Record and Library Journal
https://e-journal.unair.ac.id/index.php/RLJ
Volume 4, No. 2, 2018
e-ISSN: 2442-5168

Security and Privacy of Cloud Storage as Personal Digital Archive Storage Media

Paper Type:
Literature Review

Dwininda Kusumawardhani and Deby Claudia Masyithah

Interdisciplinary Graduate Program - Gadjah Mada University

Submitted 05 June 2018
Accepted 08 April 2019
Online 30 September 2019

* Correspondence :
Dwininda Kusumawardhani

E-mail:
dwinindakw@gmail.com

Abstract

Background of the study: The increasing use of Internet technology has given rise to new challenges in the protection of privacy and personal data, especially with the increasing practice of collecting, using and distributing one's personal data. Lagging instruments and regulations is one of the triggers for the weak mechanism of protection against privacy and personal data, especially in the use of cloud storage technology.

Purpose: This article aims to find out the security of managing archive storage in a cloud.

Method: The method used in this paper is a literature review.

Findings: The result indicates that cloud storage has created new legal problems, namely how personal data from cloud storage users are protected from various kinds of disclosure and distribution by cloud storage service providers to third parties, while in Indonesia itself the ITE (Information and Electronic Transactions) Law has not clearly regulated security protection from private files stored in the cloud storage.

Conclusion: This is an obstacle to cloud storage to be able to continue to grow like the Internet which has become a prima donna in human life.

Keywords: *Cloud Storage, Archive Security and Privacy, Archive Storage Media*

To cite this document:
Kusumawardhani, D. & Masyithah, D. C. (2018). Security and Privacy of Cloud Storage as Personal Digital Archive Storage Media. *Record and Library Journal, 4*(2),167-173
Open access under Creative Commons Attribution-Non Commercial-Share A like 4.0 International Licence
(CC-BY-SA)

Introduction

At present, information and communication technology is developing very fast. Technology provides an important place to take part in human life by presenting a world without limits, space and time so that it can facilitate human activities in everyday life. In addition to facilitating human activities, the existence of technology is able to change patterns of interaction with others and conduct information seeking. Technology also contributes to changing cultural, economic and legal patterns in a country because nowadays it is no longer taboo for technology to be used by humans and it even becomes sort of a loyal friend in human life.

Reminiscing from the conditions before the presence of technology, humans stored data that were considered important in a file which were then put in a safe so that it could not be accessed by people who had no interest. But this method was slowly being replaced with the emergence of computers. Data that were initially stored in a safe were then processed and stored using a computer. The storage media can be in the form of a hard drive, a flashdisk, a floppy disk, or a CD / DVD, or stored in a local server (LAN). As time progresses, data storage requires a bigger capacity, while the available storage media do not have enough capacity to contain them.

Technology gave birth to the latest innovation that can be used by humans in carrying out storage, namely cloud computing or commonly called cloud storage. Along with the development of the needs of each individual, cloud storage began to be used for archiving personal documents. Each individual uploads personal documents such as photos and videos on a private cloud (Ghifari, Mustika, Rosidah, & Kirana, 2015). Moreover, the development of cloud storage now has changed with the emergence of the latest features that make it easier for someone to store personal files in the cloud storage (Ilham & Salleh, 2015). Cloud storage makes it easy for someone to store personal information and personal data held from previous storage media, because the storage capacity in cloud storage is greater (Birkner & Donk, 2018), so individuals do not need to think about storage space for digital archives of their own.

With this breakthrough, cloud storage answers the needs of technology users who emphasize speed, capacity, large storage and ease of access without being restricted to the same device. The presence of cloud storage raises the nature of ubiquity (present in all places), in which the purpose of this nature is that data or information stored can be accessed and be easily shared with anyone based on the consent of the owner of information by using computer devices that users have such as laptops, cellphones, and tablets (Sundoro, 2015). With this behavior, it will increase human mobility in using information technology. This means that it is directly proportional to human needs for data storage media that has a large capacity and affordable costs, poses easy access anywhere and anytime, and does not depend on the same device.

