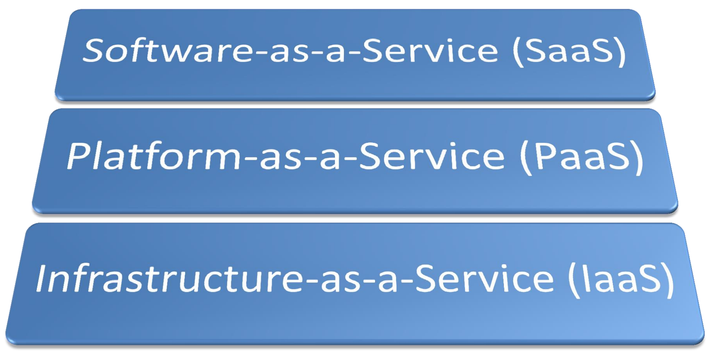
Selected security and privacy challenges in the Cloud

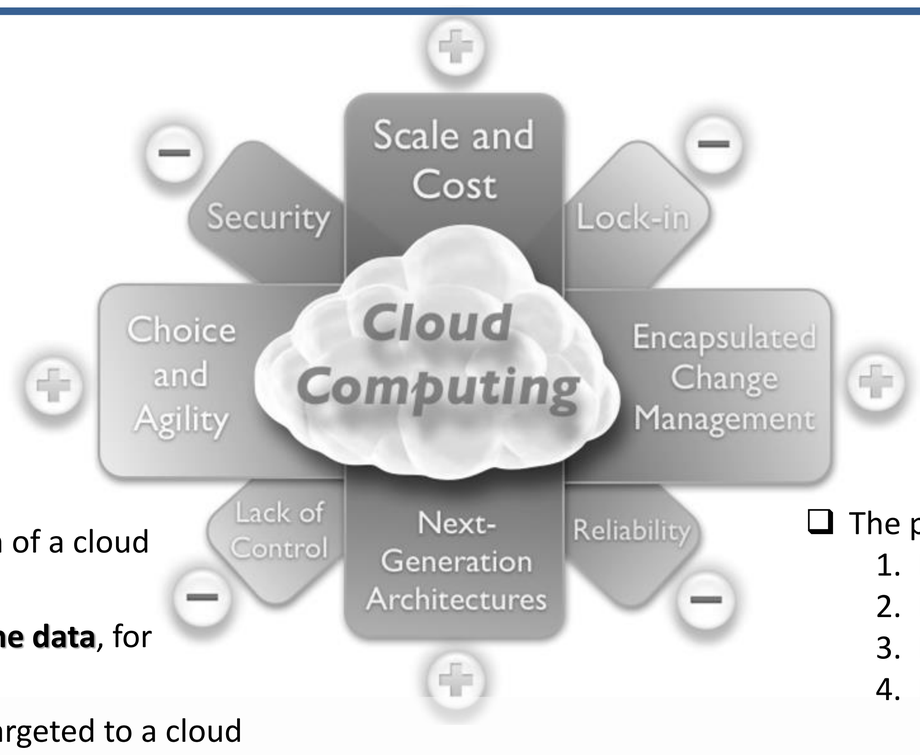
Nikolaos Tsalis, Nikos Virvilis

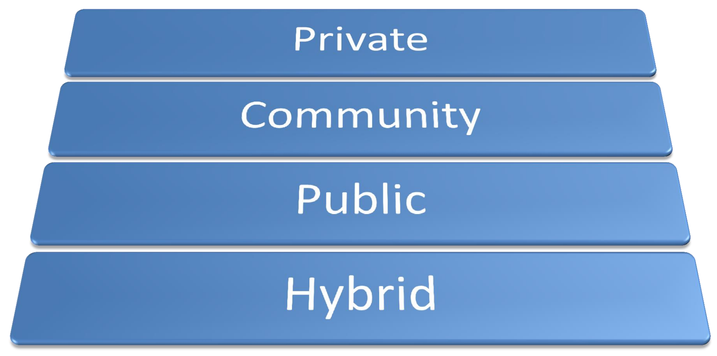
{ntsalis, nvir}@aueb.gr

Information Security & Critical Infrastructure Protection Research Laboratory

Dept. of Informatics, Athens University of Economics & Business (AUEB), Greece







Risk-Assessment-as-a-Service

A risk assessment method can be implemented in the form of a cloud service [1], which includes:

