International Journal of Engineering & Technology, *7 (4.19) (2018) 134-138*

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Data Privacy and Confidentiality in Data Breach on Cloud Computing

Faisal Shahzad[1*], Roshidi Din[2], Osman Ghazali[3]

[1]Department of Computer Science & IT, The Islamia University of Bahawalpur, Punjab, Pakistan.
[2, 3]School of Computing, Universiti Utara Malaysia, UUM, Kedah, Malaysia
**Correspponding Author Email: [1]faisalsd@gmail.com*

Abstract

The preservation of data security in cloud environment has been identified as one of the key challenges in the field of cloud computing. The breach of data privacy and confidentiality has decreased the shift of enterprises to the cloud environment. However, there is currently no single definition of the concepts of data privacy and data confidentiality that could be generalized. Existing definitions of data privacy and confidentiality are complex, ambiguous and interchangeably used. This lack of clarity leads to confusion and potentially to ineffective and inefficient efforts to secure privacy and confidentiality of data from breach. The aim of this study is threefold. Firstly, this paper tends to explores the existing definitions of data privacy and data confidentiality in cloud computing. Secondly, it purports to examine the association of data breach with data privacy and confidentiality. Lastly,it proposes new operational definitions in order to differentiate between the concepts of data privacy and data confidentiality and data breach. The studies suggested that the concept of data privacy and data confidentiality in cloud computing is closely related and both are prone to breach within cloud security domain. Therefore, devising strategies and techniques to secure privacy and confidentiality of data can ultimately results in reduction of data breach.

Keywords: *Cloud computing, Data Breach,Data Privacy, Data Confidentiality*

1. Introduction

Recently, cloud computing has emerged as a computing paradigm that operates by evolving and distributing information throughout the system providing multiple benefits to the cloud providers and consumers. This rapid emergence of cloud computing and its benefits has raised some security aspects as well, that can inhibit the adoption of cloud computing by the consumers[1–3]. A property that can increase the adoption of cloud service is the preservation of privacy and confidentiality of the data. In simple words, the usage of cloud services is increased when the customers believe that privacy and confidentiality of their data is preserved by the service providers.

In past few years, privacy and confidentiality has principally been associated with attribute of data security and has emerged as an area of research in the field of cloud security. Preserving privacy and confidentiality in cloud has become an interesting topic for researchers because new approaches are becoming dependent on cloud security domain that operates in distributed cloud computing[4].It has been stated in previous researches that multi-tenancy and sharing of information are the ones that make data vulnerable to the breach of privacy and confidentiality[5].

There are certain conditions in which the information, obligations and rights of privacy and confidentiality may change in case the information is disclosed by the use to the provider[6]. Usually, multiple storage sites and disclosure of information controls the consequences of the protection of information and legal status stored or accessed through the internet. Adding to it, Mokbel et al.[7]stated that location of information determines the issues of privacy and confidentiality and the privacy obligations of the person handling the data. Subhashini et al. [8]also stated that the provider is responsible for the development and implementation of the strategies that ensures that the information of a customer is protected and not leaked to others with or without their knowledge [9].

Therefore, the issue of privacy arises when the user’s data is shared with others or it is accessed by the provider for unauthorized usage[10]. Whereas, issue of confidentiality arises when the loopholes for leakage of information are not addressed or when information is shared without user’s authorization[11]. Keeping this in view, it has been observed that there is no single standard definition of privacy and confidentiality. Though, there are number of researches that formalized a definition of these concepts, yet the concept of terms privacy and confidentiality remains vague and ambiguous within groups and organizations that hold completely opposite views.

In addition, voluminous work has mentioned that if the security aspects of data privacy and data confidentiality are not addressed efficiently, they may lead to the breach of data. Data breach is mentioned as a major security threat in the literature as well as in the reports of Cloud Security Alliance (CSA)[12–14]. It is an incident where information is extracted from a system without informing or authorization of the owner of the system. Mostly, organizations or large companies are the victims of data breaches and the stolen data is typically sensitive, private or confidential in nature.Thus, by protecting the data privacy and confidentiality, the breach of the data can be prevented. The relation among data privacy, confidentiality and breach would be explored in accordance with the previous researches.

Hence, the narrative of this paper provides a thorough understanding of the concept of terms data privacy, data confidentiality and data breach. While there is no single intervention at its source, there is a confusion and deviation of what data privacy, confidentiality and breach means and how these are associated as well as how the domain researchers can be educated regarding the development of efficient strategies for preserving and securing transmission of data.

