Modelling Secure Cloud Systems Based on System Requirements

Shaun Shei[1], Luis Márquez Alcañiz[2]
Haralambos Mouratidis[1], Aidan Delaney[1]
David G. Rosado[3] and Eduardo Fernández-Medina[3]

[1]Computing, Engineering and Mathematics (CEM), University of Brighton, Brighton, United Kingdom
{S.Shei, H.Mouratidis, A.J.Delaney}@brighton.ac.uk
[2]Spanish National Authority for Markets and Competition (CNMC), Spain
luis.marquez@cnmc.es
[3]GSyA Research Group, University of Castilla-La Mancha, Ciudad Real, Spain
{david.grosado, eduardo.fdezmedina}@uclm.es

***Abstract*—We enhance an existing security governance framework for migrating legacy systems to the cloud by holistically modelling the cloud infrastructure. To achieve this we demonstrate how components of the cloud infrastructure can be identified from existing security requirements models. We further extend the modelling language to capture cloud security requirements through a dual layered view of the cloud infrastructure, where the notions are supported through a running example.**

I. Introduction

Cloud computing enables the provisioning of services through the abstraction of physical and virtual resources. This offers seemingly unlimited scalability, availability and flexibility of processing power through a pay-per-use model. Enterprises stand to benefit the most from cloud computing, in particular small and medium enterprises (SME) that may lack the capital expenses for adequate IT infrastructure. Legacy system migration aims to move operational systems towards new platforms, retaining original functionality whilst minimising disruption to the operational and business aspects. Legacy systems typically form the backbone of enterprise IT systems, though these systems often pose problems such as "brittleness, inflexibility, isolation, nonextensibility, lack of openness etc" [2]. Cloud computing is built upon and extends several established concepts and technologies such as Service-Oriented Architecture (SOA), distributed computing and virtualization. Moreover, the extension of existing technologies implies that any security issues and vulnerabilities are also inherited [1]. Currently there are no work with a security-centric focus for migration processes from legacy systems [3]. To address this need for secure migration, Marquez et al. propose a governance framework for the secure migration from legacy systems to the cloud [4]. The framework proposes activities for eliciting and analysing system requirements, to define and model security requirements with focus on cloud-specific attributes. Our work envisions modelling cloud systems and eliciting security requirements, creating transparency through alignment with cloud security guidelines and standards in the Cloud Control Matrix (CCM) and augmenting the proposed process in the migration framework. This paper contributes to the state of the art by:

- Defining the Cloud Infrastructure View to holistically model cloud infrastructures.
- Aligning a subset of criteria from the CCM with properties from the cloud infrastructure to provide transparency and guidelines for generating secure cloud configurations.

The structure of the paper is as follows: Section 2 describes the SMiLe2Cloud framework, the five activities involved and our extension of the Secure Tropos modelling language to augument the analysis activity. Section 3 presents the cloud infrastructure view, describing the conceptual layers for application and physical components and the alignment with the CCM in relation to the view. Section 4 discusses the related work and we conclude the paper in Section 5.

II. SMiLe2Cloud

A. Background

Here, we briefly introduce the SMiLe2Cloud framework which our proposed work complements. SMiLe2Cloud [4] is a process for migrating Legacy Information Systems (LIS) to secured cloud environments, based on the Deming cycle and the Software Engineering Institute (SEI) horseshoe model [5]. The process focuses on security aspects and thus assumes that the general reverse engineering efforts involved in migrating the LIS has already been successfully modelled through functional specifications and architectural elements, which is documented in a format that can be converted to a Knowledge Discovery Meta-Model (KDM) specification [6]. Based on the assumption that there is a KDM specification of the LIS model available, the process is then defined in detail following the Software & Systems Process Engineering Metamodel Specification (SPEM) notation.

