Secure Use of Cloud Computing for Critical Infrastructures

Martin Gilje Jaatun
Software Engineering, Safety and Security
SINTEF Digital
Trondheim, Norway
Email: Martin.G.Jaatun@sintef.no

INVITED TALK EXTENDED ABSTRACT

I. Introduction

Depending on who you ask, Cloud Computing was either something that emerged as a paradigm shift about a decade ago, or alternatively it is just the last in a long line of incremental developments in how we do computing since the 1950-ies. Be that as it may, it is nonetheless clear that the cloud is not in your basement; if you are using cloud computing, your data is being processed and stored on somebody else's computer.

There has been a fair bit of concern regarding end-user privacy and holding cloud providers to account for how they manage personal data in the cloud [1], but for critical infrastructure it's less about privacy and more about societal impact. However, some critical infrastructure services are also tightly interwoven with the lives of citizens, and so the privacy aspect can often not be ignored.

Frequently, critical infrastructures find themselves "inadvertently" procuring cloud services through a third party that is not nominally a cloud service provider, as illustrated in Fig. 1. The third party will typically provide a Software-as-a-Service (SaaS) application that in turn uses other cloud processing or storage services in a provider chain as indicated in the figure. This has previously been identified as an accountability challenge [1], but is just as relevant when critical societal functions may be impacted. The solutions most commonly seen typically involve export of time series data from, e.g., SCADA systems for off-site "number crunching", and it is easy to assume that as long as the export is "secure" (i.e., that there is no way for an attacker to abuse the communication path out of the critical infrastructure in order to gain access from the outside), the security risk is negligible. However, the point of doing the analysis is invariably to support decisions regarding operation of the critical infrastructure, and thus tampering with the data once exported may cause real damage further down the line.

II. Background

There are a number of standards and good practice documents that provide requirements and guidance on general cloud security. ISO/IEC 27017 [3] has been co-developed with the International Telecommunication Union (ITU), and provides additional controls for applying ISO/IEC 27002 [4] to cloud

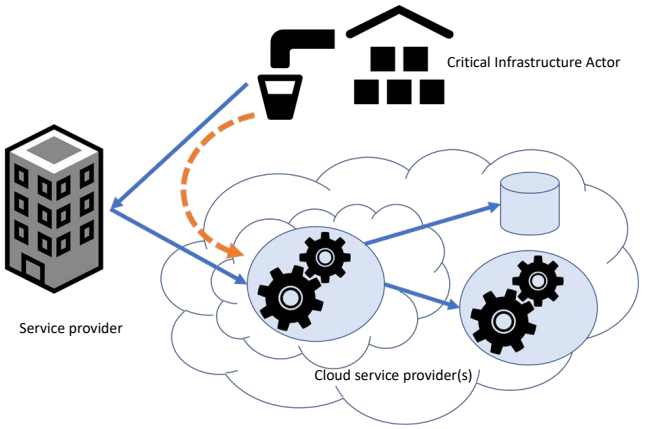

Fig. 1: Conceptual model of offering cloud services to critical infrastructure [2]

services. The Cloud Security Alliance (CSA) has created the Cloud Controls Matrix (CCM) [5] which covers both of the former, and more.

In Europe, the General Data Protection Regulation [6] received far more attention than the EU NIS Directive [7], but the latter is extremely relevant for any critical infrastructure in Europe. The NIS Directive defines Cloud Computing in much the same terms as the generally accepted NIST definition [8], and mentions cloud services in a couple of places. The NIS Directive indicates that public administrations should be able to ask cloud service providers "additional security measures beyond what [they] would normally offer", but does not go into details what these measures might be. The directive also states that member states can enforce their own national security requirements on cloud services.

The current situation is that the majority of the large cloud providers are not based in Europe, and this makes it increasingly likely that unless great care is taken, a large part of the cloud provider chain illustrated in Fig. 1 will physically reside outside Europe. This represents a jurisdictional challenge, and recent events [9] have sown doubts about to what extent US cloud providers can handle personal data of European citizens. Critical infrastructure providers thus need to think carefully

TABLE I: Requirements related to data processing

Category	Description	Requirement
Isolation	*Ensure that all data is isolated from other customers' data*	
		All in-memory data shall be segregated from data belonging to other customers
		The cloud provider must implement mechanisms that ensure that different virtual machines do not influence each other
		Data sent to the cloud service related to a specific request are not visible to other users of the service
Monitoring	*Ensuring that breaches of permissible use agreements are detected*	
		Behaviour of running virtual machines (VMs) shall be monitored continuously
Physical location	*Ensure data is processed in a specific geographic location*	
		As a rule, all data should be processed in data centres based in Europe
Migration	*Ensure that migration between different physical servers is performed securely*	
		All VMs must be encrypted during migration

about the requirements that they will pose to cloud service providers.

