A Survey of Multiple Clouds: Classification, Relationships and Privacy Concerns

By: Reem Al-Saidi[1] and Ziad Kobti[1]

Presented by: Reem Al-Saidi.
alsaidir@uwindsor.ca

1 School of Computer Science, University of Windsor

June 26-30, 2023

Table of Contents I

Table of Contents II

Presenter Bio

- Reem is a Ph.D. student in Computer Science at the University of Windsor.
- Her main research interest focuses on privacy-preserving on Multi-Cloud computing, including Genetic and Single Sign On applications.
- Currently, she is working as a privacy and security team lead for a research project funded by IRCC, where she analyzes different scenarios for cyber security risks and is involved in different discussions with other teams.

Abstract

- Multiple clouds computing environments overcome the limitations of cloud computing and bring a wide range of benefits (e.g., avoiding vendor lock-in problem).
- Numerous applications can use various multiple clouds types depending on their specifications and needs.
- Deploying multiple clouds under hybrid or public models have introduced various privacy concerns that affect users and their data in a specific application domain.

Abstract

- The present study conducted a survey to identify the various classifications of multiple clouds types and then extend the cloud entities' relationships to behave in different multiple clouds settings.
- The survey results outline users' privacy and data confidentiality concerns in multiple clouds types under public and hybrid deployment models.

Survey Objectives

- Show the classification of multiple clouds types from the state-of-the-art work.
- Investigate the challenges for public and hybrid deployment models in multiple clouds types.
- Extend the single cloud entity' s relationships to behave in different types of multiple clouds environment.
- Identify the privacy concerns in the multi-cloud, federated, cross-federated, and inter-cloud under public and hybrid deployment models at some application domains

Introduction

- Utilizing numerous clouds has emerged as an alternative way to improve cloud computing capacity for massive and real-time data [1][2].
- Collaboration and communication between clouds, known as ” Cloud Interoperability” will improve data reliability and resource availability, resulting in highquality services [3].

Multiple cloud Challenges

- Despite multi-cloud resource availability, data reliability and scalability [3][4], maintaining **cloud interoperability** while preserving users' privacy and data security is still a significant challenge[5].
- Without the users' consent, their data can be stored in another CSPs with different access rules and data processing requirements [6]
- It becomes difficult to guarantee that data is effectively protected through its entire life-cycle, including data creation, storage, processing, transfer, and deletion; different CSPs may have different security policies, methods, and procedures for data processing and storage [5].

Multiple cloud Challenges

- It is also more challenging to guarantee the consistency of security policies across all CSPs during data transfer and access, and protect the data against potential threats [3][7].
- Moreover, identifying the access roles and sharing privileges among different CSPs[5] while maintaining user-sensitive attributes without performance degradation is another critical concern while deploying multiple clouds.

Multiple cloud Challenges in applications

- While multi-cloud facilitates seamless data exchange and sharing across different clouds, it also raises privacy and security concerns concerning data access and sharing processes .
- Unauthorized and unrestricted access could expose patient information, compromising privacy and confidentiality.
- Different application domains benefit from multiple clouds deployments [8][9][10].
- In the health era[10], various health institutions can share their data and collaborate with other researchers and healthcare professionals, enabling real-time collaboration and improving personal health and treatments.

Privacy and Security concerns

To sum up:

- Without question, user privacy and data security are of the highest importance in the digital age and have attracted much more attention to the adoption of multiple clouds computing.
- The success of such adoption toward building trustworthy multiple clouds environments are primarily driven by cloud user privacy and data security.

Multiple Cloud Classification

- There are several perspectives exist on classifying multiple clouds; some consider federated clouds as inter-cloud [11]. Others disagree and claim that federated cloud is a type of inter-cloud [12].
- Figure 1 shows the authors' classification of multiple clouds.