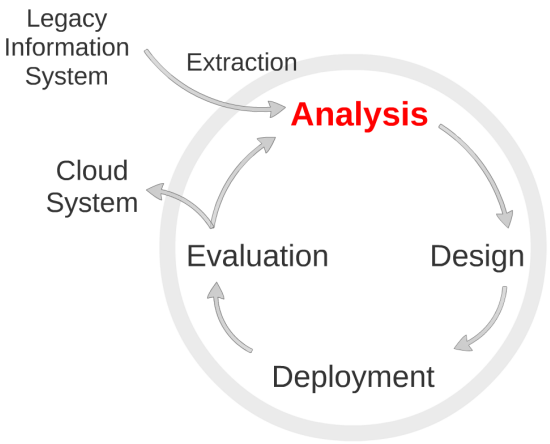

Fig. 1. A compact version of the SMiLe2Cloud process showing the Extraction, Analysis, Design, Deployment and Evaluation activities [4].

The SMiLe2Cloud process consists of five activities; Extraction, Analysis, Design, Deployment and Evaluation as illustrated in Figure 1. The iterative process is initialised from the extraction activity, where the security issues are extracted from the LIS to a security model (SMiLe model) through reverse engineering. The security requirements are analysed in the analysis activity based on the system requirements extracted during the previous activity. The design activity focuses on determining the service model, deployment model and selection of cloud service providers based on the alignment of cloud security requirements and the Cloud Security Alliance (CSA) Security, Trust & Assurance Registry (STAR) in the previous activity. The deployment activity further develops the deployment specification based on a repository of cloud migration patterns towards the implementation of the system. In the evaluation activity the migrated security model is verified and validated, where new security issues will be incorporated into the system during the next iteration of the process cycle. The extensions we propose directly compliments the analysis activity, which we now discuss in detail.

B. Extending the Analysis Activity

Our work proposes a conceptual view to holistically capture secure cloud infrastructure components, which creates a synergy with the analysis activity in SMiLe2Cloud. We present the new view by extending the existing elements found in the Secure Tropos modelling language [7] with cloud properties such as services and infrastructure. We then propose the definition of security configurations based on alignment of cloud infrastructure requirements with CCM security controls. The analysis activity is a crucial part of the SMiLe2Cloud process as the security requirements are extracted and defined based on the system requirements elicited from the previous activity. Figure 2 shows the analysis activity in a simplified view. The input for this activity is the system requirements elicited during the previous extraction activity, which is based on the KDM model and converted to the SMiLe2Cloud model as an Extensible Markup Language (XML) file. At this stage, the authors of the SMiLe2Cloud framework assume that the system requirements have already been elicited and have been modelled in the Secure Tropos tool. In order to model cloud security requirements, we extend the Secure Tropos methodology to incorporate cloud properties. Our extensions to the Secure Tropos modelling language are as follows. The system requirements are modeled using existing elements such as goal, actor, plan, resource and constraints in Secure Tropos, in order to visually represent the relationships and requirements of the legacy system. We then extend the Secure Tropos notation to capture the security requirements for cloud systems and define secure services, which are analysed in the proposed cloud infrastructure view to model components on both the application and physical layers. These extensions are described in detail in Section III.

C. Running Example

Throughout this paper we will use a running example to illustrate concepts contained within the cloud infrastructure. The running example is based on a simplified version of an existing system, the University of Brighton record management system. The modelled system represents the system and security requirements of the software system and facilitates the generation of configurations for cloud infrastructure. The example is illustrated in Figure 3.

