Methodology to obtain the security controls in multi-cloud applications

Samuel Olaiya Afolaranmi[1], Luis E. Gonzalez Moctezuma[1], Massimiliano Rak[2], Valentina Casola[3], Erkuden Rios[4] and Jose L. Martinez Lastra[1]

[1]*Factorty Automation Systems and Tescnology Lab, Tampere University of Technology, Tampere, Finland*
[2]*Dipartimento di ingegneria Industriale e dell'Informazione, Second University of Naples, via Roma Avera, Italy*
[3]*DIETI, Università Federico II of Naples, Italy*
[4]*TECNALIA. ICT-European Software Institute. Parque Tecnológico de Bizkaia, Spain*
{samuel.afolaranmi, luis.gonzalezmoctezuma, jose.lastra}@tut.fi, massimiliano.rak@unina2.it, casolav@unina.it, erkuden.rios@tecnalia.com

Keywords: Multi-cloud, Security-by-design, Cyber-security methodologies, Threat modelling

Abstract: What controls should be used to ensure adequate security level during operation is a non-trivial subject in complex software systems and applications. The problem becomes even more challenging when the application uses multiple cloud services which security measures are beyond the control of the application provider. In this paper, a methodology that enables the identification of the best security controls for multi-cloud applications which components are deployed in heterogeneous cloud providers is presented. The methodology is based on application decomposition and modelling of threats over the components, followed by the analysis of the risks together with the capture of cloud business and security requirements. The methodology has been applied in the MUSA EU H2020 project use cases as the first step for building up the multi-cloud applications' security-aware Service Level Agreements (SLA). The identified security controls will be included in the applications' SLAs for their monitoring and fulfilment assurance at operation.

1 INTRODUCTION

Multi-cloud approaches that promote the simultaneous usage of multiple cloud services are emerging as a solution to optimise availability, performance and cost of the applications (Ferry et al., 2013).

With respect to whether multi-cloud paradigm brings benefits to the application security, there are currently two main opinion streams within the research community: one that advocates multi-cloud as being strong security enabler (thanks to the strong security measures offered by professional cloud service providers and possibility to replace cloud services when needed), and one that, on the contrary, considers multi-cloud as risk enhancer (mainly due to the lack of insight and control over the consumed clouds, as well as the challenges posed by orchestration).

Different approaches for multi-cloud have been proposed in the literature (Singhal et al., 2013), (Bernstein et al., 2009), (Celesti et al., 2010). Recently, (Bohli et al., 2013) presented a four type classification of the security-enhancing architectural approaches for multi-cloud applications: replication of application tasks, partition of system into tiers, partition of logic into fragments, and partition of data into fragments. In this paper, only the last three types are considered i.e., those where the application is partitioned into components, be they application business logic or data, deployed in different clouds.

This paper presents the methodology adopted in MUSA EU H2020 project for the selection of desired security controls over multi-cloud applications. The methodology is applicable to any of the partition-based multi-cloud approaches considered and enables the identification of the application components' risks and the derivation of the appropriate security controls to apply to both application components and the cloud services exploited by such components. These security controls will be used to build the Service Level Agreement (SLA) that describes the Service Level Objective (SLO) clauses promised to the multi-cloud application customers. The SLA that includes information of guaranteed security controls is the basis for the assessment of adequate performance of security behaviour during operation.

The paper is structured as follows. Next Section 3 introduces the main security challenges of multi-cloud applications and Section 4 discusses existing approaches for threat modelling as the basis for the security control identification. The Section 5 introduces the security control identification methodology itself, while Section 6 describes the methodology applicability and results of its adoption in a particular case study of MUSA project. Finally, Section 7 concludes the paper explaining future work.