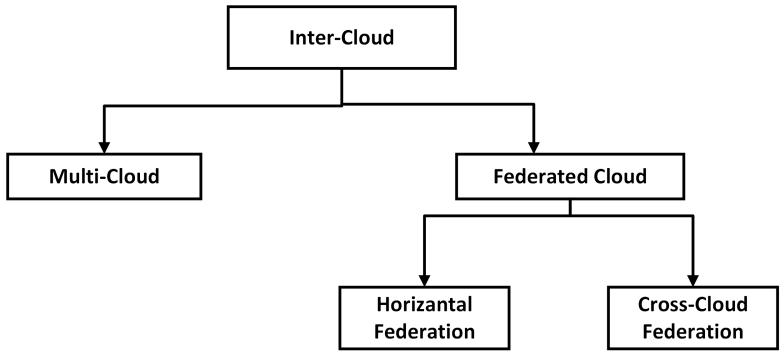

Figure 1: Multiple Cloud classification

Multiple Cloud Entities

- Cloud user/consumer(s)
- Cloud providers/ data center(s)
- Cloud-trusted entities
- Cloud auditor(s)
- Cloud carrier(s)

Multiple Cloud Settings

- Multi-cloud setting: individual user access a public cloud service provider.
- Multi-cloud setting: an enterprise with its own private cloud access a public cloud service provider.
- Cross cloud federation.
- Cloud federation.
  Figure 2 illustrates the different Multiple cloud settings and the entities.

Multiple Cloud Entities and Settings

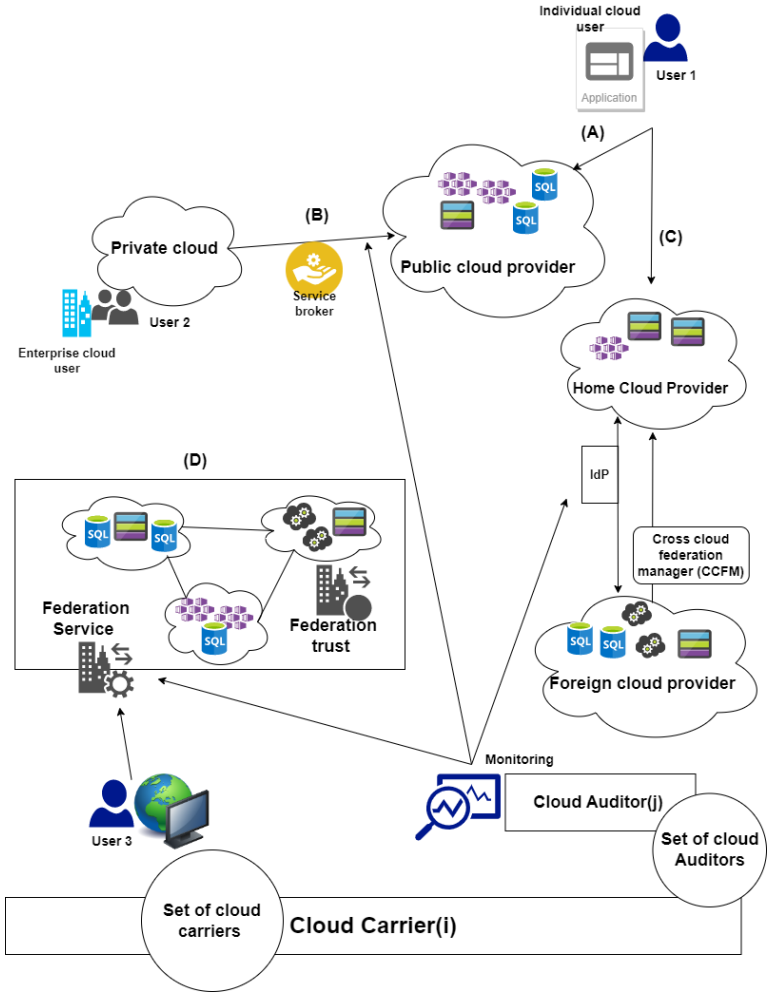

Figure 2: Multiple Cloud entities and deployment settings

Privacy concerns in multiple cloud types

Cloud type	Deployment model			Privacy concerns	Application
	Public	*Private*	*Hybrid*		
Multi-cloud			✓	• Identity privacy. • Location privacy. • Access pattern privacy. • Query privacy. • Data and access privacy.	• VANET. • Genomic domain.
Federated cloud			✓	• Risk of dynamic discovery. • Authentication privacy. • Access privacy.	Bio-informatic with SSO.
Horizontal federation	✓	✓	✓	• Trust between federation members: – No collude federated members. – longer chain of trust. • Identity privacy. • Risk of malicious service components. • Liability and legal issues. • Limited audibility.	Small organizations.
Cross-federated and inter-cloud			✓	• Identity privacy. • Attribute privacy. • Token access privacy. • Access and authorization privacy.	SSO (SAML 2.0, OIDC protocols)