III. Cloud Infrastructure View

In order to model secure software systems, the SMiLe2Cloud process aims to capture system requirements from legacy systems. The process then elicits security requirements based on the analysis of system requirements during the analysis activity. We extend the modeling language Secure Tropos to identify and model cloud-specific properties such as cloud services, infrastructure and cloud security elements. Goals represent an actors strategic interests, “Get student details” is an example of a goal. Resources represent a physical or virtual entity, “Student Data” is an example

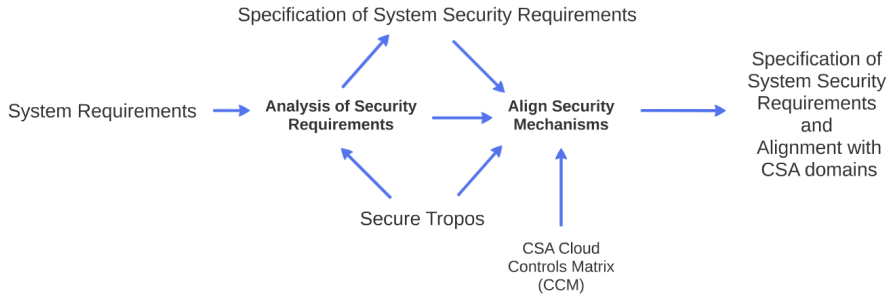

Fig. 2. The compacted version of the analysis activity [4].

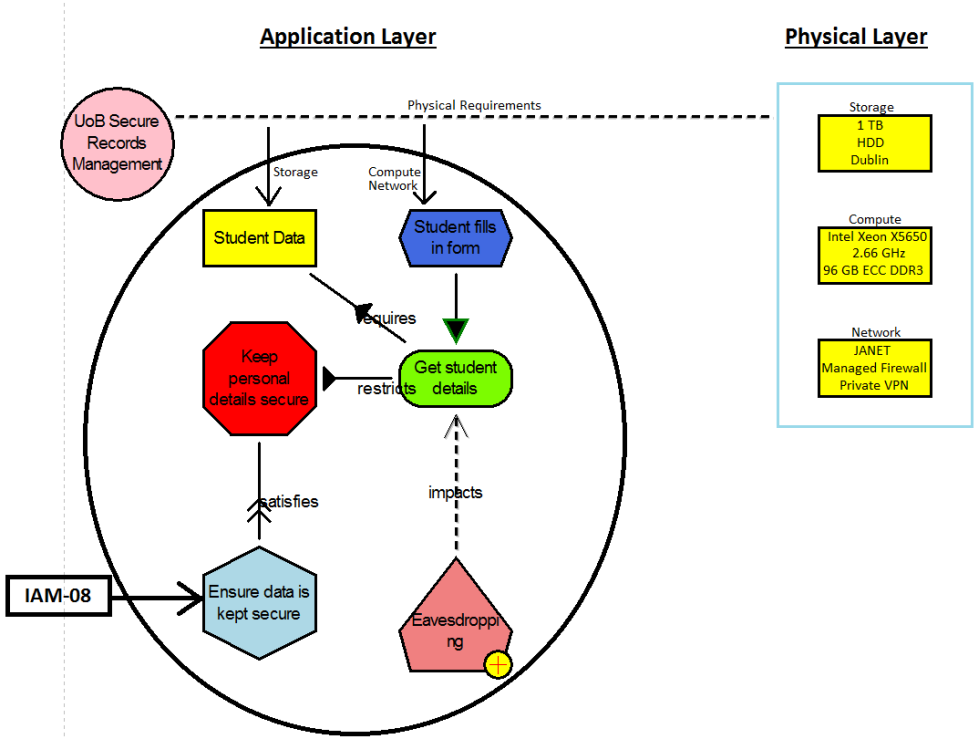

Fig. 3. The running example illustrating a typical Cloud Infrastructure View.

of a resource. A plan specifies the details and conditions under which a goal or measure is operationalised, "Student fills in form" is an example of a plan. Security constraints define security requirements through a set of restrictions that limit the way goals can be carried out, "Keep personal details secure" is an example of a security constraint. A security objective is a generic, implementation independent form of control that indicates how a constraint will be achieved, "Ensure data is kept secure" is an example of a security objective. A threat indicates the potential loss or problems that can put the system at risk, "Eavesdropping" is an example of a security threat. "IAM-08" is an example of a CCM security control, which is relevant for "Identity & Access Management, Trusted Sources".

