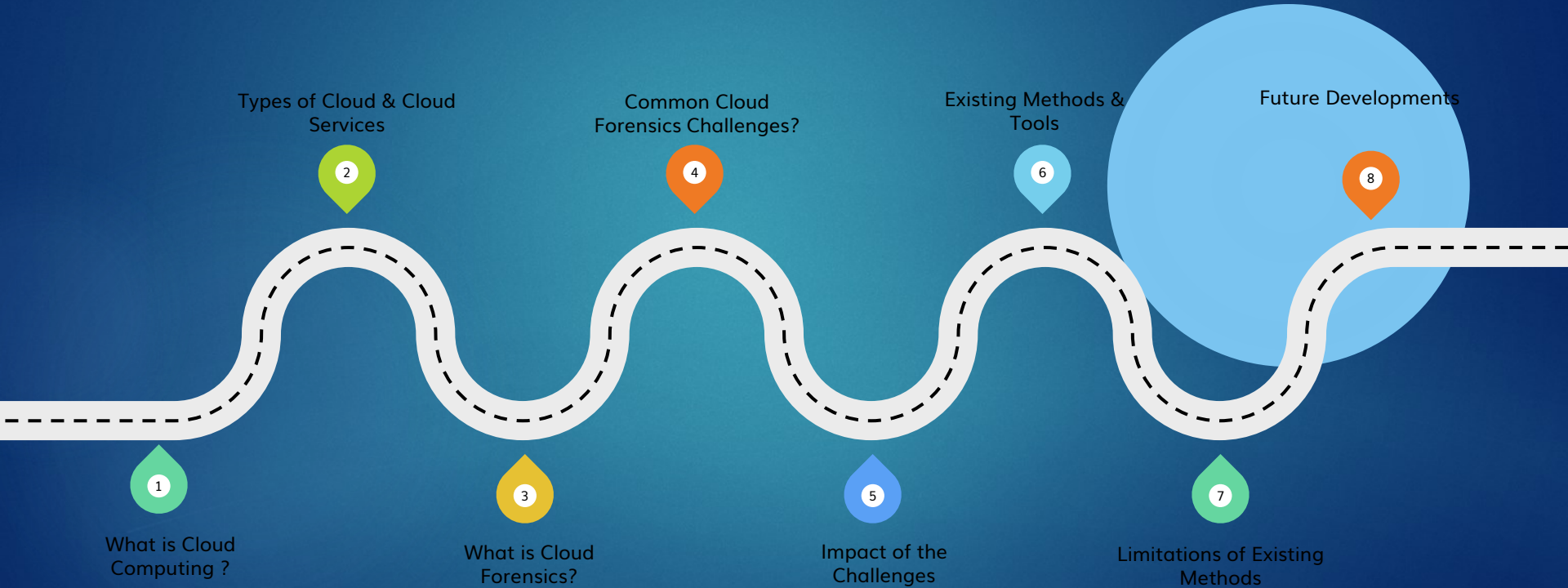


Cloud Forensics



Content

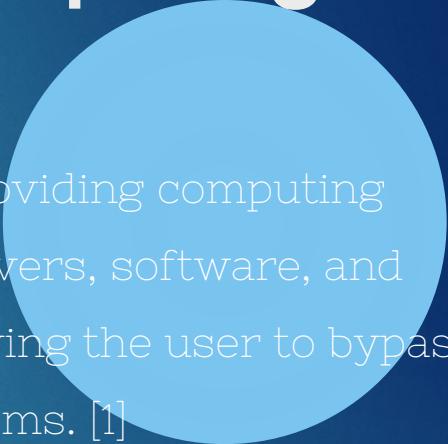




What is Cloud Computing ?

1

Cloud computing is a means of providing computing services (including databases, servers, software, and networking) via the internet, allowing the user to bypass direct management of those systems. [1]



2

Types of Cloud

Private Cloud

Public Cloud

Hybrid Cloud

Main Types of Cloud Services

IaaS – Microsoft Azure | Cisco Metacloud

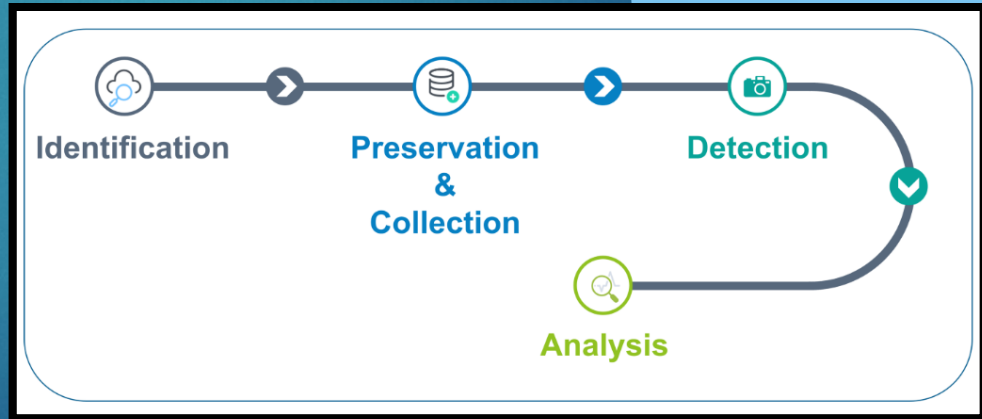
PaaS – OpenShift | AWS

SaaS – Cisco WebEx | GSuite

What is Cloud Forensics?

