INFINITY

IMMERSE. INTERACT. INVESTIGATE.

Technical Brief

State-of-the-Art Server Hosting Solutions and Data Protection Challenges and Opportunities

DISSEMINATION LEVEL PUBLIC

PARTNER

CyberPeace Institute

AUTHOR

Florent Bitschy

This project has received funding from the European Union’s Horizon 2020 Research and Innovation Programme under Grant Agreement No. 883293. The content of this document represents the view of the authors only and is their sole responsibility. The European Commission does not accept any responsibilty for any use that may be made of the information it contains.

1. Introduction[1]

Server hosting solutions are an integral part of the digital ecosystem, enabling businesses to host websites, applications, and services on remote servers. The rapid growth of digital services and the increasing demand for scalable, reliable, and cost-effective hosting solutions have driven significant innovation in this field.

In this state-of-the-art review, we explore the latest trends and advancements in server hosting solutions, focusing on cloud-based services, bare-metal servers, virtual private servers, and containerization. Additionally, we discuss the impact of edge computing, serverless computing, and green data centers on the future of server hosting.

In the second part of this brief, we also address data protection challenges and opportunities related to server hosting in the context of INFINITY.

2. State of the Art in Server Hosting Solutions

2.1 Cloud-based Services

Cloud-based hosting has emerged as a dominant solution due to its scalability, flexibility, and cost-effectiveness. The leading players in the market, such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP), offer a wide range of services, including Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS).

Some local solution exists in Europe, such as exoscale, digital ocean, and OVH.[2]

2.2 Bare-metal Servers

Bare-metal servers, also known as dedicated servers, provide users with exclusive access to a physical server's resources. These servers are ideal for resource-intensive applications and offer improved performance, security, and customization compared to shared hosting solutions.

2.3 Virtual Private Servers (VPS)

VPS hosting is a popular choice for small to medium-sized businesses that require more control and customization than shared hosting but do not have the resources for a dedicated server. VPS solutions utilize virtualization technology to partition a physical server into multiple virtual servers, each with its own operating system, resources, and software.

2.4 Containerization

Containerization technologies, such as Docker and Kubernetes, have gained traction in recent years for their ability to streamline the deployment and management of applications. Containers provide a lightweight, portable, and resource-efficient solution for hosting applications, allowing developers to package their applications with all the required dependencies and run them on any platform.

2.5 Edge Computing

The rise of edge computing has implications for server hosting solutions, as it brings computation and data storage closer to the source of data. Edge computing reduces latency, bandwidth usage, and the load on central data centers, enabling faster and more efficient hosting solutions for applications with real-time or near-real-time requirements.[3]

2.6 Serverless Computing

Serverless computing, as offered by platforms like AWS Lambda and Azure Functions, allows developers to build and deploy applications without the need to manage the underlying infrastructure. This approach can lead to lower costs, improved scalability, and reduced operational complexity.[4]

2.7 Green Data Centers

Sustainability and energy efficiency have become increasingly important in the server hosting industry, with major providers investing in renewable energy sources and green data center technologies. These initiatives not only reduce the environmental impact of data centers but can also lead to lower operational costs and improved performance.[5]

2.8 Conclusion

The server hosting landscape continues to evolve, driven by the increasing demands of businesses and the rapid advancements in technology. Cloud-based services, bare-metal servers, VPS, containerization, edge computing, serverless computing, and green data centers are shaping the future of server hosting. As businesses and developers continue to prioritize scalability, flexibility, and cost-effectiveness, we can expect to see further innovation and growth in this sector.

In view of ensuring good server performance with limited financial resource, Virtual Private Servers have been chosen a cost-effective solution in the case of the INFINITY project.

3. Data Protection

Hosting in Europe was the first option to protect data in accordance with the European General Data Protection Regulation 2016/679 (GDPR), but as explained below, US cloud providers could operate under the US Clarifying Lawful Overseas Use of Data Act (CLOUD Act). To ensure data protection in accordance with European standards, a European provider was selected for the INFINITY project.

In view of the Adequacy decision 2000/518/EC of the EU on the adequate protection of personal data provided in Switzerland, which allows to transfer data to Switzerland without requiring any further adequate data protection guarantees by contract, the INFINITY consortium made the decision to host the server in Switzerland with the provider exoscale.

