Critical Infrastructures in the Cloud

Martin Gilje Jaatun$^{orcidID\ 0000-0001-7127-6694}$ and Geir Kjetil Hanssen$^{OrcidID\ 0000-0003-2718-6637}$

Abstract Cloud computing is increasingly being used not only to support critical infrastructure applications, but actually forms a vital part of them. This paper discusses challenges faced by custodians of critical infrastructures when moving to the cloud, and outlines some security requirements that are relevant to apply to critical infrastructure cloud applications.

Key words: Cloud computing, cybersecurity, security, critical infrastructure, industrial control systems, IEC 62443

1 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 – and possibly in another legislative domain.

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 [15], but for critical infrastructure it's less about privacy and more about societal impact. However, some critical infrastructure services are also

Martin Gilje Jaatun
SINTEF Digital, Trondheim, Norway, e-mail: martin.g.jaatun@sintef.no

Geir Kjetil Hanssen
SINTEF Digital, Trondheim, Norway, e-mail: geir.k.hanssen@sintef.no

tightly interwoven with the lives of citizens, and so the privacy aspect can often not be ignored.

Traditional critical infrastructures include electric power distribution, telecommunications, and water distribution networks [7]. Another example is the exploration and production of oil- and gas resources in challenging environments, like at offshore installations [10]. With the possible exception of telecommunications, these have been considered rather conservative and staid institutions, more characterized by ”business as usual” than ”agility”.

Frequently, driven by a growing need for more computational services, critical infrastructure custodians 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 is sometimes referred to as ”mashups” or ”federated services”, where service elements are dynamically composed to form a complex internet service [18]. This has previously been identified as an accountability challenge [15], 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.

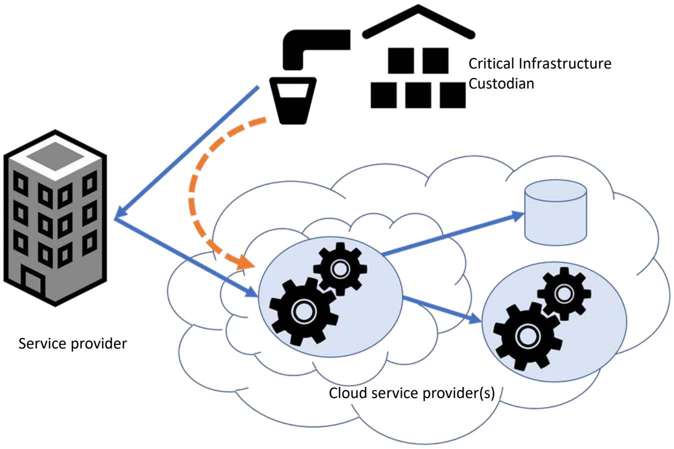


Fig. 1 Conceptual model of offering cloud services to critical infrastructure [21]

This potential weakness in the flow of data *out* of a the organization, to an external cloud-based service provider, and back *into the organization*, was highlighted within a study initiated by the Norwegian Petroleum Authority in 2020 [10]. The hypothetical (but realistic) case was that data is gathered from, e.g., sensors or edge-devices at the so-called 'sharp end' within the operational organization, e.g. at the drilling deck on an oil rig. Then, data are transferred outside the organization to a cloud-based service provider, e.g. providing operator-support services, that in return, is fed back into the orgainzation and for example, made accessible to the operator via a tablet. Then, the operator uses this information to make decisions about the activities at the drilling deck. Such a scenario may seem secure and safe as the data may be well protected within the organization; oil and gas installations meet very high cybersecurity standards and have numerous security measures, e.g. separation between information technology – IT, and operational technology - OT. Furthermore, the scenario may seem technically sound and safe since the services that are provided (by the external cloud-based service provider) have no technical interface with any of the internal systems. However, because the data to and from the cloud-based provider travel via the Internet, there is a theoretical probability that someone may tamper with the data, either out- or in-going. And reaching all the way to the sharp- and critical end of the operational organization, wrong data (or operator support) may lead to hazardous events, potentially life threatening.

