

How to Cite:

Rathi, G., & Gaur, A. (2022). eDiscovery in the cloud-challenges and benefits. *International Journal of Health Sciences*, 6(S1), 11993–11997. <https://doi.org/10.53730/ijhs.v6nS1.8080>

eDiscovery in the cloud-challenges and benefits

Garima Rathi

Assistant Professor, Galgotias University, UP
Email: garimarathi@galgotiasuniversity.edu.in

Aditi Gaur

Assistant Professor, Galgotias University, UP
Email: aditigaur@galgotiasuniversity.edu.in

Abstract---Cloud computing is a rapidly emerging area of the today's technology industry. Moving towards cloud computing continues to gain importance and enable legal practitioners and law firms to expand their capabilities. The cloud provides the access to elastic computing that can fuel everything from traditional productivity applications like personnel management, presentation development and word processing, to sophisticated business application that includes content management, data mining and sales automations. Moving all or part of the firm's e-discovery functions to the cloud may lead to navigating complex issues to effect firm's security. This paper will focus on some of basics of eDiscovery, how cloud changes the way of its working. Here, we focus on the challenges of eDiscovery in the cloud.

Keywords---eDiscovery (Electronic Discovery), ESI (electronically stored information), IaaS (Infrastructure as a Service), PaaS (Platform as a Service), SaaS (Software as a Service).

Introduction

The business documentation now a days is electronically stored information (ESI). The discovery is the exchange of information between the parties in a legal case with the intent of using it as an evidence. Electronically storage information in eDiscovery can have many types of documents such as electronic mail, social media, electronic stored documents, messages, application data, and proprietary company database. The eDiscovery process is an IT centric process with large volume of structured and unstructured data or information that is to be analyzed, identified, collected and preserved in order to transfer it in a compliant manner to the other party to analyze, process and review. eDiscovery requires notable resources when advanced level of data review and analytics technologies are applied automatically to extract the legal insights from ESI corpus. A new business market has emerged that provides eDiscovery tools and platforms as

well as provides eDiscovery cloud services to the law firms and other stakeholder. The global eDiscovery market has valued around \$11 billion in year 2018 and is expected to grow around \$17 billion in coming five years. Even today the eDiscovery solution deployment model is on premise is migrating to cloud. In the next section of this paper we will focus upon the opportunities and challenges involved in adoption of cloud computing.

eDiscovery in the cloud

Cloud computing is a broad term that encompasses many different cloud provisioned service. The term is used to describe the data centers available to many users over the internet. eDiscovery poses many challenges for IT, law firms and organization that may govern its ESI to respect with eDiscovery law requirements. Some of these IT challenges includes:

The need for collecting, storing, and managing large quantities of diverse data, along with its metadata and history. Almost 50% of the enterprise data has been created and stored outside the enterprise. Because of that, such data may not be captured by legacy eDiscovery processes. The ESI corpus lies dormant for longer period but can be easily and quickly restored when needed. IT teams of law firms and of the organization required to maintain the ESI often they might not understand the special need of infrastructure and network eDiscovery.