III. Cloud Security Requirements

Based on the previous section, it is clear that it is expected that cloud providers offering services to a critical infrastructure will be presented with additional security requirements, but it is not immediately obvious what these requirements might be. Røstum and Jaatun [2] provide a selection of requirements (based on a by now partly outdated report by Bernsmed et al. [10]) that could be relevant for a water network operator. In the following (see Table I, II, III and IV) we will present a selection of these requirements, focusing on those that have relevance to a broader set of European critical infrastructures.

Note that the requirements are not specific on, e.g., what encryption algorithms or key lengths are mandated. Each critical infrastructure operator needs to establish what represents current good practice - currently, 128-bit AES remains a reasonable choice for symmetric encryption [11], but this is a moving target, and everything may change quickly once quantum computing becomes generally available [12].

This also holds true for requirements specifying frequency of, e.g., backups; the actual frequency is highly dependent on the type of critical infrastructure and type of cloud service.

TABLE II: Requirements related to data transfer

Category	Description	Requirement
Encryption	*Ensure that data is not transferred in clear text*	
		Up- and downloading of data to/from the cloud service is encrypted
		All communication stages should be encrypted
		End-to-end encryption shall be used whenever possible
Integrity	*Ensure correctness and consistency in customer data*	
		Up- and downloading of data to/from the cloud service is integrity protected
Isolation	*Ensure that all data is isolated from other customers' data*	
		The cloud service provider offers network isolation between customers, ensuring that no data traffic to/from one customer can be eavesdropped on by another

TABLE III: Requirements related to access control

Category	Description	Requirement
Access control for administration	*Ensure secure access to the cloud administrative interface (dashboard)*	
		The cloud provider shall enforce a good practice password policy, focused on length and complexity of passwords
		The cloud provider shall support multi-factor authentication
		The cloud provider shall support third-party authentication solutions for simple login (SAML/OpenID)
Access control for users	*Ensure secure access for cloud users*	
		The cloud provider shall provide a system for creating, updating, suspending and deleting user accounts, to remove access of employees when they leave the organization
		All cloud users should have unique user accounts; no joint accounts are to be used
		Access to cloud services should be role-based

IV. Discussion

A cloud service provider will implement several layers of security that will protect against different types of attack, as illustrated in Fig. 2. Normally, any cloud provider that adheres to good practice according to, e.g., CSA [5] or ISO [3] will have these covered, but critical infrastructure providers that

TABLE IV: Requirements related to data storage

Category	Description	Requirement
Encryption	*Ensure that data is not stored in clear text when not in use*	
		All data is encrypted when stored. Disk encryption is sufficient (including virtual disks)
		Data from each infrastructure operator must be encrypted with separate encryption keys
Physical location	*Ensure data is stored in a specific geographic location*	
		As a rule, cloud providers based in Europe should be preferred
Isolation	*Ensure that all data is isolated from other customers' data*	
		Information must be segmented in such a manner that all data from a given critical infrastructure provider is segregated from data belonging to other customers
Ownership	*Ensure that the customer retains ownership of own data*	
		All data stored in the cloud solution remains the property of the critical infrastructure provider
		A data processing agreement shall be entered into with the supplier. This can be with a third party that develops services using a cloud service provider, or directly with the cloud service provider itself
		The cloud service provider may not use data from the critical infrastructure provider for the former's own purposes
Portability	*Ensuring portability of customer data*	
		Data must not be locked in on the cloud provider's platform, but must be exportable to a pre-agreed (preferably open) format on demand
Integrity	*Ensure correctness and consistency in customer data*	
		Integrity is maintained for all data stored in the cloud solution
Deletion	*Ensure proper deletion of all data upon customer request*	
		All replicated data shall be deleted within a specified deadline when requested by customer
Backup	*Ensure backup is performed and maintained in a proper manner*	
		The cloud solution shall create backups at least [daily][1]
		A local (off-cloud) backup of the cloud data shall be performed at least [weekly][1] – this should be usable also when the cloud service is not available.
		A detailed scheme for how long backups should be retained must be devised. E.g., daily backup: 21 days; weekly backup: 12 weeks; monthly backup: 6 months; quarterly backup: two years
		Backups stored in the cloud must be checked by restoring to shadow system at least monthly
		Local (off-cloud) backup must be checked [weekly] (when it is created)
		The cloud provider shall commit to a guaranteed maximum time for restoring of backup copy
		Backup copies must be stored geo-redundant with respect to where they are normally stored

make unverified assumptions with respect to the compliance of their cloud service provider do so at their peril.