Many assume that cloud storage innovation is a solution to meet human needs in increasing human mobility in storing and disseminating information to anyone who is desired. Another advantage possessed by cloud storage as a storage medium is that it no longer requires physical storage, making it easier for users to access, process and share data that have been stored on the cloud. The data stored in the cloud are in the form of personal data, namely documents, photos, audio, and video. This is very useful when users are doing collaborative work with someone remotely so that they can always share documents, data, and files that have been done even though it is not done face to face, but the work continues to be done smoothly (Doni & Giansyah, 2015).

But with the convenience that it has when using cloud storage, there have been several cases of data contamination, the first case of which happened to Yahoo in 2016. Yahoo said that the data of 1 billion Yahoo users had been hacked by an irresponsible person, which caused the selling price of Yahoo to plunge dramatically, from the initial agreement of US $ 4.83 billion to become US $ 4.48 billion only (BBC News, 2016). This was a detrimental thing for Yahoo due to its poor user data security. Another case happened to a bank in the United States in 2017 when hackers managed to break into 143 million credit card customers' data. This broken customer data was the largest in history in the United States as reported by Ars Technica (2017). This data leak included the names of the credit card owners, their

To cite this document:
Kusumawardhani, D. & Masyithah, D. C. (2018). Security and Privacy of Cloud Storage as Personal Digital Archive Storage Media. *Record and Library Journal, 4*(2),167-173
Open access under Creative Commons Attribution-Non Commercial-Share A like 4.0 International Licence
(CC-BY-SA)

social security identity numbers, dates of birth, addresses and driver's license numbers. In the end the bank apologized because the bank's security system had been hacked. Therefore, the bank compensated by giving free protections of personal identity for one year. Usually this service is subject to fees starting at US $ 27.99 per month. Thus, cloud storage users still need to be vigilant when using cloud storage methods because there are still some problems that harm cloud storage users.

From some of the cases above, it can be said that it is very important to maintain the security of cloud storage as an archive storage media so that it is not easily hacked by irresponsible people. This article aims to find out the security of managing archive storage in a cloud.

Discussion

Personal digital archives

Personal digital archives are collections of digital information that are maintained by individuals for future use. The terms archiving, backup, and storage are used in the most general sense that refer to any activity for storing personal digital information (Sinn, Kim, & Syn, 2017). The individual's goal in conducting digital archiving is to document his or her personal life history (Kaye et al., 2006). He or she potentially archives various types of digital files such as text, images, spreadsheets, databases, pdf files, sound recordings, presentations, computer programs, e-mails, websites, blogs, video files, news articles and journals, and financial, legal, or medical documents (Copeland, 2009; John, Rowlands, Williams, & Dean, 2010).

Digital archive storage is currently getting cheaper for greater capacity. This situation has resulted in a storage space that is not being easily filled, so people rarely manage their digital files (Jones, 2007). Thus, someone often keeps the files redundant that they do not really need and use. This is a new problem in one's personal digital file storage. This phenomenon illustrates that every individual tends to save and transfer everything to the cloud storage they have. Even though a person has the desire to store and neatly arrange their digital archives so that they can easily be managed, this rarely happens. This causes important and useful digital archives to be mixed and stacked up with digital files that have not been used for quite a long time (Jones, 2007; Marshall, 2008; Marshall & Bly, 2005).

Cloud storage was originally meant for industry, but in line with what Hartig said (in Syaikhu, 2010), cloud storage has become a new model of computing that is widely being utilized not only in industry but also in society nowadays. The stark reason behind the popular application of cloud storage technology is because of the Internet-based service model that is used as a place to store personal records (data, information, and documents).

At present, humans have a need for a storage that has a very large capacity but no longer has a physical for. They only need enough space to hold all the files that can be archived, so cloud storage is growing from year to year. Cloud storage is a virtual storage medium that can streamline time and storage space much better, compared to other storage media such as flash drives or CDs. With the emergence of cloud storage, it will obviously change a person's behavior in storing, processing, and managing the information he or she has.

