# Self-protecting multi-cloud applications

Antonio M. Ortiz[1], Erkuden Rios[2], Wissam Mallouli[1], Eider Iturbe[2], Edgardo Montes de Oca[1]
[1] Montimage R&D. Paris, France
Email: {antonio.ortiz, wissam.mallouli, edgardo.montesdeoca}@montimage.com
[2] ICT Division, Fundacion Tecnalia Research & Innovation. Derio, Spain
Email: {erkuden.rios, eider.iturbe}@tecnalia.com

***Abstract*—The rise and variety of cloud services and their growing availability has enabled the creation of multi-cloud applications that take advantage of cloud service combinations. These applications need to avoid security breaches and preserve data integrity and user privacy in the whole service composition. The MUSA framework arises as a global solution to support the security of the whole multi-cloud application lifecycle by providing advanced monitoring and security assurance mechanisms in multi-cloud environments. The MUSA security assurance platform will be offered as Software as a Service and will include monitoring, enforcement, and notification services to make the multi-cloud applications more secure than ever, ensuring the satisfaction of all the involved actors.**

## I. Introduction

The emerging new business models based on cloud solutions make cloud-based systems one of the most promising technologies for the coming years. As stated in [1], cloud computing initiatives are the most important project for the majority of IT departments today (16%), and are expected to cause the most disruption in the future.

One of the most challenging applications in heterogeneous cloud ecosystems are those that are able to maximise the benefits of the combination of the cloud resources in use: multi-cloud applications, that can be described as distributed applications over heterogeneous cloud resources whose components are deployed in different cloud service providers and still they all work in an integrated way and transparently for the end-user. The use of multi-cloud solutions adds value to the overall cloud client experience [2].

However, security is considered by enterprises as the first inhibitor to cloud adoption, mainly because of the difficulty in evaluating the trade-off between the benefits obtained when using this technology, and the implicated security risks and privacy issues that it might bring [3]. Moreover, the traditional three service models (IaaS, PaaS, SaaS) defined by the NIST [4] are being extended by new models such as Network as a Service (defined by the ITU-T [5]) or Data as a Service [6].

Securing multi-cloud applications needs to deal with two levels of security: (i) individual components, including security primitives to avoid compromising the security of the whole system and, (ii) communications and data flows, to protect data exchange among different application components (e.g., encryption).

The MUSA project [7] arises as a joint effort of European Commission and private companies to define, implement and test the MUSA framework, that will provide a solution to solve security issues in multi-cloud applications. It will address the need for self-protection against cyber-incidents and provide Cloud Service Providers with the privacy and security-awareness they need.

The MUSA project represents the core of this paper. It is carried out in the context of the EU Horizon 2020 objectives to support the life-cycle of multi-cloud self-protective applications. MUSA aims at ensuring the security in all multi-cloud environments by combining (i) a preventive security approach, promoting security by design practices in the development and embedding security mechanisms in the application, and (ii) a reactive security approach, monitoring application runtime to mitigate security incidents, so multi-cloud application providers can be informed and react to them without losing end-user trust in the multi-cloud application.

The remainder of this paper is organised as follows: Section II introduces related work; Section III explains why security monitoring is important; Section IV presents the MUSA approach and its main innovations; and, Sections V and VI conclude by explaining the open challenges and the future work planned.

## II. Related work

Cloud systems have limited awareness of the applications they are running and applications have little or no awareness of what is going on in the cloud. Distributing applications or data in multi-cloud environments hamper performance requirements [8] and introduce new security challenges. The work in [9] identifies particular vulnerabilities involved in different cloud deployment models. Multi-cloud environments can sometimes be used to improve security (e.g., using data deduplication, ensuring codes and proof-of-possession techniques proposed by [10]) but these techniques also introduce new vulnerabilities. Cloud security-oriented models try to address security aspects, such as the Cloud Security Alliance Security Stack [11] and Jericho Forum Security Cube Model [12], that define different levels that identify threats and mitigation from a business perspective. But these approaches have a static vision of security that does not fit well in a multi-cloud adaptive security deployment context [13].