Here we define a service in Secure Tropos based on a Goal-Plan-Resource pattern and extend this notion to identify secure services. Before we are able to define and model properties for cloud systems, we need to identify a basis for describing cloud computing. Our interpretation is based on the National Institute of Standards and Technology (NIST) definition for a cloud infrastructure, "a cloud infrastructure is the collection of hardware and software that enables the five essential characteristics of cloud computing" [8]. Thus to capture a holistic view of the cloud based on the NIST definition, we can model cloud systems by conceptually defining a dual-layered system consisting of an application layer and a physical layer as illustrated in Figure 3. The network, compute and storage attributes categorises the components found in the physical layer while services, cloud services and applications defines the application layer.

A. Application Layer

This conceptual layer hosts the logic behind the cloud system through services, cloud services and applications. Each

service represents specific goals that should be satisfied in order to fulfill some system requirements, which are then migrated towards the cloud. Cloud services are services made available to users on demand via the Internet from third party servers as opposed to the company's own on-premises servers. Cloud services are designed to provide easy, scalable access to applications, resources and services, and are fully managed by cloud service providers. In order to model and analyse software systems for cloud environments, we need to create a model for describing cloud services and the components involved in the definition of these services. This would include the software applications deployed to address the problem or tasks that the service is trying to solve or achieve, specifications of the resources required to execute the software and identifying the data that will be processed to determine the flow of data.

The left side of Figure 3 illustrates the application layer, where the *UoB Secure Records Management* is an example of what we propose as a secure cloud service based on identifying a new pattern from existing elements found in Secure Tropos. An example of an identified service is illustrated in Figure 3, consisting of the resource *Student Data*, the plan *Student fills in form* and goal *Get student details*. A secure service is a service that take security elements such as constraints, objectives and threats into account. In the running example Figure 3, a secure service includes the security constraint *Keep personal details secure*, security objective *Ensure data is kept secure* and the threat *Eavesdropping*. The components of the secure cloud service is indicated by the encapsulating of components within the circle. The dotted link between the secure cloud service and the grouped resources indicate the dependency relation and requirements of the service on physical components, while arrows to the application elements indicate the impact of specific physical components. The storage component located in the physical layer in the running example specifies that the location is based in *Dublin*, which is linked to and impacts the resource *Student Data* in the application layer.

B. Physical Layer

We sort the components in the physical layer into three primary categories based on the NIST definition "... typically includes server, storage and network components." [8]. Based on this definition, we propose that the *server* concept represents the computational components required to process data, which we have adapted as the *Compute* category in our work. These categories are described in more detail below.

1) Network: The network is a prerequisite for cloud computing; access to the technology wouldn't be possible without an Internet connection for clients. There are many variables in the configuration of the network, ranging from topology, switches, firewalls and routing to cabling and how each physical component is connected in relation to others. These properties are all essential in determining a template for matching the system requirements, in addition to satisfying security requirements. Other examples of networks connecting services include Joint Academic Network (JANET), New NHS Network (N3) and Public Services Network (PSN). This property also contributes towards the task of determining service model and deployment model of cloud services, specifically when choosing private, public or hybrid deployment models. Private cloud models are typically indicated by on-premise network connections for resources, while public cloud models are given by out-sourced connections and the hybrid model is a combination of both models. An example of a network resource is illustrated in the running example shown in Figure 3, with specifications such as the HEANet network, a managed firewall and Virtual Private Network (VPN). These are given as a guideline based on the requirements from the secure cloud service components in the application layer.

2) Compute: Computation represents the physical hardware required to execute code which implements services and applications. This includes components required for processing data, such as Central Processing Unit (CPU), Random Access Memory (RAM), Graphics Processing Unit (GPU), Virtual CPU (vCPU) and Virtual Machine (VM). The processing power or quantity of these components are specified in order to determine suitability to the system requirements. This will also be used to create a template matching security requirements, acting as a guideline for Cloud Service Provider (CSP) selection and further analysis. The specification of VMs such as number of instances, allocation to tenants and physical location enables the elicitation of cloud-specific requirements. For example the number of instances allocated effects spin-up time of provisioning and affects elasticity measurements. In Figure 3, the compute resource indicates the guideline specifications for provisioning the secure cloud service modelled in the application layer.