The sceptical reader may argue that this constructed scenario is exaggerated and not realistic. However, we believe it illustrates the general trend within critical domains and infrastructures, where the access to rich data is growing rapidly. This is followed by new technology and computational capacity to exploit data, typical via cloud-based resources and AI solutions. In short, data can be used to digitally transform and enhance businesses – in search for more efficient and profitable operations. An example taken from the oil- and gas domain, is that ”intelligent oil fields” can increase productivity by 2-8%, with 2-6% better extraction [16].

With this backdrop, we look into the case of security in critical infrastructures that interface with the cloud. Our aim is to highlight the need for well-considered cybersecurity measures and strategies, and to invite the research community in developing an understanding of this emerging challenge, and the countermeasures that should compensate for the risks.

2 Background

There are a number of standards and good practice documents that provide requirements and guidance on general cloud security. ISO/IEC 27017 [14] has been co-developed with the International Telecommunication Union (ITU), and provides additional controls for applying ISO/IEC 27002 [13] to cloud services. The Cloud Security Alliance (CSA) has created the Cloud Controls Matrix (CCM) [3] which covers both of the former, and more.

In Europe, the General Data Protection Regulation [4] received far more attention than the EU NIS Directive [5] (also known as NIS1). NIS1 only mentions ”cloud” 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 second version of the NIS-directive (NIS2) [6] mentions cloud specifically in recital 33, 34, 35, 113, 114, 116, and 117. These mentions group cloud providers with any other service providers, and specify that for a cloud provider, the competent national authority will be the EU country where the cloud provider has their main establishment.

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

Most critical infrastructures have primarily been focused on Operational Technology (OT) rather than Information Technology (IT), and the premier OT security standards can be found in the IEC 62443 standards series [11]. IEC 62443 is still under development and does not actually discuss cloud solutions, but IEC 62443-3-2 [12] mentions that ”the [System Under Consideration] may include [...] emerging technologies such as [...] cloud-based solutions”.

3 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 [21] provide a selection of requirements (based on a by now partly outdated report by Bernsmed et al. [2]) that could be relevant for a water network operator. In the following (see Section 3.1, 3.2, 3.3 and 3.4) 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 custodian of a critical infrastructure needs to establish what represents current good practice – currently, 128-bit AES remains a reasonable choice for symmetric encryption [1], but this is a moving target, and everything may change quickly once quantum computing[1] becomes generally available [17].

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.

3.1 Requirements related to data processing

- 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[2]
- Migration – *Ensure that migration between different physical servers is performed securely*
  - All VMs must be encrypted during migration

[1] Generally, the public-key algorithms based on the hard problems of integer factorization and discrete log (RSA, Diffie-Hellman) will be trivially broken, and most symmetric algorithms (such as AES) will need to double their key size.

[2] This assumes that the critical infrastructure in question is based in Europe – in the general case, it will be an advantage that the cloud provider is located in the same jurisdiction as the critical infrastructure.

3.2 Requirements related to data transfer

- 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
    Integrity protection can be performed using different means, such as digital signatures, message authentication codes, and other combination of encryption mechanisms and hash functions.
- 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

3.3 Requirements related to access control

- 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 [19]/OpenID [20])
- 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
  - The principle of least privilege should be applied when assigning privileges to roles

3.4 Requirements related to data storage

- 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 custodian 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 (see also requirements to data storage)
- 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 (see data transfer requirements above)
- 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][3]
  - A local (off-cloud) backup of the cloud data shall be performed at least [weekly][3] – this should be usable also when the cloud service is not available.

[3] The actual frequency must be decided by the critical infrastructure custodian.

- 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

4 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 [3] or ISO [14] will have these covered, but critical infrastructure providers that make unverified assumptions with respect to the compliance of their cloud service provider do so at their peril. In many critical infrastructures, the concept of safety barriers has a long history, but with increased connectivity a need for specific cybersecurity barriers [22] has emerged. How such cybersecurity barriers can interact with cloud security controls remain a topic for future study.