3 MULTI-CLOUD APPLICATIONS SECURITY

The term Multi-Cloud denotes the usage of multiple, independent clouds by a client or a service, unlike Cloud Federations that are achieved when a set of cloud providers voluntarily interconnect their infrastructures to allow sharing of resources among each other (0, (Nikolay Grozev and Buyya, 2012)). Even if, at state of art, few concrete multicloud solutions exists, the topic is considered extremely relevant: the need for multicloud solution is well demonstrated by the number of research projects that are proposing solutions and techniques to address the multicloud approach, like OPTIMIS, mOSAIC, MODAClouds, PaaSAge, Cloud4SOA ((Petcu et al. 2011), (Ferrer et al. 2012)). It is out of the scope of this paper to offer a complete survey of such activities, it is suggested that the interested reader check the following papers: ((Nikolay Grozev and Buyya, 2012), (Baryannis et al., 2013) and (Zeginis et al., 2013)).

Multicloud approaches are debatable, respect to security topic: some authors proposes multicloud approaches as a way to improve the level of security for customers, other authors suggests that distributing applications among multiple CSPs increase the number of security issues, obtaining as a result a lower level of security.

(Alzain et al., 2014) and (Bernstein and Vij, 2010) offers simple surveys of solutions that try to improve the security using multicloud techniques. In concrete, the main results are available for storage services, as an example (Yan et al., 2012) and (Oliveira et al., 2010) proposes techniques to distribute a file over multiple provider or untrusted network, granting higher confidentiality and the integrity of data.

It is worth noticing that all the paper that sustain the higher security of the multicloud approach focuses on increase of one or more specific security property offered to the customers.

0 and 0 face the security in multi-cloud application in a different perspective: they analyses different multicloud solutions and try to make a security assessment of the overall application behaviour, outlining the new security issues introduced by the multicloud approach.

While the security assessment approach is very interesting, both papers deals with a very high-level description of the solution and does not offer a clear solution to make an assessment for a real multicloud application.

At best of author's knowledge there are no concrete techniques that try to address the issue of developing multicloud application trying to take in consideration user security requirements from the early development stages.

4 THREAT MODELLING TECHNIQUES

In order to address systematically security issues in multicloud application, it is proposed in this paper according to security best practices (Myagmar, 2005), to perform a security assessment from the very early development stages: multicloud application design will include the definition of a threat model, which is a structured representation of all the information that affects the security of an application.

Thanks to the integrated threat model, it will be possible to perform a systematic risk analysis of the multicloud application identifying the security requirements requested to Cloud Service Providers (CSPs).

At state of art, there are at least two general approaches to threat modelling: attack-based and software-based.

Attack-based approaches build a threat model starting from the attacker point of view and aiming at identifying the possible attacks to the target software. Examples of such an approach are threat models based on attack tree (Shostack, 2008), (Saini et al., 2008).

Software-based approaches focus on the architecture of the software to be secured an aims at classifying the possible risks in order to rank their importance and address them according to different priority levels (Oladimeji et al., 2006), (Sodiya et al., 2007).

It is out of the scope of this paper to propose a complete survey over threat modelling techniques, it is suggested that the interested reader check (Hussain et al., 2014) and (Tondel et al., 2008), which summarize the most common approaches and compare them.

In this paper the multicloud application are mainly composed of web application (see further sections, so the approaches suggested by the OWASP project (OWASP, 2015) was adopted as it collects tools devoted to web security. The threat modelling technique adopted is STRIDE methodology, proposed by Microsoft and largely adopted in the context of web applications (Sodiya et al., 2007).

According to such approach, threats are classified in 6 simple categories: *Spoofing Identity*, *Tampering with Data*, *Repudiation*, *Information Disclosure*, *Denial of Service* and *Elevation of Privilege*.

In the following STRIDE methodology is adopted in order to identify the security requirements and the needed countermeasures (represented in terms of security controls) for each of the component of a multi-cloud application, with the goal of offering an approach that aims at making a complete security assessment of multi-cloud applications.

5 PROPOSED METHODOLOGY

One core aspect of the proposed methodology is that the security controls address not only the threats identified during the risk assessment process, but also those business requirements that can be tackled by security controls. For example, in the realm of cloud computing, data location is a variable where the service consumer has little influence; nevertheless, applications storing personal data must have very clear control on the location where this data is stored. These types of requirements are identified in a business requirements capture phase and addressed by security controls, which otherwise would be skipped by traditional threat modelling techniques, which focus on security attacks.