3) Storage: The input/output data required and produced by services are stored on physically storage devices, which may be distributed globally in terms of geographical locations. The type and configuration of storage ranges from components such as; Magnetic, Solid State Drive (SSD), Redundant Array of Independent Disks (RAID) and Storage Area Network/Network-Attached Storage (SAN/NAS). The specifications for storage is typically defined as the space available, file access time and geographical location. The location is crucial in eliciting security and privacy requirements due to the impact of jurisdictions and legal issues in different regions of the world. For example data stored on a physical storage device in the United States can be governed by the Patriot Act, which allows U.S. law enforcement and national security agencies unrestricted access to any data, anywhere, any time. An example of a storage component can be seen in Figure 3, where the *Student Data* resource represents the security requirement that the data should be stored on physical devices located in *Dublin*, in order to satisfy certain legal jurisdictions as an example. Each cloud service will include

deployment models, service models and specifications for resources, based upon the user requirements and restrictions identified in the early stages of the requirements modelling. This process allows us to define the exact requirements when planning for resource provision, utilisation and optimisation.

C. Cloud Security Controls

Ensuring that security standards and guidelines are followed and certified is crucial for building and maintaining a healthy relationship based on trust, assurance and transparency between cloud service providers and customers. While there are many standards bodies providing a large variety of best practices, guidelines and controls towards security in cloud computing, there are unfortunately no de-facto standards that are universally accepted and adopted by cloud service providers. The Cloud Security Alliance (CSA) is one such organisation that aims to provide security assurance within cloud computing through various guidelines and standards. One of their offerings is the CCM, which is a security controls framework for cloud providers and customers. The CCM aims to guide cloud providers and customers in the assessment of security risks in cloud offerings. It provides a detailed analysis of security principles and concepts based on the "Security Guidance for Critical Area of Focus in Cloud Computing v3.0" [13]. The controls framework consists of 16 domains, which are cross-referenced to industry-accepted security standards and regulations.

The latest version of the CCM is 3.0.1, consisting of 16 domains and 133 controls. Each control domain contains a specification describing the conditions and policies of the control. The architectural relevance of the control is provided through several fields covering the cloud infrastructure; physical, network, compute, storage, application and data. The applicability of the domain to cloud service delivery models is given through the standard SaaS, PaaS, IaaS (SPI) model, which informs the user which service models are affected for a given control. The relation of the control is described involving the service provider and tenant. Finally the applicability of the scope is given through a comprehensive list of standards and regulations, in order to facilitate transparency. We select three diverse controls as an example from the list of 133 controls due to restricted space. The first control "Identity & Access Management Trusted Sources" *(IAM-08)* seen in the first column in Table I is applicable for data, relevant to the Software-as-a-Service and Platform-as-a-Service service models and determines that the service provider is responsible for this control. Thus this control would be of interest for security policies that cover data exchange in services. The "Application & Interface Security Application Security" *(AIS-01)* control is relevant for compute, storage, application and data whilst applicable for the SPI service models with the service provider holding responsibility as seen in the second column of Table I. Another example for controls covering other areas is "Business Continuity Management & Operational Resilience Datacenter Utilities / Environmental Conditions" *(BCR-03)* seen in the third column of Table I, which involves the physical, network and the SPI model whilst both the service provider and tenant is responsible for adhering to the control. An example of aligning security controls is shown in Figure 3 with the control *IAM-08* linked to the security objective *Ensure data is kept secure*.