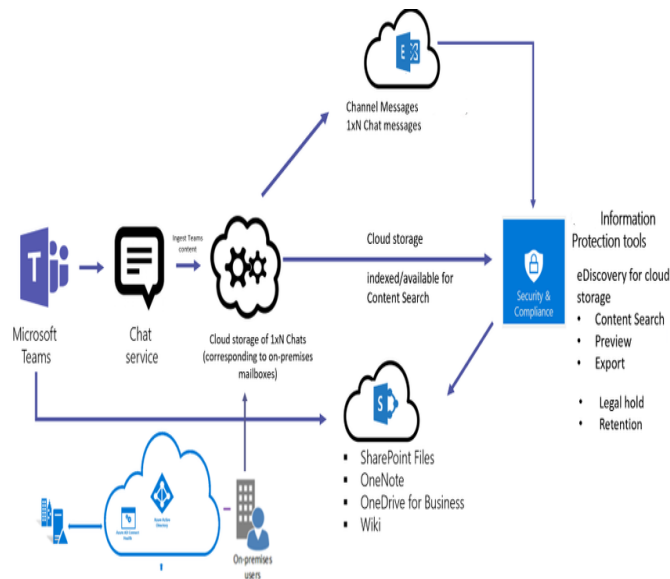


Fig. 1. Moving eDiscovery to Cloud

Cloud Service Models

IaaS (cloud Infrastructure as a Service)

IaaS is the flexible model of the cloud service models. It allows the organization to have complete and scalable control over the management. In the IaaS model, the provider of cloud hosts the infrastructure components that would be present in an on-site data center. The organization however maintains the control over

storage, operating system, and deployed applications [1].

PaaS (Platform as a Service)

This third-party vendor system can provide the organization a platform upon which an organization can develop and run the required applications. As vendor hosts the cloud infrastructure that supports the platform, PaaS eliminates the need to install in-house software or hardware. The organization would not even have to manage the underlying infrastructure of cloud, but also maintain control over the deployed applications, unlike with SaaS [2].

SaaS (Software as a Service)

This model helps an organization to access the cloud-based web application without the need of installing new infrastructure. The application runs on the vendor's cloud. The application is available for use with paid license subscription or freely available with the limited access. It does not need installation that eliminates the requirement to install, update or maintain the application on each computer system [3].

Data Protection and Security

This is not surprising to say that security can be perceived as the first barrier to cloud computing's adoption. As the breaches of online security is the main reason behind this barrier. The result one of the research study shows 78% of Business organizations recognize privacy and security of data as part of their responsibilities, 22% are aware of this part of their role [4]. One way to bridge this gap is to enforce a reliable and robust security program that ensures strict firewall, data encryption, intrusion detection, and access control [5].

Best ways to overcome this is to limit access permissions to inside and outside authorized personnel involved in the hosting, processing, production of data and review. This may lead to litigation support, eDiscovery specialists, paralegals or database administrators [6].

Storage and Privacy Issues

When the data resides, it can significantly affect eDiscovery and physical location of data storage is fundamental for evaluating cloud providers. Now this can be asked whether the cloud will involve shared pools of storage data that is public cloud that may be dispersed across different geographical locations throughout the world [6]. This approach means that the law firm's client data is distributed to various parts of the globe at the convenience of the data host providers to manage their internal capacity [7].

Factors to consider before switching

A. If a company is moving to cloud computing, then information storage and backup will be the important concern. It is important to know for how long the vendors of the cloud can keep the information and what are the required backup plans for the respective systems? However, these concerns cannot affect the importance of cloud computing. Some common application such as

- Facebook, Gmail, Microsoft Office, etc. are already providing the storage on cloud that can be formatted or accessed with the help of eDiscovery software systems [7].
- B. Accessing the electronically stored information (ESI) using cloud is not simple. Before, using cloud computing, practitioners should determine the appropriate cloud vendors such that whether they have tools to collect, find and lockdown the data. Cloud vendors should consider the discovery time limit and deadlines for vendor to download the huge amount of collected data in a meaningful format that can be useful for eDiscovery review [7].
 - C. Another factor that legal practitioner should analyze is the organizational resource persons for which the cloud computing can be required. Discoverable electronically storage information is expected to expand across legal personnel's, HR, IT's, and another department. The resource persons of these departments should not convey this information outside of their team and will probably have no information of what kind of report data they have accessed to [8].
 - D. When acknowledging the request of discovery, this will be necessary to find complete location of data where information could be preserved. The Boilerplate language can direct the custodian for producing the required documents that are under its custody, control and possession [9].
 - E. The plan of switching needs to provide not only the process of how to conduct eDiscovery on data stored in the cloud but also how to review the data alongside [10].