The characteristics of cloud storage according to NIST (Muhammad Ibrahim, 2013) are as follows: 1.) Resource pooling; cloud storage service providers provide services through resources (data, information, important documents) into one or various data center storage locations that consist of a number of servers with multi-tenant mechanisms. In general, cloud storage users have no control over the location provided by the service provider, 2.) Broad network access; cloud storage service providers have made it easy to access data or information that has been uploaded in cloud storage with various types of computer devices, 3.) Measured service; there are services to optimize and monitor services that are used automatically. It can be seen that the computing resources that are often used are bandwidth, storage, processing, and the number of active users. Cloud storage users are monitored, controlled, and reported as an effort to provide transparency for providers of cloud storage services (Syaikhu, 2010), 4.) Rapid elasticity; the capabilities of cloud storage services can be used by cloud users dynamically depending on the needs of its users, and 5.) Self service; cloud storage services can be configured

To cite this document:
Kusumawardhani, D. & Masyithah, D. C. (2018). Security and Privacy of Cloud Storage as Personal Digital Archive Storage Media. *Record and Library Journal, 4*(2),167-173
Open access under Creative Commons Attribution-Non Commercial-Share A like 4.0 International Licence
(CC-BY-SA)

independently by users through existing systems without the need to interact with cloud storage service providers.

According to NIST (National Institute of Standard and Technology) the characteristics of cloud infrastructure are divided into 4 (four) sections (in Purbo, 2011), namely 1.) Public cloud is a service model that has been provided by service providers and is intended for public or public services , 2.) Private cloud is where cloud storage services are used, managed and operated by a company for internal purposes in storing and processing stored data. 3.) Community cloud is cloud storage that is used to support shared interests such as missions, security requirements, policies, and policy considerations, and 4.) Hybrid cloud is a combination of one or more of the existing clouds which are still interrelated with common technology ownership standards in the use of data and application probabilities.

One of the most used cloud storages is Google Docs. Google Docs is one of Google's products that can process, store, create, and edit archives online. The benefits that can be felt when using the Google Docs is that it is easy to access archives that have been saved without having to use the same device. This reduces the risk of missing archives on storage devices (Budiyanto, 2012).

According to Thia (2008), the advantages of using cloud storage as an archive storage include: 1.) Minimizing storage device costs, 2.) Increasing productivity, and 3.) Integrating stored archives with all devices (Roana, 2013). Meanwhile, the disadvantages of using cloud storage as an archive storage medium according to Robbins (2009) include: 1.) Service level, which indicates that the possibility of less consistent service performance from the provider. This cloud provider's inconsistency includes data protection and data recovery; 2.) Privacy, which means there is a risk that user data will be accessed by others because hosting is done together; 3.) Compliance, which refers to the risk of a level compliance deviation from the provider to regulations that are applied to the user; 4.) Archive ownership, which refers to the risk of losing ownership of the archive when the archive is stored in the cloud; and 5.) Archive mobility, which refers to the possibility of sharing archives between cloud services and how to recover files if a user terminates cloud storage (Zackky, 2013).

Archive Security in Cloud Storage

Archive security is very important for users when storing and processing data in cloud storage. This is because there are personal files in the cloud storage that must be kept confidential. Cloud storage service providers as holders of important roles in protecting archives users have the obligation to maintain the security and confidentiality of archives in carrying out their services. Archival security refers to policy procedures, processes, and activities to protect information from various types of loss or stolen and leaked by irresponsible people. Security archives include various aspects such as Confidentiality, Integrity, Authentication, Availability, Access Control, and Non Repudiation.

Leakage of files that have been stored in cloud storage is something that is feared by cloud storage users. User data that have been uploaded to the cloud storage server can be lost in the cloud, and this can be caused by hacking. Users who fully entrust the storage, processing, and management of their data on a cloud storage will experience a quite detrimental impact, both materially and immaterially. With the occurrence of data leakage phenomena experienced by many individuals, archive security in cloud storage services is of particular concern to users and service providers. This is because both users and service providers become an important commodity for hackers to take advantage of.