IV. Related Work

There are currently many ongoing or completed European research projects and related work which aims to migrate, modernise or adopt existing or legacy systems towards cloud computing environments. The key characteristics of each project range from improving system efficiency through virtualisation, interoperability across multiple cloud vendors to maximising cost versus performance. Jamshidi et al. carried out a systematic literature review on 23 studies based on migrating from legacy systems to cloud environments, the results were analysed using their characterisation-based framework [9]. The synthesised research indicates that cloud migration is still in the early stages of maturity and that there is a need for migration frameworks to improve maturity level and trust. There is also a lack of support for automation of migration tasks and there is a need for architectural adaptation and self-adaptive cloud-enabled systems. The majority of related projects specialise in specific deployment or service models, while there is a lack of holistic solutions to capture both cloud and security requirements for migration.

The ARTIST project [11] adapts an Model-Driven (Software) Modernisation (MDM) approach to reverse-engineer legacy software systems and migrate towards cloud-based environments, where the main novelty of their methodology is the additional pre-migration and post-migration phases which are explicitly defined. They propose a migration method supported through a comprehensive tool suite, where they focus on both technical and business aspects although security is not a primary consideration during their process. PaaSage aims at delivering an open and integrated platform to support both design and deployment of cloud applications, together with an accompanying methodology that allows model-based development, configuration, optimisation, and deployment of existing and new applications independently of the existing underlying cloud infrastructures [10]. REMICS is an European FP7 project which aim to provide a model-driven methodology and tools to support re-usability and migration of legacy systems to cloud systems, by transforming legacy models to cloud services [12]. While these projects provide a highly specialized approach for a particular area, they fail to consider security as a critical component during any stage in the elicitation of system requirements and migration towards cloud-based systems.

Iankoulova et al. carries out a systematic review of current work in the literature that addresses security requirements in cloud computing, where their goal was to provide a comprehensive view of the areas that are under-researched and most investigated. They identified nine sub-areas; "Access Control, Attack/Harm Detection, Non-repudiation, Integrity,

TABLE I
EXAMPLES OF CONTROLS FROM VARIOUS DOMAINS IN THE CCM.

	Phys	Network	Compute	Storage	App	Data	SaaS	PaaS	IaaS	Service Provider	Tenant
IAM-08						x	x	x		x	
AIS-01			x	x	x	x	x	x	x	x	
BCR-03	x	x					x	x	x	x	x

Security Auditing, Physical Protection, Privacy, Recovery, and Prosecution" [14] where non-repudiation, physical protection, recovery and prosecution were the most under-researched based on a sample of 55 selected papers. Zardari et al. argue that their Goal Oriented Requirements Engineering (GORE) approach provides a paradigm which addresses the lack of requirements engineering methodologies that can be applied towards cloud adoption to facilitate the negotiation and alignment of user requirements with cloud provider provisioning [15]. They categorise goals into business, core and operational goals, though their end-goal is to search for and select potential CSP through pattern-matching based on analysing mismatches between user requirements and service provisions, trade-offs and risk management. Our approach will provide tools to (semi)automate the generation of configuration files that assist users in adopting or verifying the satisfiability and compliance of cloud systems, based on both security and user requirements. Menzel et al. proposes a model-driven approach that allows the user to define security requirements at the modelling layer and facilitate a transformation based on security configuration patterns towards enforceable security policies [16]. Their cloud-based Service Security Lab provides a virtualised testing environment for users to monitor and analyse the enforcement of their security requirements and policies.

V. CONCLUSION

In this paper we demonstrate our proposed technique for modelling secure cloud systems by extending the Secure Tropos modelling language. This is achieved by creating the cloud infrastructure view, which conceptually captures the cloud infrastructure by defining components from the application and physical layer. The security requirements for cloud services are defined and enhanced through alignment with the CCM, which provides guidelines for cloud security through security controls. We then indicate how our work integrates into a secure governance framework by enhancing the analysis activity in the SMiLe2Cloud process for migrating legacy IT systems to secure cloud environments. The work is validated through constructed examples of real life systems, demonstrating the applicability for modelling secure cloud systems from existing legacy systems or stakeholder requirements.