Conclusion

Here we can conclude that for setting successful eDiscovery policies for cloud computing is to know the cloud vendors that is what they will and will not do in that event of eDiscovery. According to one of the surveys, more than 70% of respondents do not know about their cloud vendor's policy. Despite of having various benefits of eDiscovery in the cloud computing, it does not come without its issues. Initially, the security of electronically storage information data in the cloud was considered as hurdle or barrier.

References

1. Mehdi Bahrami, Mukesh Singhal, A Light-Weight Permutation based Method for Data Privacy in Mobile Cloud Computing in 2015 3rd Int. Conf. 3rd IEEE International Conference on Mobile Cloud Computing Services and Engineering (IEEE Mobile Cloud 2015) San Francisco IEEE, 2015.
2. L. Zhou, V. Varadharajan, M. Hitchens, "Cryptographic role-based access control for secure cloud data storage systems", *IEEE Trans. Inf. Forensics Secur.*, vol. 10, no. 11, pp. 2381-2395, Nov. 2015.
3. H. Poor, *An Introduction to Signal Detection and Estimation*. New York: Springer-Verlag, 1985, ch. 4.
4. F. Chen, T. Xiang, Y. Yang, S. S. M. Chow, "Secure cloud storage meets with secure network coding", *Proc. IEEE Conf. Comput. Commun.*, pp. 673-681, 2014.
5. FA: Mohammed, R. A., Saifaddin, A. L., Mahmood, H. F., & Habibi, N. (2022). Seismic Performance of I-shaped Beam-column Joint with Cubical and

- Triangular Slit Dampers Based on Finite Element Analysis. *Journal of Studies in Science and Engineering*, 2(1), 17-31.
6. FA: Hersh F. Mahmood, Hooshang Dabbagh, Azad A. Mohammed, Comparative study on using chemical and natural admixtures (grape and mulberry extracts) for concrete, *Case Studies in Construction Materials*, Volume 15, 2021,
 7. Kumar, S. (2022). A quest for sustainium (sustainability Premium): review of sustainable bonds. *Academy of Accounting and Financial Studies Journal*, Vol. 26, no.2, pp. 1-18
 8. Allugunti, V.R. (2019). Diabetes Kaggle Dataset Adequacy Scrutiny using Factor Exploration and Correlation. *International Journal of Recent Technology and Engineering*, Volume-8, Issue-1S4, pp 1105-1110.
 9. J. Shen, S. Moh, I. Chung, "Identity-based key agreement protocol employing a symmetric balanced incomplete block design", *J. Commun. Netw.*, vol. 14, no. 6, pp. 682-691, 2012.
 10. D. Van, der Merwe, A. Roos, T. Pistorius, S. Eiselen, "Information and communications technology law", Durban: LexisNexis 2008, 2008.
 11. B.T. Ward, J.C. Sipior, J.P. Hopkins, C. Purwin, L. Volonino, "Electronic discovery: Rules for a digital age", *Boston University Journal of Science and Technology Law*, vol. 18, no. 150, 2012.
 12. J.M. Redgrave, *The Sedona Principles: Best Practices Recommendations and Principles for Addressing Electronic Document Production*, Silver Spring, ML:Pike & Fischer, 2007M. Young, *The Technical Writers Handbook*. Mill Valley, CA: University Science, 1989.
 13. M.H. Runyan, L. Powell, "Electronic discovery and records management", *Product Liability Advisory Council Spring Conference*, 2005.
 14. B.J. Rothstein, R.J. Hedges, E.C. Wiggins, F.J. Center, "Managing discovery of electronic information: A pocket guide for judges", *Federal Judicial Centre*, 2007
 15. A.O. Van Langham, "Navigating in the brave new world of e-Discovery: Ethics sanction and spoliation", *Quarterly Federation of Defense and Corporate Council*, vol. 54, no. 4, pp. 327, 2007