To overcome these limits, [13] proposes taking advantage of [14] to generate and deploy service-related policies that will be used to take into account non-functional requirements (as security and quality of service) while deploying and monitoring service oriented systems over a multi-cloud infrastructure.

This allows rising the abstraction level and introducing more automation in software development, improving re-usability of requirements, platform-independent models and parts of platform-specific models depending on the deployment platform. Moreover, Model-Driven Engineering is also adapted for defining Model-Driven Security (MDS) strategies [15]. MDS defines a framework used to generate security policies out of annotated business process models. This approach requires enriching the traditional XaaS layer model with a Business as a Service level, used to express business-dependant performance and security requirements. This approach modifies and increases the complexity of the standard model.

Several EU research projects, such as SeaClouds [16], Cloud4SOA [17], etc., do not specifically address multi-cloud security. Others, such as SPECS [18] propose a Security-as-a-Service solution based on monitoring Service-Level Agreements (SLAs). In MUSA the specification and enforcement of security is also based on SLAs: the security properties are specified in the application SLAs and the monitoring and enforcement mechanisms are aligned to them.

On the one hand, there are several commercial products that support the Cloud-based Application Performance Monitoring (CAPM) [19]. These solutions are focused in SLA-based performance monitoring, concerning QoS. However, the security properties monitoring (e.g., data encryption, access control, etc.) is not addressed by this kind of approach. Examples of such solutions are: AppDynamics APM [20], CA APM [21], and IBM APM [22].

The CAPM concept can be combined with the cloud resource performance monitoring, but they are different concepts. Cloud resource monitoring is concerned with CPU, disk and memory utilisation; i.e., it is related to the provisioned cloud resource by the application provider. There are some cloud standards (such as OCCI [23] and CIMI [24] for cloud infrastructure management and CDMI [6] for data management and Cloud Application Management for Platforms (CAMP) [25] for cloud platform management) that specify interfaces for the cloud consumer that can be invoked in order to monitor some cloud resource metrics. But the decision as to when and how the cloud consumer (the multi-cloud application provider) must be informed remains a prerogative of the cloud service provider.

The approaches present in the current state of the art do not provide any satisfactory solution that can be considered cost-efficient and offering enough control for enforcing security policies in multi-cloud environments at different levels (e.g., at the business process, service and network levels).

## III. The Need for Monitoring and Enforcement in Multi-Cloud Environments

Multi-cloud application solutions have to deal with the security of the individual components as well as with the overall application security including the communications and the data flow between the components. Even if each of the cloud service providers offers its own security controls, the multi-cloud application has to ensure integrated security across the whole composition. Therefore, the overall security depends on the security properties of the application components, which in turn depend on the security properties offered by the cloud resources they exploit.

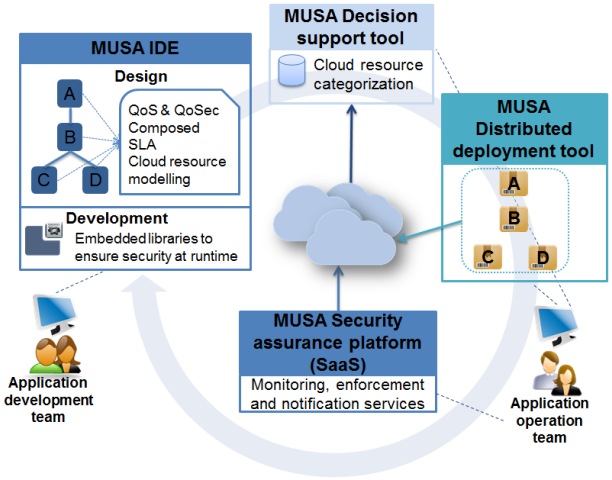


Figure 1. MUSA overall concept

To reach the required security, there is a need to combine preventive security approaches with reactive ones. The coordination of these two approaches in the application life-cycle management is needed in order to ensure that the preventive oriented security is embedded and aligned with the reactive security measures in the context of potential SLA violations.