The following are important factors in the security aspect that must be considered in operating cloud storage (Garfinkel, Spafford, & Schwartz, 2003), namely 1.) Confidentiality. This aspect is an attempt to secure information from irresponsible parties. In this case, it is related to the data of the customers of an Internet Service Provider (ISP) that must be maintained by a cloud storage service provider; 2.) Integrity. Information obtained cannot and should not be changed for any reason without the permission of the owner of the information. This is usually related to the alteration of email contents of cloud storage owners; 3.) Authentication. This aspect focuses on the authenticity of data/information, so that only the sole proprietor of the information who can access or share it, not someone else. Authentication is also the differentiator among users because it has unique data/information, since in

To cite this document:
Kusumawardhani, D. & Masyithah, D. C. (2018). Security and Privacy of Cloud Storage as Personal Digital Archive Storage Media. *Record and Library Journal, 4*(2),167-173
Open access under Creative Commons Attribution-Non Commercial-Share A like 4.0 International Licence
(CC-BY-SA)

this case it usually deals with the use of passwords; 4.) Availability. This aspect is an intermediary between the availability of information needed; 5.) Access control. This aspect regulates the rules in making changes to the data used by their users, so that not everyone can change user's information data. This is intended to avoid those who want to use other people's personal information; and 6.) Non repudiation. This aspect forces someone to acknowledge sending or receiving information via email. For example, when someone sends an email to confirm the order of an item belonging to him, he or she cannot deny that he or she did not send the email (Haryani, Nugroho, & Adhipta, 2014).

Cloud security is closely related to the project created by the National Security Agency (NSA) with the prism project title that is used to directly access the user's personal files from several cloud storage service providers. This causes user privacy to be disrupted because the prism project can directly access the user's personal files (Haryani et al., 2014). With this case, the security of cloud storage must always be considered, both by users and service providers, so that users are interested in migrating to cloud storage services as a media for storing, processing and managing their records.

The things that must be considered by users in conducting activities using cloud storage are as follows: 1.) Data protection. This is when the user has decided to use cloud storage as a storage medium, then what must be considered is how service providers provide protection so that the security of the data that users upload in the cloud is ensured, and where the data center is located because this will be related to data security regulation policies that vary in each country; 2.) Security Control, which means that after the user knows how the data is stored, the next step is to find out how the procedure for accessing data in the cloud is. This procedure also applies to cloud service providers in accessing user data; 3.) Compliance, which deals with knowing the standards set by cloud storage service providers, for example whether they have used ISO 27001 or, and as for cloud storage service providers they can use COBIT Cloud Security; 4.) Multi-tenancy, which deals with knowing how to minimize fraud committed by other users of our data because cloud storage essentially also acts as a sharing medium; and 5.) Security Governance, which deals more with police governance from service providers or from users.

The following is a table about the 2014 cloud readiness index from several countries in Asia and Australia.