ACKNOWLEDGEMENT

This research is part of the following projects: SERENIDAD (PEII11-037-7035) financed by the Viceconsejería de Ciencia y Tecnología de la Junta de Comunidades de Castilla-La Mancha (Spain) and FEDER, and SIGMA-CC (TIN2012-36904) financed by the Ministerio de Economía y Competitividad (Spain).

REFERENCES

[1] Armbrust, Michael, O. Fox, Rean Griffith, Anthony D. Joseph, Y. Katz, Andy Konwinski, Gunho Lee et al. "M.: Above the clouds: a Berkeley view of cloud computing." (2009).

[2] J. Bisbal, D. Lawless, B. Wu, J. Grimson, V. Wade, R. Richardson, & D. O. Sullivan. "An overview of legacy information system migration". *Software Engineering Conference, 1997. Asia Pacific... and International Computer Science Conference* 1997. APSEC'97 and ICSC'97. Proceedings. IEEE, 1997.

[3] L. Márquez Alcañiz, D. G. Rosado, D. Mellado, and E. Fernández-Medina, Security in Legacy Systems Migration to the Cloud: A Systematic Mapping Study, in *11th International Workshop on Security in Information Systems*. Lisbon, Portugal. 2014 p. 93–10.

[4] L. Márquez Alcañiz, D. G. Rosado, H. Mouratidis, D. Mellado, and E. Fernández-Medina. A Framework for Secure Migration Processes of Legacy Systems to the Cloud. in *Fifth International Workshop on Information Systems Security Engineering - Advanced Information Systems Engineering Workshops*. Springer International Publishing, 2015.

[5] Seacord, R. , Plakosh, D. & Lewis, G. , Modernizing legacy systems: software technologies, *Engineering Processes, and Business Practices*, 2003.

[6] OMG, Architecture-Driven Modernization. Knowledge Discovery Meta-Model (KDM), v1.3. 2011.

[7] Mouratidis, H. & Giorgini, P. , 2007. Secure Tropos: a Security-Oriented Extension of the Tropos Methodology. *International Journal of Software Engineering and Knowledge Engineering*, 17(02), pp.285–309.

[8] Mell, Peter, and Tim Grance. "The NIST definition of cloud computing." (2011).

[9] P. Jamshidi, A. Ahmad and C. Pahl, "Cloud Migration Research: A Systematic Review," *IEEE Transactions on Cloud Computing*, 1(2), pp.142–157, 2013.

[10] Consortium, P. , PaaSage: model based cloud platform upperware, 2012. URL http://www. paasage. eu.

[11] Bergmayr, Alexander, et al. "Migrating legacy software to the cloud with ARTIST." *Software Maintenance and Reengineering (CSMR)*, 2013 17th European Conference on. IEEE, 2013.

[12] P. Mohagheghi, A. J. Berre, A. Henry, F. Barbier, A. Sadovykh. "REMICS-REuse and migration of legacy applications to interoperable cloud services." *Towards a Service-Based Internet*. Springer Berlin Heidelberg, 2010. 195–196.

[13] Simmonds, P., Yeomans, A. & Dobson, I., 2011. Security Guidance for Critical Area of Focus in Cloud Computing v3.0. Cloud Security Alliance (CSA).

[14] Iankoulova, Iliana, and Maya Daneva. "Cloud computing security requirements: A systematic review." *Research Challenges in Information Science (RCIS)*, 2012 Sixth International Conference on. IEEE, 2012.

[15] Zardari, Shehnila, and Rami Bahsoon. "Cloud adoption: a goal-oriented requirements engineering approach." *Proceedings of the 2nd International Workshop on Software Engineering for Cloud Computing*. ACM, 2011.

[16] M. Menzel, R. Warschofsky, I. Thomas, C. Willems, & C. Meinel (2010, July). The service security lab: A model-driven platform to compose and explore service security in the cloud. *6th World Congress on Services (SERVICES-1)*, IEEE, 2010, pp. 115–122.