The proposed methodology is composed of five steps, namely application decomposition, threat identification and risk assessment, business requirements capture, cloud security requirements identification and selection of security controls. These five steps constitute a process of application security analysis which is very essential in the identification of threats, determination of mitigating measures and implementation of security controls in multi-cloud applications. It ensures that threats are identified and business requirements captured. These serve as a basis for determining the appropriate countermeasures and implementing security controls. The second and third steps (threat identification & risk assessment and business requirements capture) of the methodology may be performed in parallel and they are both inputs for step four (cloud security requirements identification). The final step, five (Selection of security controls), ensure that the security requirements are satisfied. The sequence of the proposed methodology is shown in Figure 1. Next these steps are described in detail.

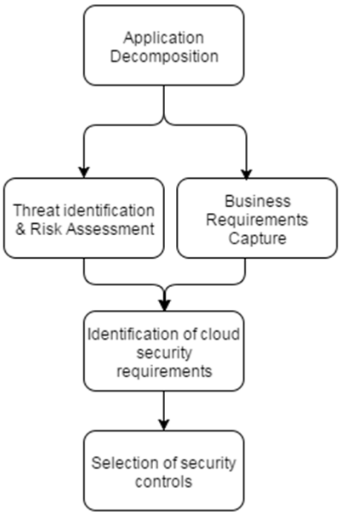

Application Decomposition
Threat identification & Risk Assessment
Business Requirements Capture
Identification of cloud security requirements
Selection of security controls

Figure 1: Proposed methodology for obtaining security controls

5.1 Application Decomposition

The first step of the methodology is application decomposition. It is a process of breaking down an application into the different components which make up the application. This activity provides an insight on the operation and relationship of the application with external entities. It is essential because it helps to identify potential threat targets. Basically, application decomposition consists of three stages, namely identification of assets, identification of entry points and identification of trust levels. Asset identification is the identification of application components that are prone to attack i.e., the components in which a potential attacker might be interested in. Identification of entry points involves identifying the interfaces through which connection may be made to the application i.e., the points of connection through which a potential attacker can access the application such as HTTP ports etc. The identification of trust levels involves identifying the different levels of access rights that would be granted to external entities by the application.

5.2 Threat Identification and Risk Assessment

The second step of the methodology is threat identification and risk assessment. Threat identification is the determination of threats associated with each of the application components. This process will ensure that the likely threats which may impact the application based on the intention of a potential attacker are clearly identified. An evaluation of the risk associated with the identified threats is then estimated. Threat identification and risk assessment basically involves two stages, namely determination & ranking of threats and risk assessment. Determination and ranking of threats is a process of determining the threats associated with the application components using STRIDE as a threat categorization methodology, as outlined in the previous section. Risk assessment involves the evaluation of the potential risks associated with the identified threats. In risk assessment, the likelihood of the occurrence and the impact of the identified threats in each of the components are evaluated. This helps to determine the extent of damage in the application in the case of an attack. The risk associated with each of the identified threats can be estimated using a value-based risk model like DREAD (OWASP, 2015) or quantitative risk model i.e., where Risk is computed as the product of likelihood and impact. (Risk = likelihood x impact).

5.3 Business requirements capture

The third step of the methodology is business requirements capture. This is performed in order to identify the cloud compliance requirements for example for data governance. In multi-cloud applications, certain requirements have to be met in order to fulfil data governance particularly as it concerns storage, back-up, transfer and protection of data. These sets of requirements constitute the business requirements capture for the multi-cloud application. For example, as it relates to the location and storage of data, there are certain data governance law and regulation that a data controller (*who determines the use of personal data*) must comply with before processing personal data. Therefore, the business requirements capture must be made in order to identify these requirements and also to ensure that the cloud components of the multi-cloud application comply with the relevant data law requirements.