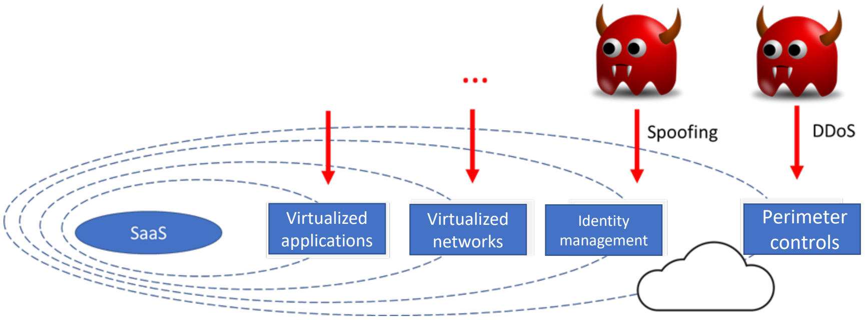
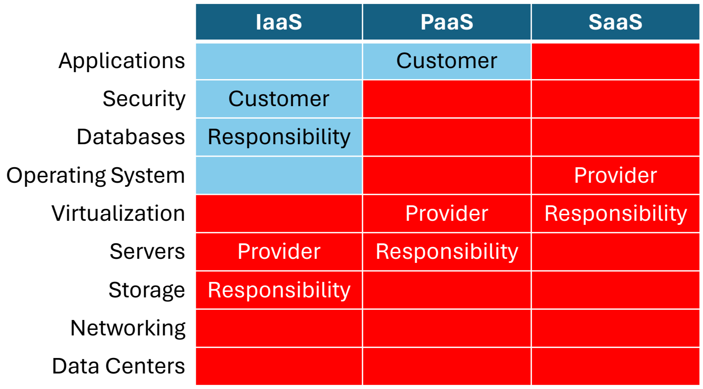


Fig. 2 Layers of security controls in the cloud [21]

Depending on the cloud service model that is applied, there will be different degrees of shared responsibility for cloud security between the cloud customer (i.e., the critical infrastructure custodian) and the cloud provider [9]. For the most part, we have assumed a Software-as-a-Service (SaaS) service model, in which case the responsibility rests solely on the cloud provider, but if a Platform-as-a-Service (PaaS) or Infrastructure-as-a-Service (IaaS) service model has been chosen, the cloud customer has to take increasing responsibility, as illustrated in Fig. 3.



	IaaS	PaaS	SaaS
Applications		Customer	
Security	Customer		
Databases	Responsibility		
Operating System			Provider
Virtualization		Provider	Responsibility
Servers	Provider	Responsibility	
Storage	Responsibility		
Networking			
Data Centers			

Fig. 3 Shared responsibility between cloud provider and cloud customer

The NIS1 Directive [5] indicated 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. Geopolitical events and shifting regimes have highlighted the challenges that are inherent in putting all your cloud eggs in a single foreign basket – after Russia's full-on invasion of Ukraine in February 2022, many organizations rushed to shift their operations from data centres in Ukraine to Western Europe. Many European players are also wary about recent developments in US politics, with fears that the next president will take the country in a non-democratic direction, with ensuing disregard for international law and existing bilateral agreements. This is effectively eroding the traditional trust that Europeans have had in US-based cloud services, and has fuelled the search for European[4] alternatives.

Considering that the cloud-specific guidance in official EU documents [5, 6] 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.

[4] For all practical purposes, this means the European Union and the European Economic Area (EU/EEA).

5 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.

Acknowledgments

This paper is based on research funded by the Research Council of Norway through the Cybersecurity Barrier Management project, grant no. 326717; the Norwegian Petroleum Safety Authority; Norwegian Water; and the European Commission through the STOP-IT project, grant no. 740610.