The NIS Directive [7] indicates that national security requirements may be imposed on cloud service providers, but the jurisdictional challenges represented by overseas providers are likely to make this interesting, to say the least.

Considering that the cloud-specific guidance in official EU documents [7] is so vague, there might be a market for more concrete guidelines tailored to various critical infrastructures. The suggestions provided here barely scratch the surface, but they could provide a starting point in conjunction with the good practice publications mentioned above.

V. Conclusion

Cloud services are global in nature, and a cloud provider chain that starts in one country is likely to cross several borders, both inside Europe and beyond. Critical infrastructures are already using the cloud for a myriad of tasks, and this will only increase in the future. The relevant players need to embrace this fact, and work actively toward standards and guidelines that allow them to use the cloud in an acceptably secure manner.

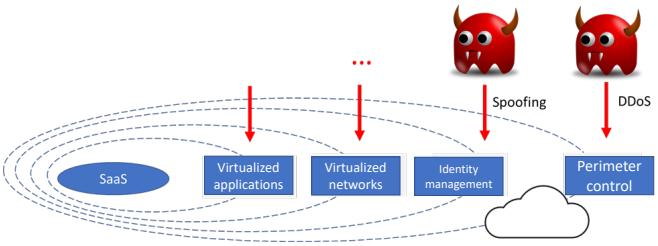

Fig. 2: Layers of security controls in the cloud [2]

Keywords—Cloud computing, critical infrastructure, security

ACKNOWLEDGMENTS

This talk is based on research funded by the Norwegian Petroleum Safety Authority; Norwegian Water; and the European Commission through the STOP-IT project, grant no. 740610.

BIOGRAPHY

MARTIN GILJE JAATUN [SM] is an adjunct professor at the University of Stavanger, and a senior scientist at SINTEF Digital in Trondheim, Norway. He is vice chair of the IEEE Computer Society Technical Committee on Cloud Computing (TCCLD) and an IEEE Cybersecurity Ambassador.

REFERENCES

[1] M. G. Jaatun, S. Pearson, F. Gittler, R. Leenes, and M. Niezen, "Enhancing accountability in the cloud," *International Journal of Information Management*, 2016. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0268401216301475

[2] J. Røstum and M. G. Jaatun, "Informasjonssikkerhet og skybaserte tjenester for vannbransjen (in Norwegian)," Tech. Rep., May 2018, rapport 238/2018. [Online]. Available: https://norskvann.no/index.php/kompetanse/va-bokhandelen/produkt/681-a238-informasjonssikkerhet-og-skybaserte-tjenester-for-vannbransjen

[3] ISO, "Information technology – security techniques – code of practice for information security controls based on ISO/IEC 27002 for cloud services," ISO/IEC Standard 27017:2015, 2018. [Online]. Available: https://www.iso.org/standard/43757.html

[4] ——, "Information technology – security techniques – code of practice for information security controls," ISO/IEC Standard 27002:2013, 2013. [Online]. Available: https://www.iso.org/standard/54533.html

[5] Cloud Security Alliance, "Cloud Controls Matrix." [Online]. Available: https://cloudsecurityalliance.org/artifacts/cloud-controls-matrix-v3-0-1/

[6] European Commission, " Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) ," 2016. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2016/679/oj

[7] ——, "Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union," 2016. [Online]. Available: https://eur-lex.europa.eu/eli/dir/2016/1148/oj

[8] P. Mell and T. Grance, "The NIST definition of cloud computing," NIST Special Publication 800-145, 2011.

[9] F. Gilbert, "What Schrems 2 Means for your Privacy Shield Program," CSA Blog. [Online]. Available: https://cloudsecurityalliance.org/blog/2020/08/10/what-schrems-2-means-for-your-privacy-shield-program/

[10] K. Bernsmed, P. H. Meland, and M. G. Jaatun, "Cloud security requirements," Tech. Rep., August 2015, report number A27131. [Online]. Available: https://infosec.sintef.no/wp-content/uploads/2015/08/Cloud-Security-Requirements-v2.0.pdf

[11] E. Barker and A. Roginsky, "Transitioning the use of cryptographic algorithms and key lengths," National Institute of Standards and Technology, Tech. Rep., 2018. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-131Ar2.pdf

[12] V. Mavroeidis, K. Vishi, M. D. Zych, and A. Jøsang, "The impact of quantum computing on present cryptography," *International Journal of Advanced Computer Science and Applications*, vol. 9, no. 3, 2018. [Online]. Available: http://dx.doi.org/10.14569/IJACSA.2018.090354