5.4 Cloud security requirements Identification

The fourth step of this methodology is cloud security requirements identification. Cloud security requirements refer to the security and privacy requirements for cloud services. These requirements are derived from cloud computing industrial standards and relevant data protection laws. It serves as a guide for assessing the level of security and identifying the security requirements needed to protect the cloud environment. Cloud security requirements further supplements the threats and business capture requirements identified in the previous steps. It helps to identify security requirements needed to mitigate identified risks in the second step of the methodology and also other security requirements needed to fulfil legal and business requirements.

5.5 Selection of Controls

The last step of the methodology deals with the identification of the countermeasures needed to respect the security requirements.

Countermeasures are represented using standard security control Frameworks ((NIST, 2014), (CSA, 2011)). Security controls are *"a safeguard or countermeasure prescribed for an information system or an organization designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements"* (NIST, 2014).

Security Control Frameworks collects and organize security controls in order to offer guidelines to building secure systems in a standard way: thanks to the standard list of controls it is possible to assess the security of a system and compare it with requirements, verifying how many and in which way controls are concretely implemented. At state of art Controls are adopted by certification authorities and or third parties that by a (human–driven) audit verify compliance with security requirements and eventually regulations.

In order to apply the proposed approach in the cloud environment and for specific services, instead that respect to the overall CSPs infrastructure, recently such controls are embedded into Security SLA in order to grant the level of security offered by each service ((Casola, 2015b), (Luna et al., 2015)).

In the proposed methodology, the security control of the NIST framework is classified with respect to category of threats, type of components and security requirement, in order to identify the set of controls needed for each component.

The final result is a simple Security SLA that summarizes the needs, in terms of security control, for each of the component of the multicloud application. Such information can be used by a broker in order to acquire resources respecting the security requirements requested (Casola, 2015a).

6 APPLICATION OF THE METHODOLOGY IN A CASE STUDY

The methodology explained in the foregoing section is applied in a case study in order to identify the threats and determine the appropriate security control measures. The case study is Tampere Smart Mobility (TSM). TSM is a smart mobility multi-cloud application which enables and supports an energy efficient and smart mobility of citizens of Tampere, Finland. The TSM application provides users with customized journey recommendations from which they can make their choice. To achieve this, the TSM stores their personal data, such as name, age and mobility habits on the cloud. Therefore, adequate security controls must be integrated into the TSM application to protect the personal data of the users. The next section shows how the methodology is applied in this case study.

6.1 Application Decomposition

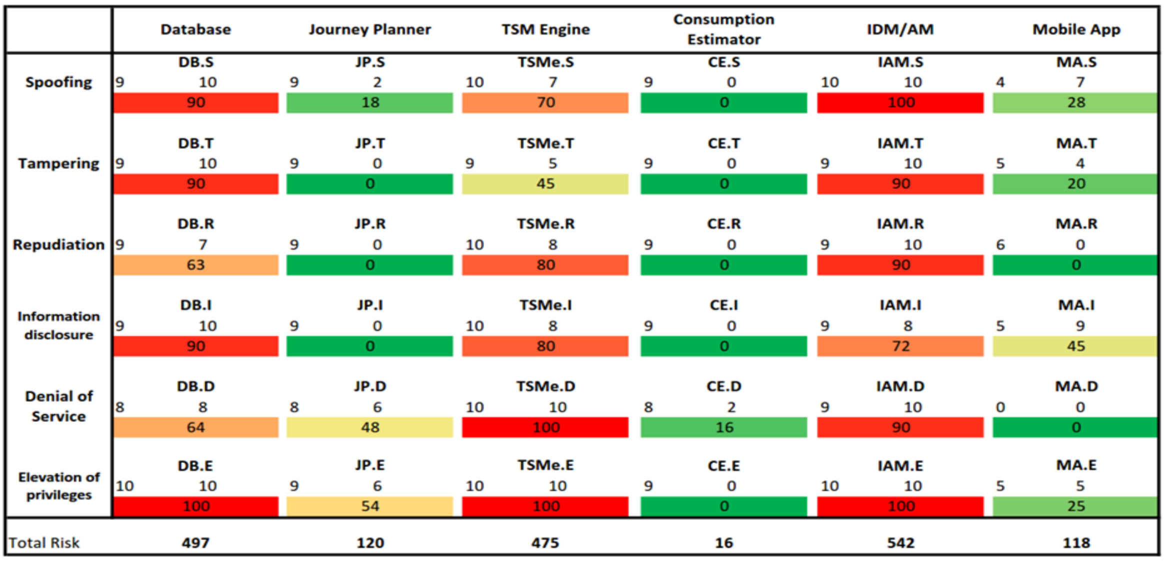
The TSM application is carefully analyzed in order to identify the assets, entry points and trust levels. On decomposing the TSM application, six assets i.e., the threats targets were identified, namely mobile app, database, TSM engine, Journey planner, Consumption estimator and the Identity manager/Access manager. All the assets apart from the mobile app would be deployed in a multi-cloud layout. The TSM application entry points are mobile user interface, HTTP, web server and HTTP port. The trust levels are: administrator (back-end application manager), end user (citizens) and TSM components (TSM assets).