Therefore, this paper is divided into different sections in order to fulfill the purpose of this paper. Section 2 will explore the existing definitions of data privacy and data confidentiality that have emerged from the field of cloud security aspects to address the question ofdifference between data privacy and confidentiality. Section 3will discusses the association of data privacy and confidentiality with data breach andSection 4 will present the proposed definitions followed by the discussion, conclusion and future recommendations in the proceeding sections.

2. Existing Concept of “Data Privacy” and “Data Confidentiality” in Cloud

Previously, it has been believed that the terms "Privacy" and “Confidentiality" are interchangeable, ignoring the important differences between them. From the research standpoint, these two terms privacy and confidentiality are similar although they both have significant roles in their application to data and data security aspects. In[15], the researchers have clearly defined both terms separately. According to them “privacy is the ability to protect information related to the user’s personal sphere” whereas “confidentiality is the ability to limit access and disclosure of information to only authorized users”. These definitions clearly states that privacy is a state of protecting information and rights to keep thing yourself while confidentiality is limiting the information access and avoiding it to get exposed to unauthorized individual. In addition, following are the various definitions of data privacy and data confidentiality that can further clear the concept of these two terms.

2.1 Data Privacy

Privacy is a broad concept varying among countries and jurisdictions.Some of the existing definitions of privacy that are presented worldwide are as follows:

- According to Oxford Dictionary, privacy is a state of being free from attention of others[16].
- Privacy is defined as a status on which a person and organization is agreed regarding the furnishing and receiving of data considering the degree of protection with which it is provided (OECD) [17].
- The privacy, according to Generally Accepted Privacy Principles (GAPP) is the right and obligation of a person and organizations with respect to the usage, retention and disclosure of personal data [17], [18].

These definitions of privacy provides a notion that it is a basic human right to be free and left alone. From commercial point of view, privacy is the protection of personal information of users and using it according to the expectations of the users. For organization, law, policies and standards should be involved through which personal information of users is managed[19]. Some differences can be noted in the definitions. While OECD defines privacy as a direct link between an individual and its related data, GAPP, Oxford Dictionary and [19]go one step further, including to the definition the right management of that information. Considering the concerns regarding privacy, a clear definition is essential that can accurately define privacy.

2.2 Data Confidentiality

Confidentiality**,** in literature, appears to be a blurry term that does not seem to be understandable by the researchers as the main differences between privacy and confidentiality are not yet clear. Mostly, privacy is globally used by researchers whilst, they could use confidentiality as well according to the definition stated below. In literature, three papers make a definition over the term confidentiality:[20–22]. Other definitions found are mentioned as follows:

- “It is the property that information is not disclosed to any unauthorized person or entity”[20].
- “Keeping users’ data secret in the Cloud systems”[21].
- It implies that data is kept confidential from both the cloud consumers and providers[22].

These definitions of confidentiality are in contrast with the definitions of privacy stated above. For example, in[16]X. Ma defined privacy as a state of being free from others. Mostly obligations are related to collection, retention and disclosure of data. As it can be noted, confidentiality is illustrated more specifically related to the domain of “keeping data secret and unavailable” whilst privacy is a more global concept, which entangles rights, obligations and management over this data. In addition, the capability of securing information relating to the personal capacity of users [11]is termed as privacy whereas, data confidentiality means that data on cloud is protected from an unintended or unauthorized access. Confidential data is considered as sensitive data, that means to limit the access of data only to authorize person and protect the data from accidental or purposeful unauthorized access on cloud environment.

Zissis and Lekkas[23]states that “privacy is a wish of a person to control the disclosure of personal data” whereas “confidentiality is the access of information to only authorized parties and systems”. These definitions explain that privacy is the right of an individual to protect the personal information. It is state where there is no public interference while confidentiality refers to situation in which one’s important information is not disclosed until the person himself allows to disclose it to others.Adding to it, Subashini and Kavitha[8]while illustrating the issues regarding privacy and confidentiality of data in cloud domain mentions that “privacy is of personal information while confidentiality is of business and governmental information”. This shows that privacy is a consumer’s right to protect his information from disclosure to others. In [24]considering the privacy risk in cloud, privacy has been explained as “the capability of securing personalized information regarding location, preferences and social networks” whereas “confidentiality is the treatment of information in a way that it could not be disclosed to any authorized individual”. These definitions show that privacy is secured only if the service providers handlethe private information. While, confidentiality refers to treatment of information that is disclosed by an individual.

