V) Technology," July 2011. [Online]. Available: http:/ /sites .amd.com /us/business/it-solutions /virtualization /Pages/amd-v.aspx