6.2 Threat Identification and Risk Assessment

In the identification of threats in the TSM application, the STRIDE categorization methodology was used. The STRIDE methodology was applied to all the TSM application assets identified in the previous step **(6.1)**. The likelihood and impact of each threat on each asset was estimated, thus resulting in the risk assessment of the TSM application. A quantitative approach was used to evaluate the risk associated with each asset i.e., on a scale of (0-10), numerical values were estimated for the **likelihood** and **impact** of each threat on each component. With these parameters the computer risk ranges from 0 (no risk) to 100 (high risk).

The result of the threat identification and risk assessment step is provided in the Table 1. The ID notation goes as follow: DB.S represents Database spoofing threat; JP.T represents Journey planner tampering threat and so on.

Table 1: TSM Application Threat identification and Risk assessment



	Database	Journey Planner	TSM Engine	Consumption Estimator	IDM/AM	Mobile App
Spoofing	DB.S 9 10 90	JP.S 9 2 18	TSMe.S 10 7 70	CE.S 9 0 0	IAM.S 10 10 100	MA.S 4 7 28
Tampering	DB.T 9 10 90	JP.T 9 0 0	TSMe.T 9 5 45	CE.T 9 0 0	IAM.T 9 10 90	MA.T 5 4 20
Repudiation	DB.R 9 7 63	JP.R 9 0 0	TSMe.R 10 8 80	CE.R 9 0 0	IAM.R 9 10 90	MA.R 6 0 0
Information disclosure	DB.I 9 10 90	JP.I 9 0 0	TSMe.I 10 8 80	CE.I 9 0 0	IAM.I 9 8 72	MA.I 5 9 45
Denial of Service	DB.D 8 8 64	JP.D 8 6 48	TSMe.D 10 10 100	CE.D 8 2 16	IAM.D 9 10 90	MA.D 0 0 0
Elevation of privileges	DB.E 10 10 100	JP.E 9 6 54	TSMe.E 10 10 100	CE.E 9 0 0	IAM.E 10 10 100	MA.E 5 5 25
Total Risk	497	120	475	16	542	118

6.3 Business requirements capture

In identifying the cloud compliance requirements for data governance in the TSM application, the Finnish Personal Data Act (523/1999) was applied. This is because Tampere University of Technology (TUT) who is the data controller is established in Finland. The Act specifies the requirements and guidelines aimed at protecting the rights and privacy of users in the processing of their personal data. The business requirements identified through the application of the Finnish Data Act were duties of data controller and data owner, data storage location & transfer of data and data security.

In summary, this act requires that the collected data must be store within the territory of the EU. In case it is transferred out of EU, the destination must be in within a list of authorized countries. The data controller must inform the users about the location of their data, so data awareness is required. The controller should also provide data privacy protection.