3.1 GDPR vs CLOUD Act

The CLOUD Act was enacted in the United States in March 2018, allowing US law enforcement agencies to access data stored by US-based technology companies, regardless of where the data is physically stored. This legislation has raised significant concerns in the European Union (EU) about data protection and privacy, particularly in light of the EU's stringent data protection framework, the GDPR.

The GDPR, which came into effect in May 2018, is designed to protect the personal data of EU citizens and residents, giving them greater control over their data and imposing strict rules on organizations that collect, process, and store personal data. The GDPR also includes provisions on data transfers outside the EU, which are only allowed under specific circumstances and conditions.

The conflict between the CLOUD Act and the GDPR arises from the fact that US law enforcement agencies can request access to data stored by US-based companies, even if that data belongs to EU citizens and is stored within the EU. This situation can put US-based cloud service providers in a difficult position, as complying with a CLOUD Act warrant might result in a breach of the GDPR.

To address these concerns and ensure compliance with both the CLOUD Act and the GDPR, some measures have been taken:

- **EU-US Privacy Shield:** This framework was designed to enable companies on both sides of the Atlantic to transfer personal data between the EU and the US while ensuring adequate data protection. However, the Court of Justice of the European Union (CJEU) invalidated the Privacy Shield in July 2020 in a case known as "Schrems II" due to concerns about US surveillance practices and the lack of sufficient data protection guarantees.

- **Standard Contractual Clauses (SCCs):** SCCs are legally binding contracts between data controllers and processors or between data exporters and importers that ensure GDPR-compliant data transfers. Following the invalidation of the[8]Privacy Shield, SCCs have become the primary mechanism for transferring personal data from the EU to the US. However, companies relying on SCCs must assess whether the level of data protection in the destination country is adequate, which can be challenging due to the CLOUD Act.

- **Data Localization:** Some organizations choose to store their data within the EU to avoid potential conflicts between the CLOUD Act and the GDPR. This approach may provide a higher level of data protection, but it can also limit the scalability and flexibility of cloud-based services.

- **European Cloud Initiatives:** In response to concerns about data protection and sovereignty, the EU has launched several initiatives to foster the development of European cloud infrastructure and services, such as GAIA-X and the European Data Strategy. These initiatives aim to create a competitive and secure cloud ecosystem that complies with EU data protection regulations.

In conclusion, the CLOUD Act and the GDPR represent two different approaches to data protection and privacy, and navigating the legal complexities between them can be challenging for organizations. It is essential for companies that handle personal data of EU citizens to understand the requirements of both frameworks and implement appropriate measures to ensure compliance while minimizing potential conflicts.[6]

Examples of relevant use cases and legal conflicts:

- **Microsoft Ireland case (pre-CLOUD Act):** In 2013, the US government issued a warrant under the Stored Communications Act (SCA) for Microsoft to provide emails stored in a data center in Ireland. Microsoft challenged the warrant, arguing that US law did not have extraterritorial reach. The case reached the US Supreme Court, but the proceedings were rendered moot by the enactment of the CLOUD Act, which clarified that US law enforcement can access data stored abroad by US-based companies.[7]

- **Schrems II case:** Austrian privacy activist Max Schrems filed a complaint against Facebook Ireland with the Irish Data Protection Commissioner, arguing that Facebook's transfer of personal data from the EU to the US did not provide adequate data protection due to US surveillance practices. The case reached the Court of Justice of the European Union (CJEU), which invalidated the EU-US Privacy Shield in July 2020, effectively limiting the available mechanisms for transferring personal data between the EU and the US.[8]

These use cases demonstrate the complex legal landscape surrounding cross-border access to electronic evidence and the challenges faced by companies and governments in navigating the conflicting regulations of the CLOUD Act and the GDPR.

3.2 Conclusion: Future Challenges and Opportunities

The intersection of the CLOUD Act and the GDPR presents both challenges and opportunities for organizations, governments, and the technology industry as a whole. As global data flows continue to increase and the digital economy becomes more interconnected, striking the right balance between law enforcement needs, data protection, and privacy will be crucial.

Challenges:

- **Legal conflicts:** The conflicting requirements of the CLOUD Act and the GDPR pose significant legal challenges for organizations, particularly US-based technology companies that handle personal data of EU citizens. Navigating these complex regulations and finding ways to comply with both frameworks will remain a key challenge in the foreseeable future.

- **Data localization and fragmentation:** Concerns about data protection and privacy may lead to increased data localization efforts, which could hinder the free flow of data across borders and potentially result in a more fragmented digital ecosystem.