The basic idea is to provide a security assurance platform in form of a SaaS that allows supporting multi-cloud application run-time security control and transparency by offering services for: a) continuous monitoring of the security behaviour of the application components and the cloud resources they exploit; b) security enforcement mechanisms, such as authentication, data signature and encryption; and, c) notification of security incidents to the application provider.

## IV. The MUSA Approach

The self-protection character of multi-cloud applications can be translated into ability of being able to adapt and reconfigure at run-time whenever a security incident happens in one of the application components or in any of the underlying cloud services in use. In order to achieve such self-protection, the MUSA project proposes an integrated framework to support the security-intelligent life-cycle management of multi-cloud applications based on DevOps (Development and Operation) approach. The MUSA framework includes a number of tools described in Table I and depicted in Fig. 1.

The MUSA security assurance platform ensures the security of the whole application distributed across heterogeneous cloud providers. It will be offered as-a-service to the application providers integrating the following services:

1) **MUSA monitoring service**: to evaluate the security and functional measures gathered over the multi-cloud application and the cloud resources it exploits.

| Title | Description |
|---|---|
| MUSA Integrated Development Environment (IDE) | An IDE to support the design of the breakdown/composition of multi-cloud applications based on the security requirements over the cloud resources (of CSPs) to be provisioned and over the application itself. |
| MUSA security libraries | A set of libraries embedded in multi-cloud application components that allow to link the data with their security requirements through the programming model of the multi-cloud application following a non-intrusive approach. |
| MUSA decision support tool | A DevOps oriented tool supporting the selection of the adequate combination of cloud services (and their providers) where the application components will be deployed, balancing security (QoSec), business (costs) and functional requirements (QoS). |
| MUSA distributed deployment tool | A DevOps oriented tool that allows the automated distributed deployment and re-deployment of the multi-cloud application components to multiple cloud providers. |
| MUSA security assurance platform (SaaS) | This platform is composed of MUSA monitoring, MUSA enforcement and MUSA notification service and takes profit of the joint outcome providing a holistic security assurance at runtime for multi-cloud applications. |

Table I. TOOLS INCLUDED IN THE MUSA FRAMEWORK

2) **MUSA enforcement support service** ollaborates with the MUSA security libraries (see Table I) to enforce the security of multi-cloud application components.
3) **MUSA notification service** in charge of sending the alerts to the application provider when relevant security incidents have been detected.

All these three services will be implemented as cloud services, all of them working together with the MUSA embedded security libraries.

### A. *Security monitoring*

Monitoring will rely on the use of multiple mechanisms such as standard APIs offered by the cloud provider or the MUSA security libraries. Furthermore, it is able to trigger security alerts based on the event rules defined by the application operation team. The monitoring solution will be innovative as it proposes a vendor independent open-source solution, centred on security and dependability assurance, which can be easily used by applications by defining security SLAs.

The monitoring will also rely on different technologies (i.e., DPI, data mining) that will allow it to perform metrics at different levels and analyse the information using statistics and machine learning algorithms that can be dynamically deployed in multi-cloud environments. It introduces formal specifications of the properties to detect, the detection algorithms to use and the actions to trigger. In this way, it becomes an essential element to obtain resilient self-healing cloud-based applications and enable building solutions for security monitoring, auditing, forensics and incident response that, furthermore, provide user situational awareness.

The monitoring methods and tools implemented in MUSA will use and extend the Montimage Monitoring Tool (MMT) developed by Montimage in SHIELDS [14] and Inter-Trust [26]. It is composed of three complementary but independent modules as shown in Fig. 2.

- MMT-Extract is the core packet processing module. It analyses network traffic to identify network and application-based events by using Deep Packet/Flow Inspection (DPI/DFI) techniques. It also allows analysing any structured information generated by applications. MMT-Extract incorporates a plugin architecture for the addition of new input formats, and a public API for integration into third party probes.
- MMT-Security is a security analysis engine based on MMT-Security properties. It analyzes and correlates network and application events to detect operational and security incidents. A set of security properties for SLAs checking has been specified in MMT to analyse their respect by the multi-cloud based application.
- MMT-Operator is a visualization application for MMT-Security currently under development. It allows collecting and aggregating security incidents to present them via a graphical user interface. MMT-Operator is conceived to be customizable, i.e., the user will be able to define new views or customize them.