References

1. Barker, E., Roginsky, A.: Transitioning the use of cryptographic algorithms and key lengths. Tech. rep., National Institute of Standards and Technology (2018). URL https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-131Ar2.pdf
2. Bernsmed, K., Meland, P.H., Jaatun, M.G.: Cloud security requirements. Tech. rep., SINTEF ICT (2015). URL https://infosec.sintef.no/wp-content/uploads/2015/08/Cloud-Security-Requirements-v2.0.pdf. Report number A27131
3. Cloud Security Alliance: Cloud Controls Matrix. URL https://cloudsecurityalliance.org/artifacts/cloud-controls-matrix-v3-0-1/
4. 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). URL https://eur-lex.europa.eu/eli/reg/2016/679/oj
5. European Commission: 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). URL https://eur-lex.europa.eu/eli/dir/2016/1148/oj
6. European Commission: DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 december 2022 on measures for a high common level of cybersecurity across the union, amending regulation (EU) no 910/2014 and directive (EU) 2018/1972, and repealing directive (EU) 2016/1148 (NIS 2 Directive) (2022). URL https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2555
7. George, R.: Critical infrastructure protection. International Journal of Critical Infrastructure Protection **1**, 4–5 (2008). DOI https://doi.org/10.1016/j.ijcip.2008.08.010. URL https://www.sciencedirect.com/science/article/pii/S1874548208000061

8. Gilbert, F.: What Schrems 2 Means for your Privacy Shield Program. CSA Blog. URL https://cloudsecurityalliance.org/blog/2020/08/10/what-schrems-2-means-for-your-privacy-shield-program/
9. GSA: Cloud basics — cloud information centre. URL https://cic.gsa.gov/basics/cloud-basics
10. Hanssen, G.K., Onshus, T., Jaatun, M.G., Myklebust, T., Ottermo, M.V., Lundteigen, M.A.: Principles of digitalisation and IT-OT integration. Tech. rep., SINTEF Digital (2023). URL https://ntnuopen.ntnu.no/ntnu-xmlui/handle/11250/3127881
11. IEC: IEC/TS 62443-1-1:2009 Security for industrial automation and control systems - Part 1-1: Terminology, concepts and models (2009)
12. IEC: IEC 62443-3-2:2020 Security for industrial automation and control systems - Part 3-2: Security Risk assessment for system design (2020). URL https://webstore.iec.ch/publication/30727
13. ISO: Information technology – security techniques – code of practice for information security controls. ISO/IEC Standard 27002:2013 (2013). URL https://www.iso.org/standard/54533.html
14. 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). URL https://www.iso.org/standard/43757.html
15. Jaatun, M.G., Pearson, S., Gittler, F., Leenes, R., Niezen, M.: Enhancing accountability in the cloud. International Journal of Information Management (2016). DOI http://dx.doi.org/10.1016/j.ijinfomgt.2016.03.004. URL http://www.sciencedirect.com/science/article/pii/S0268401216301475
16. Lu, H., Guo, L., Azimi, M., Huang, K.: Oil and gas 4.0 era: A systematic review and outlook. Computers in Industry **111**, 68–90 (2019)
17. Mavroeidis, V., Vishi, K., Zych, M.D., Jøsang, A.: The impact of quantum computing on present cryptography. International Journal of Advanced Computer Science and Applications **9**(3) (2018). DOI 10.14569/IJACSA.2018.090354. URL http://dx.doi.org/10.14569/IJACSA.2018.090354
18. Meland, P.H.: Composite services with dynamic behaviour. In: Secure and Trustworthy Service Composition: The Aniketos Approach, pp. 1–9. Springer (2014)
19. OASIS: Security Assertion Markup Language (SAML) v2.0 (2005). URL https://www.oasis-open.org/standard/saml/
20. OpenID: OpenID Foundation (2023). URL https://openid.net/
21. Røstum, J., Jaatun, M.G.: Informasjonssikkerhet og skybaserte tjenester for vannbransjen (in Norwegian). Tech. rep., Norsk Vann (2018). URL https://norskvann.no/index.php/kompetanse/va-bokhandelen/produkt/681-a238-informasjonssikkerhet-og-skybaserte-tjenester-for-vannbransjen. Rapport 238/2018
22. Øien, K., Hauge, S., Jaatun, M.G., Flå, L., Bodsberg, L.: A survey on cybersecurity barrier management in process control environments. In: 2022 IEEE International Conference on Cloud Computing Technology and Science (CloudCom), pp. 113–120 (2022). DOI 10.1109/CloudCom55334.2022.00026