6.4 Cloud security requirements Identification

In order to identify the cloud security requirements for the TSM application, the SINTEF catalog was used. The SINTEF cloud security requirements catalog is a checklist with security and privacy requirements for public cloud services (Bernsmed et al., 2015). It is essentially meant for evaluating cloud security requirements. Based on the results of the risk assessment carried out in the threat identification and risk assessment step (**6.2**) and the business requirements capture step (**6.3**), a security requirement matrix was generated. See Table 2 in appendix. It specifies the relevant security requirements per component of the TSM application. The security requirements are listed as rows while the TSM application components are listed as columns.

For a given multi-cloud component, a security requirement might or might not be needed. It is needed if it can mitigate the risk of a threat computed in the step two of the methodology or if it can address a business requirement, captured in the step three of the methodology. In case the requirement is not needed the cell value will be null, otherwise it will have a unique ID. For example, in Table 2 the security requirement **Encryption** is associated with the risk ID DB.S (Database Spoofing). This means, that Encryption is needed to mitigate the spoofing risk within the database component.

6.5 Selection of Controls

According to the Threat analysis performed and to the selection of security requirements, the identification of specific security controls needed, can now be addressed.

As anticipated, the security controls are associated to threat classes and the type of components.

According to the high level collection of security requirement shown before, a set of properties to be respected have been identified for each of the threat categories of the STRIDE methodology and for each of the component. Figure 2, available in appendix, illustrate an example of properties for the Tampering of Data category, associated to the TSM Engine component.

In order to identify the security controls requested to our multi-cloud application, the properties identified above are listed, and the control family which addresses the security issue and the specific controls that must be implemented to grant the correct level of security is also identified.

Table 3, in appendix, summarizes the list of controls that were selected for each of the properties proposed.

It is worth noticing that, at the end of the full process, a full list of security requirements that affect the multicloud application architecture (as reported in Table 2) and a list of security controls that must be verified against the final application configuration and the technologies adopted to implement the multi-cloud application are derived (reported in Table 3).

7 CONCLUSIONS

Application security assurance in multi-cloud environments is a challenging topic due to the lack of standards and widely adopted best practices. The proper selection of security controls over multi-cloud application components and the cloud services they use is crucial for an adequate assessment of SLA fulfilment and regulatory compliance. As explained above, this selection depends on the risk profile wanted for the application and the multi-cloud approach adopted.

This paper introduces a methodology for the systematic identification of multi-cloud application threats and risks, as well as the derivation of security controls that can be used to monitor and manage desired security aspects of multi-cloud applications at runtime. The methodology is compatible with SLA-driven continuous security assurance and it will be supported by the MUSA framework tools which first prototypes will be ready in July 2016.

It is expected that in future publications, the security-aware SLAs created following the methodology explained herein will be presented, together with the MUSA methods and tools to generate them. One of the major challenges in that research is on the indicators and metrics applicable to each security control and their composability to derive actual values of the security controls.

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

Ferry, N., Rossini, A., Chauvel, F., Morin, B., & Solberg, A. (2013, June). Towards a model-driven provisioning, deployment, monitoring, and adaptation of multi-cloud systems. *In Cloud Computing (CLOUD), 2013 IEEE Sixth International Conference on (pp. 887-894)*. IEEE.

Singhal, M., Chandrasekhar, S., Ge, T., Sandhu, R., Krishnan, R., Ahn, G. J., & Bertino, E. (2013). Collaboration in multicloud computing environments: Framework and security issues. *Computer*, (2), 76-84.

Bernstein, D., Ludvigson, E., Sankar, K., Diamond, S., & Morrow, M. (2009, May). Blueprint for the intercloud-protocols and formats for cloud computing interoperability. In *Internet and Web Applications and Services, 2009. ICIW'09. Fourth International Conference on* (pp. 328-336). IEEE.