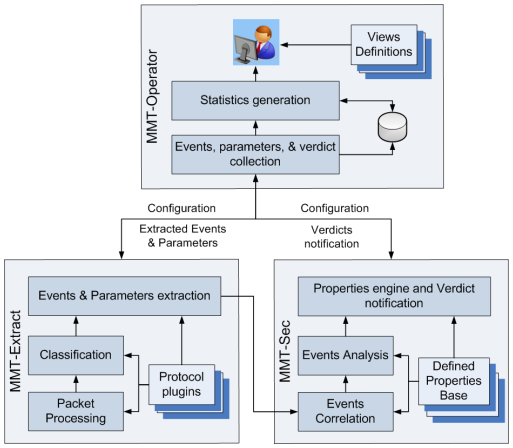


Figure 2. MMT global architecture.

In the context of MUSA, MMT tool has been adapted to be deployed in multi-cloud environments. MMT is included in the software image of the virtual machine and it is thus automatically initiated when instantiating each virtual machine

running an application component with no further configuration needed.

This solution offers the best performance in terms of security. Here, the processing power and memory required are distributed among the virtual machines. Despite of the individual probes installed on each virtual machine, there is the need of a global monitoring coordinator that supervises the monitoring tasks of each probe installed on each virtual machine. For this, each probe must be able to directly interact with any other probe, as well as with the monitoring coordinator. Local decisions can be taken by the individual monitoring probes installed on each virtual machine, and the monitoring coordinator can perform coordination, orchestration and complex event detection.

Figure 3 represents a possible deployment scenario for MMT in a multi-cloud environment where each virtual machine is running an application component. As depicted, MMT probes capture performance and security meta-data from each virtual machine, and are able to perform countermeasures to mitigate attacks and security risks. MMT probes have P2P communication capabilities to share relevant information with the aim of increasing the efficiency of the security mechanisms and, thus, ensure the correct operation of the whole system.

To perform coordination and orchestration of the whole monitoring system, a central MMT Operator will receive information from the distributed MMT probes. The MMT Operator is also in charge of correlating events to create reports to inform network managers of the system activities, attacks avoided and countermeasures taken. Furthermore, it will be able to globally analyse the information provided by individual MMT probes with the ultimate objective of detecting complex situations that may compromise the system.

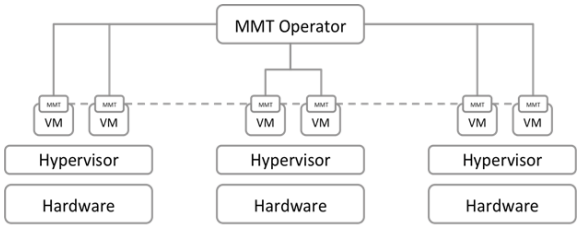


Figure 3. MMT deployement in multi-cloud environments.

### B. Security enforcement

The security requirements definition and their compliance assurance by MUSA are focused on data protection addressing the following security objectives: data confidentiality, data integrity, data localisation and data access. These are in line with the major security objectives related to cloud computing identified by the Cloud Standards Coordination Working Group within the European Cloud Computing Strategy [27]: (i) protect data from unauthorised access, disclosure and modification, (ii) prevent unauthorised access to cloud computing resources, (iii) ensure effective governance, control and compliance processes are in place, (iv) ensure appropriate security provisions for cloud applications, (v) ensure security of cloud connections and networks, and (vi) enforce privacy policies.

Moreover, as the security management of multi-cloud applications cannot be approached in isolation, it has to be balanced with functional and business features such as availability, scalability, performance, or pricing models.