“Cloud forensics is the application of digital forensics in cloud computing as a subset of network forensics to gather and preserve evidence in a way that is suitable for presentation in a court of law.”[2]

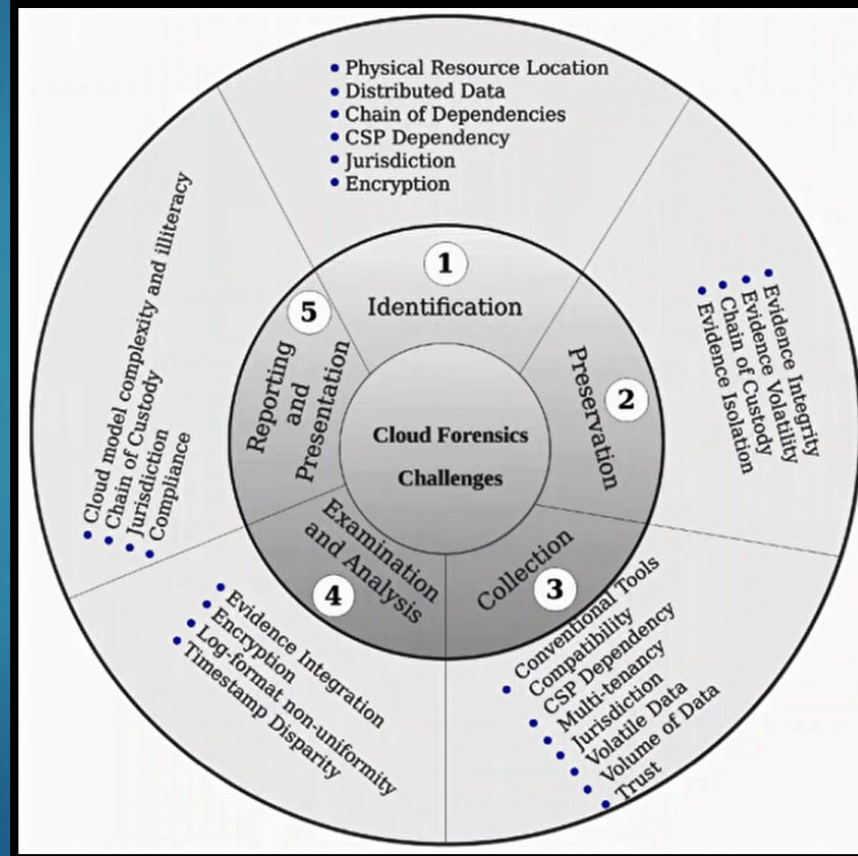
3



Cloud Forensics Steps

Common Cloud Forensics Challenges?[3]

4





Impact of the Challenges in Identification Stage

- ▶ Access to the Evidence in Logs
- ▶ Unknown or Not Accessible Physical Location



Impact of the Challenges in Collection & Preservation Stage

- ▶ Multi-tenancy & Resource Sharing
- ▶ Chain of Custody
- ▶ Dependence on CSP [4]

Impact of the Jurisdictional Challenges

Jurisdiction Challenges

Involvement of international & local law enforcement parties

Bulletproof hosting

Right to access data



Existing Methods for Mitigating the Challenges

5

- 1) Resource Tagging
- 2) Isolating cloud instance & Sandboxing
- 3) RSA Signature [5]
- 4) SLA specifying the specific forensic Services

Tools Using for Challenge Mitigation

6

1) UFED Cloud Analyzer

- Google My Activity and Facebook
- iCloud and Google backup
- Uber, Lyft
- DJI drones
- API logs
- Guest firewall logs
- Virtual disks

2) FROST

- API logs
- Guest firewall logs
- Virtual disks

Existing Methods

Limitations Related to Jurisdiction

7

1) International Communication and Cooperation

Limitation – Only effective for non urgent investigations

2) Foreign Jurisdiction Remote Examination

Limitation – Risk of damaging the target system

Future Developments

8

- 1) Method of Evidence Collection and Provenance Preservation for Cloud Using SDN and Blockchain Technology [6].
- 2) Permission Block Chain Based Data Logging and Integrity Management System for Cloud Forensics [7].

References

- [1] <https://www.talend.com/resources/what-is-cloud-computing/>
- [2] <https://kumarshivam-66534.medium.com/cloud-forensics-be18e14230de>
- [3] A Systematic Survey on Cloud Forensics Challenges, Solutions, and Future Directions | ACM Computing Surveys. (2022). ACM Computing Surveys (CSUR). Retrieved from <https://dl.acm.org/doi/fullHtml/10.1145/3361216>
- [4] Ruan, K., et al. Key Terms for Service Level Agreements to Support Cloud Forensics. in IFIP Int. Conf. Digital Forensics. 2012. Springer.
- [5] Lin, C.-H., C.Y. Lee, and T.-W. Wu, A cloud-aided RSA signature scheme for sealing and storing the digital evidences in computer forensics. International journal of security and its Applications, 2012. 6(2): p. 241-244.
- [6] M. Pourvahab and G. Ekbatanifard, "Digital Forensics Architecture for Evidence Collection and Provenance Preservation in IaaS Cloud Environment Using SDN and Blockchain Technology," in IEEE Access, vol. 7, pp. 153349-153364, 2019, doi: 10.1109/ACCESS.2019.2946978.
- [7] Park, Jun & Park, Jun & Huh, Eui. (2017). Block Chain Based Data Logging and Integrity Management System for Cloud Forensics. 149-159. 10.5121/csit.2017.71112.



Thank You!

Any questions?