- ❑ Dynamic and continuous collection of accurate **real-time data**, for specific deployments, tenants, and assets.
- ❑ Comprehensive **qualitative and quantitative metrics**, targeted to a cloud environment.
- ❑ A **knowledge base** (e.g. ontologies [2]) that cumulates the knowledge by public available resources and modeling tools to mitigate applicable threat.

Figure 1: *Implementing RAaaS*

Cloud migration

- ❑ The process of the ***cloud migration decision*** includes [3]:
  1. Definition of deployment profile
  2. Definition of a set of controls
  3. Evaluation of benefit and cost metrics
  4. Evaluation of the Return on Security Investment (RoSI)

Cloud security metrics

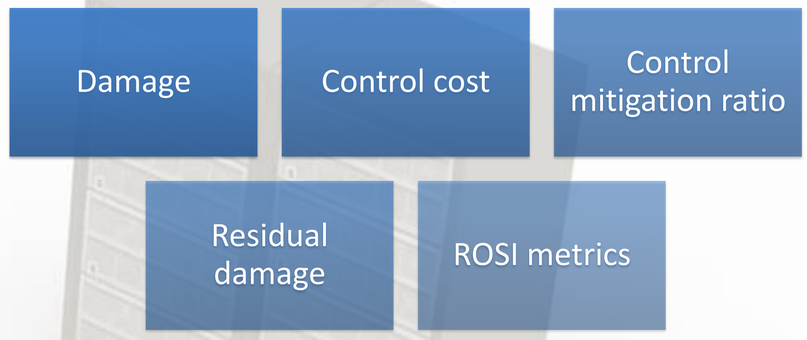


Figure 3: *ROSI assessment*

Security Threat Categorization

The available cloud security threats are categorized by [1] into ***network-related***, ***system or data-oriented***, ***organizational***. Thus, each threat is mapped to vulnerabilities examples and whether it affects the baseline security attributes, i.e. ***Confidentiality (C)***, ***Integrity (I)***, and ***Availability (A)***.

Threat	Vulnerability	C	I	A
T1. Malicious probes or scans	• Open ports • Unavailable or misconfigured IDS	✓		
T2. Cross-VM attack via side channels	• Multi-tenancy	✓	✓	✓
T3. Data leakage T4. Man-in-the-middle	•Communication encryption vulnerabilities • Weak authentication mechanism • Poor patch management	✓	✓	✓

Figure 2: *Network-related Cloud Threats*

Privacy threats and vulnerabilities

According to CSA [4], several ***top security identified threats*** refer to information disclosure, placing privacy as a top priority:

- ❑ Data Breaches/Leakage
- ❑ Account or Service Traffic Hijacking
- ❑ Insecure Interfaces and APIs
- ❑ Shared Technology Vulnerabilities
- ❑ Malicious Insiders
- ❑ Insufficient Due Diligence

Also, [5] was based on both the above mentioned threats and [6] in order to create a detailed and thorough mapping for each threat:

Vulnerability	CCM Code	Client	CSP	Infrastructure	Data	Software	Network
Undocumented data flows	-	×	×		×	×	×
Insecure or ineffective data disposal	DG-05		×		×	×	
Lack of or weak data leakage controls	DG-07		×		×	×	