### C. Incident notification

When a security incident is detected, or when the application is at risk of not fulfilling its SLA, it becomes vital that this be notified to the application provider in order to trigger the necessary preventive measures that will keep the required security parameters well balanced with the performance margins specified in the SLA. For instance this could be done by redeploying application components across a different combination of cloud resources. In this way, the application provider can rapidly react to possible security breaches.

### D. Major innovations of MUSA security assurance

The main contributions and advances of the monitoring approach introduced by MUSA can be summarised as follows:

- Integrated multi-cloud application performance and security monitoring tools, beyond the CAPM concept including security aspects.
- A twofold security management mechanism: (i) overall application security assurance and, (ii) cloud resource security and performance monitoring.
- Run-time assurance controls and mechanisms that exploit the DevOps paradigm for the seamless integration with design mechanisms so the security assurance at application operation is smoothly aligned with security controls introduced at design time (security-by-design).
- Continuous monitoring and enforcement of overall security at runtime, including those security properties impacted by the behaviour of the used cloud resources.
- Security enforcement mechanisms, such as authentication, data signature and encryption.
- Notification of security incidents to the application provider.

## V. Open challenges

When designing, deploying and testing monitoring solutions in multi-cloud environments, there are a number of challenges that must be considered so that the monitoring mechanisms do not interfere with the normal operation of the system, yet perform well when detecting the required metrics.

The main challenges that need to be addressed are: (i) interaction of monitoring functions with the multi-cloud application components, (ii) achieve integrity protection during runtime without interfering with the normal operation of the system, (iii) find the best compromise between the OPEX[1],

[1]Operational expenditure

the CAPEX[2], the performance, scope and granularity of the monitoring function, (iv) introduce the distribution of the monitoring tasks and the use of multi-cloud resources to improve the scalability of the monitoring function, (v) assure that the monitoring system is open enough to deal with the required flexibility of the multi-cloud application environment, without losing any of its functionality and required performance, (vi) coordination and orchestration of the distributed monitoring probes in order to create a secure and efficient multi-cloud ecosystem, (vii) determine the multi-cloud specific metrics, and (viii) in the case of encrypted traffic, part of the monitoring can be done using the unencrypted headers and statistics that do not require any decryption. For deeper analysis (Deep Packet Inspection, DPI), monitoring of encrypted traffic needs to be decrypted or to be analysed at the end-points.

## VI. Conclusions and future work

Besides security-by-design and SLA-oriented design tools, the MUSA framework includes the MUSA Security Assurance Platform to aid at operation time. The design tools are oriented to prepare, at design time, the multi-cloud application and its composed SLA for being security and privacy-aware. The MUSA Security Assurance Platform is in charge of exploiting such preparedness in the application components to orchestrate integrated security and performance assurance based on measurements over components and over Cloud Service Providers.

MUSA innovation in monitoring cloud applications is based on: (i) incorporating security assurance at run-time, this includes not only monitoring but also enforcement and notification; and, (ii) monitoring the whole cloud stack provisioned for the application and not just the application layer.

The innovative enforcement of MUSA will provide security controls as enforcement mechanisms and covering multiple security areas related to data protection (data confidentiality, data integrity, data localisation, data access). These security controls will be applied at two different levels by: (i) the application itself for self-protection (by embedding in its components run-time enforcement mechanisms, as well as by invoking these mechanisms as-a-service of the MUSA security assurance platform); and, (ii) the Cloud Service Provider in the lower levels of the cloud stack.

## Acknowledgements

The project leading to this paper has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 644429.

## References

[1] L. Columbus, "Computerworld's 2015 forecast predicts security, cloud computing and analytics will lead it spending," *Online at http://www.forbes.com/sites/louiscolumbus/2014/11/26/computerworlds-2015-forecast-predicts-security-cloud-computing-and-analytics-will-lead-it-spending/*, 2014.

[2] M. Vukolić, "The byzantine empire in the intercloud," *ACM SIGACT News*, vol. 41, no. 3, pp. 105–111, 2010.

[3] North Bridge in partnership with GigaOM Research, "The future of cloud computing, 3rd annual survey 2013," *Online at http://www.northbridge.com/2013-cloud-computing-survey*, 2013.