Cloud Readiness Index 2014

	1. Privacy	2. International Connectivity	3. Data Sovereignty	4. Broadband Quality	5. Government Regulatory Environment and Usage	6. Power Grid and Green Policy	7. Intellectual Property Protection	8. Business Sophistication	9. Data Centre Risk	10. Freedom of Information	CRI2014 SCORE	RANK	CHANGE
JP Japan	9.5	5.5	8.0	9.1	5.0	7.1	8.1	8.2	6.6	9.7	76.8	1	-
NZ New Zealand	8.8	4.6	7.9	7.6	5.6	9.2	8.6	6.8	7.8	9.5	76.3	2	+4
AU Australia	8.8	4.4	7.6	8.0	5.3	7.8	7.6	6.7	9.4	9.6	75.1	3	+4
SG Singapore	6.0	8.2	7.8	8.8	6.1	5.9	8.7	7.3	7.4	8.6	74.8	4	-
HK Hong Kong	6.8	7.7	7.6	9.3	5.1	5.6	8.1	7.5	7.4	9.6	74.7	5	-2
KR South Korea	9.7	5.5	7.2	9.4	5.1	6.6	5.7	6.9	8.6	8.6	73.3	6	-4
TW Taiwan	4.6	6.3	6.8	8.5	5.0	6.7	7.4	7.4	6.9	8.6	68.2	7	-2
MY Malaysia	5.8	5.8	6.7	7.1	5.2	4.9	6.9	7.2	8.5	8.2	66.2	8	-
TH Thailand	4.0	5.0	6.2	8.0	3.7	6.3	4.4	6.3	7.6	7.8	59.3	9	+4
PH Philippines	5.8	5.4	5.9	4.1	3.7	5.5	5.1	6.1	5.5	9.0	56.1	10	+2
CN China	5.9	3.0	4.8	5.9	4.3	4.3	5.6	6.2	6.5	7.0	53.3	11	-1
ID Indonesia	4.4	2.9	6.2	3.1	3.9	5.7	5.6	6.3	6.4	7.9	52.4	12	-1
IN India	4.6	2.3	6.5	3.6	4.1	5.0	5.3	6.3	3.4	7.8	48.8	13	-4
VN Vietnam	3.6	3.2	5.6	4.2	3.8	4.7	4.1	5.3	6.4	7.0	47.8	14	-1

Source: Asia Cloud Computing Association 2014

Source: *Cloud Readiness Index* 2014.

To cite this document:
Kusumawardhani, D. & Masyithah, D. C. (2018). Security and Privacy of Cloud Storage as Personal Digital Archive Storage Media. *Record and Library Journal*, *4*(2),167-173
Open access under Creative Commons Attribution-Non Commercial-Share A like 4.0 International Licence
(CC-BY-SA)

Referring to the data in that 2014 Cloud Readiness Index, Indonesia is in the bottom three for data security in cloud storage, which shows that the country is still lacking in securing data on cloud storage. Regulations regarding the protection of data contained in cloud storage cannot be found comprehensively mentioned in any regulations in Indonesia. Only the ITE (Information and Electronic Transactions) Law that can be used as a basis in carrying out cloud storage service activities in Indonesia that regulates and facilitates the use and transaction of information using electronic media. Article 26 of ITE Law regulates the use of any information and data of a person through electronic media carried out without the consent of the owner of the data to be a violation. However, Article 26 only regulates the protection of personal data. The ITE Law has not clearly regulated how to protect electronic documents and data stored in a cloud storage.

Seeing this statement, service providers also need clear regulations on the sustainability of the cloud storage business. The government as the highest authority holder should be able to make a clear legal umbrella for service providers so that Indonesians who want to migrate to cloud storage do not have to worry about the security and protection of the data that they have.

Conclusion

Cloud storage is a technology that develops from cloud computing for the next generation that emphasizes speed, accuracy, and ease of access to information or commonly called as ubiquity. The biggest problems in cloud storage are the security and privacy of users who are not guaranteed. This is because in Indonesia itself the ITE (Information and Electronic Transactions) Law has not clearly regulated the security protection of personal files stored in a cloud storage. This is an obstacle to cloud storage to be able to continue to grow like the Internet which has become a prima donna in human life.

Acknowledgement

The authors would like to express their gratitude to Safirotu Khoir, SS., M.Sc., PhD as the authors' lecturer in providing her knowledge and guidance in writing this article, to Esti Putri Anugrah S.IIP., Who has helped in writing, and to friends of MIP UGM 2017 who have provided support in writing this article.

References

BBC News (2016, December 16). Satu milyar pengguna Yahoo jadi korban peretasan. *BBC News Indonesia*.

Budiyanto, A. (2012). Pengantar Cloud Computing. Cloud Indonesia, 1–10. Retrieved from http://www.cloudindonesia.or.id/apa-itu-public-cloud-private-cloud-dan-hybrid-cloud.html

Copeland, A. (2009). Writing information literacy assessment plans: A guide to best practice. *Communications in Information Literacy*, 3(2), 80–90. https://doi.org/10.1002/asi

Doni, & Giansyah, F. (2015). *Menggunakan private cloud computing berbasis*, 2–7.