Figure 4: *Data breaches or leakage threat*

A cloud provider-agnostic secure storage protocol

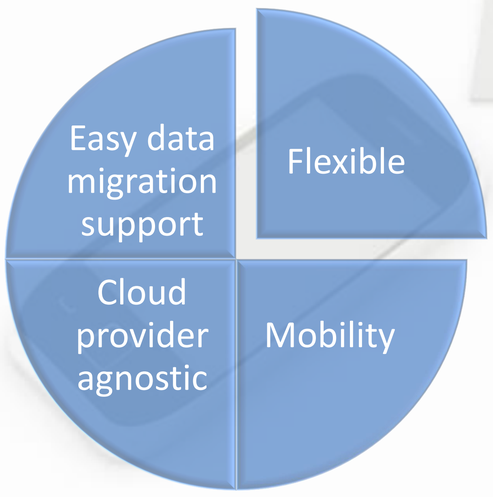


Figure 5: *Model's properties*

- ❑ A model [7] for outsourcing both static and dynamic data to third parties, while preserving their ***confidentiality*** and ***integrity***.
- ❑ Cloud-provider ***transparent-agnostic***, i.e. it can be used with ***any cloud provider***.
- ❑ Supports ***dynamic data management***, allowing users to update, delete or append new data and facilitating file sharing between users.

Procedural steps

1. The ***file is split into fixed size chunks***.
2. A ***MAC*** (Message Authentication Code) of each chunk is computed.
3. ***Each chunk is encrypted*** using a symmetric algorithm and a second randomly generated key.
4. The links between the correct order of the chunks and the random name are stored on a file called ***Index File***.
5. The ***index file is encrypted*** using the client's public key.
6. The ***encrypted chunks*** and the ***index file*** are ***uploaded on the cloud provider*** in random order.

Some early conclusions

- ❑ Existing ***cloud risk assessment*** approaches are considered premature, mainly due to the antithesis of the ***static nature of the procedure*** and the ***dynamic features of the cloud***.
- ❑ ***Cloud migration*** is a complex decision, while the tenant must fully understand the underlying ***threats, vulnerabilities and existing controls*** of such an environment.
- ❑ ***Proposed solutions*** should ensure the preservation of the security attributes, i.e. ***confidentiality***, ***integrity*** , and ***availability***.
- ❑ The ***provided controls*** in a CSP should be evaluated on a ***cost-benefit basis***, while existing research is in a still early stage.

This topic combines well with some of the security-focused publications of our Lab [8-10].

References

1. Theoharidou, M., Tsalis, N., Gritzalis, D., "In Cloud we Trust: Risk-Assessment-as-a-Service", 7th IFIP International Conference on Trust Management, pp. 100-110, Springer (AICT 401), 2013.
2. Dritsas, S., Tsoumas, B., Dritsou, V., Konstantopoulos, P., Gritzalis, D. "OntoSPIT: SPIT management through ontologies", Computer Communications, vol. 32, no. 1, pp. 203-212, 2009.
3. Martens, B., Teuteberg, F., "Decision-making in cloud computing environments: A cost and risk based approach," Information Systems Frontiers, vol. 14, no. 4, pp. 871-893, 2012.
4. CSA, "The notorious nine: Cloud computing top threats in 2013", v.1.0, Cloud Security Alliance, February 2013. Available: http://cloudsecurityalliance.org/research/top-threats/
5. Theoharidou, M., Papanikolaou, N., Pearson, S., Gritzalis, D., "Privacy risks, security and accountability in the Cloud", 5th IEEE Conference on Cloud Computing Technology and Science, IEEE Press, 2013.
6. CSA, "Security guidance for critical areas of focus in cloud computing," v3.0, Cloud Security Alliance, November 2011. Available: http://www.cloudsecurityalliance.org/guidance/
7. Virvilis, N., Dritsas, S., Gritzalis, D., "A cloud provider-agnostic secure storage protocol", 5th International Conference on Critical Information Infrastructure Security, pp. 104-115, Springer (LNCS-6712), 2010.
8. Mylonas, A., Dritsas, S., Tsoumas, B., Gritzalis, D., "On the feasibility of malware attacks in smartphone platforms", 9th International Conference on Security and Cryptography, pp. 217-232, Springer (CCIS-314), 2012.
9. Theoharidou, M., Mylonas, A., Gritzalis, D., "A risk assessment method for smartphones", 27th IFIP International Information Security and Privacy Conference, pp. 443-456, Springer (AICT 267), Greece, June 2012.
10. Gritzalis, D., "Embedding privacy in IT applications development", Information Management & Computer Security, vol. 12, no. 1, pp. 8-26, 2004.