Celesti, A., Tusa, F., Villari, M., & Puliafito, A. (2010, July). How to enhance cloud architectures to enable cross-federation. In *Cloud Computing (CLOUD), 2010 IEEE 3rd International Conference on* (pp. 337-345). IEEE.

Bohli, J.-M., Gruschka, N., Jensen, M., Iacono, L. L., and Marnau, N. (2013). Security and Privacy-Enhancing Multicloud Architectures. IEEE Transactions on Dependable and Secure Computing, 10(4):212-224.

Global Inter-cloud Technology Forum (2010). Use Cases and Functional Requirements for Inter-Cloud Computing. Technical report.

Nikolay Grozev and Buyya, R. (2012). Inter-Cloud architectures and application brokering: taxonomy and survey. Software - Practice and Experience, 44(3):369|-390.

Petcu D, Crciun C, Neagul M, Panica S, Di Martino B, Venticinque S, RakM, Aversa R. Architecturing a sky com- puting platform. In Proceedings of the International Conference Towards a Service-Based Internet ServiceWave'10, Vol. 6569, CezonM,Wolfsthal Y (eds). Springer-Verlag: Ghent, Belgium, 2011; 1–13.

Ferrer AJ, Hernández F, Tordsson J, Elmroth E, Ali-Eldin A, Zsigri C, Sirvent R, Guitart J, Badia RM, Djemame K, Ziegler W, Dimitrakos T, Nair SK, Kousiouris G, Konstanteli K, Varvarigou T, Hudzia B, Kipp A, Wesner S, Corrales M, Forgó N, Sharif T, Sheridan C. OPTIMIS: a holistic approach to cloud service provisioning. Future Generation Computer Systems 2012; 28(1):66–77.

Zeginis, D., D'Andria, F., Bocconi, S., Gorronogoitia Cruz, J., Collell Martin, O., Gouvas, P., Ledakis, G., and Tarabanis, K. a. (2013). A user-centric multi-PaaS application management solution for hybrid multi-Cloud scenarios. Scalable Computing: Practice and Experience, 14(1):17-32.

Alzain, M., Soh, B., and Pardede, E. (2014). TMR-MCDB: Enhancing Security in a Multi-cloud Model through Improvement of Service Dependability.

Bernstein, D. and Vij, D. (2010). Intercloud security considerations. Proceedings - 2nd IEEE International Conference on Cloud Computing Technology and Science, CloudCom 2010, pages 537-544.

Yan, Z., Hongxin, H., Gail-Joon, A., and Mengyang, Y. (2012). Cooperative Provable Data Possession for Integrity Verification in Multicloud Storage. IEEE Transactions on Parallel and Distributed Systems,,23(12):2231-2244.2

Oliveira, P. F., Lima, L., Vinhoza, T. T. V., Barros, J., and Medard, M. (2010). Trusted Storage over Untrusted Networks. Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE, pages 1-5.

Myagmar, S. (2005). Threat Modeling as a Basis for Security Requirements. In StorageSS '05: Proceedings of the 2005 ACM workshop on Storage security and survivability, pages 94-102.

Shostack, A. (2008). Experiences threat modeling at Microsoft. CEUR Workshop Proceedings, 413:1{11.

Saini, V., Duan, Q., and Paruchuri, V. (2008). Threat modeling using attack trees. Journal of Computing Sciences, (APRIL):124-131.

Oladimeji, E. a., Supakkul, S., and Chung, L. (2006). Security threat modeling and analysis: A goal-oriented approach. Proc of the 10th IASTED International Conference on Software Engineering and Applications SEA 2006, pages 13-15.

Sodiya, A. S., Onashoga, S. A., and Oladunjoye, B. A. (2007). Threat modeling using fuzzy logic paradigm. Informing Science: International Journal of an Emerging Transdiscipline, 4(1):53-61.

Hussain, S., Kamal, A., Ahmad, S., Rasool, G., and Iqbal, S. (2014). Threat Modelling Methodologies: a Survey. 26(4):1607-1609.

Tondel, I. A., Jaatun, M. G., and Meland, P. H. (2008). Security requirements for the rest of us: A survey. IEEE Software, 25(1):20-27.