- **Trust in cloud services:** The potential for extraterritorial access to data by US law enforcement agencies under the CLOUD Act may undermine trust in US-based cloud service providers, driving customers to seek alternative solutions or local providers.

Opportunities:

- **Strengthening international agreements:** The current challenges highlight the need for stronger international agreements and frameworks that facilitate cross-border access to electronic evidence while ensuring adequate data protection and privacy. This can include updating mutual legal assistance treaties (MLATs), negotiating new data-sharing agreements, or developing new mechanisms like the proposed EU-US e-Evidence Agreement.

- **European cloud initiatives:** The legal conflicts between the CLOUD Act and the GDPR have spurred the development of European cloud initiatives like GAIA-X, which aim to create a competitive and secure cloud ecosystem that complies with EU data protection regulations. This presents an opportunity for European technology companies to innovate and capture a larger market share.

- **Enhanced privacy and security:** The ongoing debate about data protection and privacy may lead to increased awareness and demand for more privacy-centric solutions, driving innovation in technologies such as encryption, zero-knowledge proofs, and decentralized systems.

In conclusion, the conflicts between the CLOUD Act and the GDPR present a complex landscape of challenges and opportunities. To seize these opportunities and address the challenges, stakeholders, including governments, technology companies, and policy makers, will need to work collaboratively to develop balanced solutions that enable effective law enforcement, while safeguarding data protection and privacy in an increasingly interconnected digital world.

For a project like INFINITY, which deals with confidential data while addressing cybercrime, a European hosting solution ensures the adherence to high-level data protection standards.

References

1. This Technical Brief was prepared by the CyberPeace Institute, as part of T10.5.
2. Cf. Buyya, R., Yeo, C. S., Venugopal, S., Broberg, J., & Brandic, I. (2009), "Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility", in: Future Generation Computer Systems, 25(6), pp. 599-616, at: https://doi.org/10.1016/j.future.2008.12.001; and Morabito, V. (2017), "Trends and challenges in cloud datacenters", in: Cloud Computing, pp. 11-30, Springer, Cham., at: https://doi.org/10.1007/978-3-319-54645-1_2.
3. Cf. K. Cao, Y. Liu, G. Meng and Q. Sun (2020), "An Overview on Edge Computing Research", in IEEE Access, vol. 8, pp. 85714-85728, 2020, doi: 10.1109/ACCESS.2020.2991734, at: https://ieeexplore.ieee.org/document/9083958.
4. Cf. Brown, N., & Forsgren, N. (2018), State of DevOps Report, Puppet, Inc., at: https://puppet.com/resources/whitepaper/state-of-devops-report; see also Turner, M., Budgen, D., & Brereton, P. (2003), "Turning software into a service", in: Computer, 36(10), pp. 38-44, at: https://doi.org/10.1109/MC.2003.1236470.
5. Chen, H., Zhang, Y., & He, C. (2016), "Green Data Center: How green can we perform?", in: 2016 IEEE International Conference on Consumer Electronics-Taiwan (ICCE-TW), pp. 1-2, IEEE, at: https://doi.org/10.1109/ICCE-TW.2016.7520999.
6. Cf. inter alia, Schwartz, P. M., & Paul, M. (2018), Transatlantic data privacy law, Georgetown Law Journal, 106, 115-179, https://scholarship.law.georgetown.edu/cgi/viewcontent.cgiarticle=3012&context=facpub; Daskal, J. (2018), The CLOUD Act and the future of cross-border law enforcement requests for data, in: Lawfare, at: https://www.lawfareblog.com/cloud-act-and-future-cross-border-law-enforcement-requests-data; Van Alsenoy, B. (2019), "Microsoft Ireland, the CLOUD Act and the European Investigation Order: Analysing the legal framework for cross-border access to electronic evidence", in: Computer Law & Security Review, 35(1), 21-42. https://doi.org/10.1016/j.clsr.2018.05.015; and The Court of Justice of the European Union (2020), Judgment of the Court (Grand Chamber) in Case C-311/18 - Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems (Schrems II), at: http://curia.europa.eu/juris/document/document.jsftext=&docid=228677&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=9575854.
7. Cf. https://jusletter-it.weblaw.ch/en/issues/2020/fses/19_s_373_418_de-hert_29c39cf0a6.html.
8. Cf.https://epic.org/documents/data-protection-commissioner-v-facebook-and-max-schrems-standard-contractual-clauses/.