[4] P. Mell and T. Grance, "The NIST definition of cloud computing," *Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology Gaithersburg*, 2011.

[5] ITU-T Recommendation, "Cloud computing - functional requirements of network as a service," Y.3512 (08/14). 2014.

[6] ISO/IEC Specification, "Information technology – Cloud Data Management Interface (CDMI)," ISO/IEC 17826:2012. 2012.

[7] MUSA H2020 project, "Multi-cloud Secure Applications," 2015-2017. Available at http://musa-project.eu/.

[8] J. Chinneck, M. Litoiu, and M. Woodside, "Real-time multi-cloud management needs application awareness," in *Proc. of the 5th ACM/SPEC Int. Conf. on Performance engineering*. ACM, 2014, pp. 293–296.

[9] W. F. Ouedraogo, F. Biennier, and P. Ghodous, "Adaptive security policy model to deploy business process in cloud infrastructure." in *CLOSER*, 2012, pp. 287–290.

[10] C. W. Ling and A. Datta, "Intercloud raider: A do-it-yourself multi-cloud private data backup system," in *Distributed Computing and Networking*. Springer, 2014, pp. 453–468.

[11] Cloud security alliance, *Online at https://cloudsecurityalliance.org/wp-content/uploads/2011/10/TCI_Whitepaper.pdf*, 2011.

[12] Jericho Forum, "Cloud cube model: Selecting cloud formations for secure collaboration, version 1.0," *Online at http://www.opengroup.org/jericho/cloud_cube_model_v1.0.pdf*, 2009.

[13] J. Li, W. F. Ouedraogo, and F. Biennier, "Multi-cloud governance service based on model driven policy generation." in *CLOSER*, 2013.

[14] SHIELDS project, "Detecting known security vulnerabilities from within design and development tools. FP7-ICT-2007.1.4," 2008-2010. Available at www.shields-project.eu/.

[15] M. Clavel, V. da Silva, C. Braga, and M. Egea, "Model-driven security in practice: An industrial experience," in *Model Driven Architecture–Foundations and Applications*. Springer, 2008, pp. 326–337.

[16] Seaclouds project, "Supporting agile deployment and operation on multiple clouds. FP7 ICT Call 10," 2013-2016. Available at http://www.seaclouds-project.eu/.

[17] Cloud4SOA project, "Bringing Interoperability & Portability to PaaS. FP7 25753," 2010-2013. Available at http://www.cloud4soa.eu/.

[18] SPECS project, "Secure Provisioning of Cloud Services based on SLA management. FP7-ICT-2013.1.5," 2013-2016. Available at www.specs-project.eu/.

[19] Rouse, Margaret, "Cloud Application Performance Management (CAPM)," *Online at http://searchcloudapplications.techtarget.com/definition/cloud-application-performance-management-cloud-APM*, 2014.

[20] AppDynamics, "Application Performance Management," *Online at http://www.appdynamics.com/product/application-intelligence-platform/*.

[21] CA Technologies, "Application Performance Management," *Online at http://www.ca.com/us/products/application-performance-management.aspx*.

[22] IBM, "Application Performance Management," *Online at http://www-03.ibm.com/software/products/en/category/application-performance-management*.

[23] OCCI Standards, "Open Cloud Computing Interface)," *Online at http://occi-wg.org/*.

[24] CIMI Standards, "Cloud Infrastructure Management Interface)," *Online at http://dmtf.org/standards/cmwg*.

[25] OASIS, "Cloud Application Management for Platforms (CAMP standard)," *Online at https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=camp*.

[26] INTER-TRUST project, "Interoperable Trust Assurance Platform. FP7-ICT-2011.1.4," 2012-2015. Available at http://inter-trust.lcc.uma.es/.

[27] Cloud Standards Coordination, "Final Report)," *Online at http://www.etsi.org/images/files/Events/2013/2013_CSC_Delivery_WS/CSC-Final_report-013-CSC_Final_report_v1_0_PDF_format-.PDF*.

[2] Capital expenditure