Open Web Application Security Project (OWASP). Application Threat Modeling. Available at: https://www.owasp.org/index.php/Application_Threat_Modeling

EU directive 95/46/EC. Available at: http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

Finnish Personal Data Act (523/1999). Available at: www.finlex.fi/en/laki/kaannokset/1999/19990523

National Institute of Standards and Technology (NIST), “SP 800-53 Rev.4 – Security and Privacy Controls for Federal Information Systems and Organizations,” Natl. Inst. Stand. Technol. – Spec. Publ., vol. 800-53, pp. 1-460, 2014.

Cloud Security Alliance, “Cloud Controls Matrix, Version 1.2”, Aug. 2011; https://cloudsecurityalliance.org/research/initiativesccm.

Valentina Casola, Alessandra de Benedictis, Massimiliano Rak,” On the Adoption of Security SLAs in the Cloud”, Springer International Publishing, 2015

Jesus Luna, Neeraj Suri, Michaela Iorga and Anil Kamel, “Leveraging the Potential of Cloud Security Service Level Agreements through Standards”, IEEE Cloud Computing Magazine, Volume 2, Issue 3, Pages 32-40, July 2015

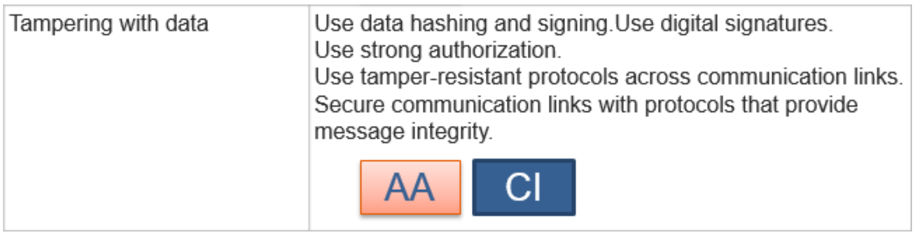
Valentina Casola, Alessandra De benedictis, Massimiliano Rak and Umberto Villano, “SLA-based Secure Cloud Application Development: the SPECS Framework”, In MICAS 2015, Timisoara, 21-22 September 2015.

Bernsmed, K., Hakon Meland, P., Gilje Jaatun, M. (2015). Cloud Security Requirements. SINTEF ICT, Norway, 2015

APPENDIX

Table 2: Multi-cloud security requirements matrix (Excerpt)

		DB	JP	TSMe	CE	IAM
Security Requirement		**DataBase**	**Journey Planner**	**TSM engine**	**Consumption Estimator**	**Identity/ Access Manager**
Data Storage Requirements	Back-up (S1)	(S1)				(S1)
	Encryption (S2)	DB.S, DB.T, DB.I				IAM.S, IAM.T, IAM.I
	Location (S3)	(S3)				(S3)
Data Processing Requirements	Isolation (P1)					
	Monitoring (P2)	(P2)	(P2)	(P2)	(P2)	(P2)
	Location (P3)	(P3)		(P3)		(P3)
	Forensics (IR4)					



Tampering with data	Use data hashing and signing.Use digital signatures. Use strong authorization. Use tamper-resistant protocols across communication links. Secure communication links with protocols that provide message integrity.

Figure 2: Threat category, main countermeasures identification, classes of issues (Excerpt)

Table 3: Threats, Requireents and Countermeasures (Excerpt)

Property	CONTROL GROUP	NIST SP800-53 R3
Data hashing **Digital signature**	Encryption & Key Management Encryption	SC-13 SC-8
	Identity & Access Management Audit Tools Access	AU-9
Strong authorization	Identity & Access Management User Access Authorization	AC-3 AC-6
	Identity & Access Management User Access Restriction / Authorization	IA-5 (IA-5(1-12))
Message integrity protocols	Encryption & Key Management Encryption	SC-8 SC-16
	Identity & Access Management Audit Tools Access	AU-9