Garfinkel, S., Spafford, G., & Schwartz, A. (2003). *Practical UNIX and internet security*. O'Reilly & Associate Inc. Sebastopol.

Ghifari, M., Mustika, V. E., Rosidah, H. K., & Kirana, A. (2015). Pemanfaatan media sosial oleh mahasiswa Universitas Muhammadiyah Surakarta. *In SEMNAS Penguatan Individu di Era Revolusi Informasi* (pp. 216–222).

Haryani, P., Nugroho, E., & Adhipta, D. (2014). Pengaruh dimensi trust, keamanan dan privasi. *In Seminar Nasional Teknologi Informasi dan Multimedia* (pp. 13–18).

Ilham, N. M. M., & Salleh, M. A. M. (2015). Isu privasi dan keselamatan dalam kalangan pengguna aplikasi media sosial. *Journal of Social Sciences*, *10*(2), 203–216. Retrieved from http://www.myjurnal.my/filebank/published_article/50874/15.pdf

John, J., Rowlands, I., Williams, P., & Dean, K. (2010). Digital lives: personal digital archives for the 21st century: an initial synthesis. *Digital Lives Research Paperaper*, *2*, 234. https://doi.org/http://www.paradigm.ac.uk/workbook/pdfs/index.html

To cite this document:
Kusumawardhani, D. & Masyithah, D. C. (2018). Security and Privacy of Cloud Storage as Personal Digital Archive Storage Media. *Record and Library Journal*, *4*(2),167-173
Open access under Creative Commons Attribution-Non Commercial-Share A like 4.0 International Licence
(CC-BY-SA)

Jones, W. (2007). Personal information management. *Annual Review of Information Science and Technology*, 41(1), 453–504.

Kaye, J. 'Jofish, Vertesi, J., Avery, S., Dafoe, A., David, S., Onaga, L., … Pinch, T. (2006). To have and to hold: exploring the personal archive. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* - CHI, 275–284. https://doi.org/10.1145/1124772.1124814

Marshall, C. C. (2008). *Rethinking personal digital archiving*. Retrieved from http://www.dlib.org/dlib/march08/marshall/03marshall-pt1.html

Marshall, C. C., & Bly, S. (2005). Saving and using encountered information: implications for electronic periodicals. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, 5*, 111–120.

Muhammad Ibrahim. (2013). Analisis dan implementasi Owncloud sebagai media penyimpanan pada Yayasan Salman Al-Farisi Yogyakarta. *Analisis Sistem Penyimpanan Data Menggunakan Sistem Cloud Computing Studi Kasus SMK N 2 Karanganyar*, *14*(04), 32.

Roana, S. (2013). Kelebihan dan kekurangan Cloud Computing. Retrieved January 1, 2017, from http://sraportofolio.blogspot.co.id/2013/03/kelebihan-dan-kekurangan-cloud-computing.html

Sinn, D., Kim, S., & Syn, S. Y. (2017). Personal digital archiving: influencing factors and challenges to practices. *Library Hi Tech*, 35(2), 222–239. https://doi.org/10.1108/LHT-09-2016-0103

Sundoro, D. (2015). Awareness penggunaan dan pemanfaatan public cloud storage di Indonesia. *Teknika*, *4*(1), 17–19.

Syaikhu, A. (2010). Komputasi awan (Cloud Computing) perpustakaan pertanian. *Jurnal Pustakawan Indonesia*, 10(1), 1–12.

Zackky, M. (2013). Pengertian, kelemahan, kelebihan cloud computing. Retrieved January 1, 2017, from http://creativersity.blogspot.co.id/2013/06/pengertian-kelebihan-dan-kelemahan.html

To cite this document:
Kusumawardhani, D. & Masyithah, D. C. (2018). Security and Privacy of Cloud Storage as Personal Digital Archive Storage Media. *Record and Library Journal*, *4*(2),167-173
Open access under Creative Commons Attribution-Non Commercial-Share A like 4.0 International Licence
(CC-BY-SA)