Table 1: Privacy concerns in multiple cloud types

Conclusion

- Privacy is still of utmost importance in the digital world and has become vital for adopting different kinds of multiple clouds under a specific application domain.
- The success of multiple clouds adoption and a trustworthy environment is primarily driven by cloud security and preserving cloud users' privacy.
- The results of the present study provide classifications of multiple clouds types and outline the most common multiple clouds taxonomy.
- **Future work** should explore the potential of developing new techniques for privacy preservation in multiple clouds.

References I

[1] U. Ahmed, I. Raza, and S. A. Hussain, "Trust evaluation in cross-cloud federation: Survey and requirement analysis," *ACM Computing Surveys (CSUR)*, vol. 52, no. 1, pp. 1–37, 2019.

[2] B. Varghese, N. Wang, S. Barbhuiya, P. Kilpatrick, and D. S. Nikolopoulos, "Challenges and opportunities in edge computing," in *2016 IEEE international conference on smart cloud (SmartCloud)*. IEEE, 2016, pp. 20–26.

[3] D. Petcu, "Multi-cloud: expectations and current approaches," in *Proceedings of the 2013 international workshop on Multi-cloud applications and federated clouds*, 2013, pp. 1–6.

References II

[4] A. Celesti, F. Tusa, M. Villari, and A. Puliafito, "How to enhance cloud architectures to enable cross-federation," in *2010 IEEE 3rd international conference on cloud computing*. IEEE, 2010, pp. 337–345.

[5] D. C. Marinescu, *Cloud computing: theory and practice*. Morgan Kaufmann, 2022.

[6] N. Thillaiarasu and S. ChenthurPandian, "Enforcing security and privacy over multi-cloud framework using assessment techniques," in *2016 10th International Conference on Intelligent Systems and Control (ISCO)*. IEEE, 2016, pp. 1–5.

References III

[7] J. Hong, T. Dreibholz, J. A. Schenkel, and J. A. Hu, "An overview of multi-cloud computing," in *Web, Artificial Intelligence and Network Applications: Proceedings of the Workshops of the 33rd International Conference on Advanced Information Networking and Applications (WAINA-2019) 33*. Springer, 2019, pp. 1055–1068.

[8] M. A. Bouras, Q. Lu, F. Zhang, Y. Wan, T. Zhang, and H. Ning, "Distributed ledger technology for ehealth identity privacy: state of the art and future perspective," *Sensors*, vol. 20, no. 2, p. 483, 2020.

[9] J. Zhang, N. Xue, and X. Huang, "A secure system for pervasive social network-based healthcare," *Ieee Access*, vol. 4, pp. 9239–9250, 2016.

References IV

[10] B. Fabian, T. Ermakova, and P. Junghanns, "Collaborative and secure sharing of healthcare data in multi-clouds," *Information Systems*, vol. 48, pp. 132–150, 2015.

[11] M. R. Assis and L. F. Bittencourt, "A survey on cloud federation architectures: Identifying functional and non-functional properties," *Journal of Network and Computer Applications*, vol. 72, pp. 51–71, 2016.

[12] A. N. Toosi, R. N. Calheiros, and R. Buyya, "Interconnected cloud computing environments: Challenges, taxonomy, and survey," *ACM Computing Surveys (CSUR)*, vol. 47, no. 1, pp. 1–47, 2014.

Acknowledgments:

We acknowledge the support of the Natural Sciences and Engineering Research Council of Canada (NSERC [funding reference number 03181]).

Thanks!