Moreover, the definition of privacy by[18]states that “privacy is a right of a person or an organization during the collection, usage and disclosure of personal data”. Whereas confidentiality in[25]is defined as “the property that information is not disclosed to unauthorized entities”. Hence, it is apprehended that privacy is rooted in common law while confidentiality is an ethical duty.Summarizing the above mentioned definitions, it is stated that confidentiality is actually a characteristic of privacy that focus on the protection of information from leakage by devising preventive measures of disclosure of data. In fact, in their review paper about security in Cloud Computing, Xiao et al.[22]explain that confidentiality is an attribute of privacy and regards privacy-preservability as the core attribute of privacy. Therefore, it is believed that preserving privacy is the strict form of preserving confidentiality because both prevent data from leakage. If confidentiality in cloud is breached than privacy is also violated. This could be the reason that literature use term confidentiality very sparsely, as most solutions dealing with data safety can assure confidentiality and preserve privacy.

Thus, it can be concluded from the above statements that if the service provider or the owner fails to secure the privacy and confidentiality of data while outsourcing, multi-tenancy or controlling massive data, “breach of data” occurs. This “breach of data” appears as a main security threat as reported by the CSA reports of year 2010 to 2016[12–14]. The data breach is defined as the release of information to an unauthorized environment that results due to the failure in secure outsourcing of data. This definition is covering the concept of both privacy and confidentiality which means that failure in preventing privacy and confidentiality of data can lead to the breach of data. Source of privacy and confidentiality breach could be internal or external and the intent of confidentiality might be accidental or purposeful [18].

This accidental release of information to the unauthorized individuals increases the complications in data privacy and data confidentiality mostly enhancing the criticality of user [18].Therefore, privacy and confidentiality both depends on security measures on cloud. Major concern of security is to help prevent accidental or purposeful breaches from occurring which ensures that if breaches occur, they are detected and addressed quickly. This association of breach with privacy and confidentiality of data is stated in the proceeding section.

3. Relationship of Data Privacy and Data Confidentiality with Data Breach

Data breach as a security threat is the release of secure information in an untrusted environment intentionally or unintentionally. It may also be taken as unintended disclosure of information, data spill and leak [25], [26].In other words, such damage created by breach is often presented as the loss of company’s reputation with the customers because of “betrayal of trust”. This damage may include damages to financial records as they could be the part of stolen information.Moreover, data breach is explained by Subashini el al. as an incident involving illegal or unauthorized viewing or access of data by another individual or service[8]. It is a breach of security which is intended to steal or publish data to an illegal or unsecure location. Adding more to the knowledge of data breach, Chandramohan[27]narrates that data breach occurs when a secure repository or database is accessed by a hacker or unauthorized attacker. Data breach is mostly geared towards digital or logical data and is conducted over network connection. The consequences of data breach is the loss of personal data such as financial, personal or health information.

In short, data breach is the term that implies to the theft of data which is a malicious action performed by unauthorized parties. Breach occurs only when the data is viewed, if it is copied and transmitted then the consequences are more threatening. This loss of privacy and confidentiality of the data is the nefarious step in online crimes. The term of data breach also describes the accidental release of private and confidential data to an “untrusted environment” due to the fault of authorized party. Thus, lack of strong authentication leads to unauthorized access to cloud resulting in breach of privacy and confidentiality[28].

Conclusively, keeping in view the security aspects as well as breach as a major security threat in cloud computing, the present study considered the privacy and confidentiality as two main security aspects associated with the breach of data. It is due to the fact that privacy and confidentiality are found to be the major security concerns in the cloud environment and that the breach issues are raised while processing and outsourcing of data. Therefore, considering to preserve the privacy and confidentiality of data in cloud environment is essential to prevent data breach. Following section explains the relationship of data breach, data privacy and data confidentiality as well as propose the definitions of these terms.

4. Proposed Definitions

As mentioned earlier, privacy and confidentiality are the security aspects of the cloud computing whereas failure in preserving these two leads to the breach of information to the unauthorized access which is the major security threat. Additionally, with the growth of personal, enterprise or government data, the services are moved to the cloud for storage and processing. Here the chances of data breach of privacy and confidentiality increases as cloud services are used by end clients or organizations that want to get subscribed to a service offered by a cloud provider. While storage and outsourcing of data, there are some requirements of security such as protection of data from exposure, control to access and communication protection, privacy in multitenant environment, availability of service and security of software[22], [27], [29].

Furthermore, Kolevski and Michael[30]also states that failure in preserving privacy and confidentiality as a result of accidental or illegal destruction, alteration and disclosure of personal information leads to the data breach. Privacy and confidentiality breach is directly propositional to the cloud technologies as the breach of privacy and confidentiality is increasing with the increase in technology. Therefore, preserving privacy and confidentiality holds more importance as compared to other security aspects. This presents a notion that when the privacy and confidentiality of the data in the cloud environment is preserved, it eventually prevent the data from breach and also protect data from an unauthorized access. Considering the above mentioned definitions of data privacy, data confidentiality and data breach, Figure 1.presents proposed definitions of these concepts which is the main contribution of this paper.

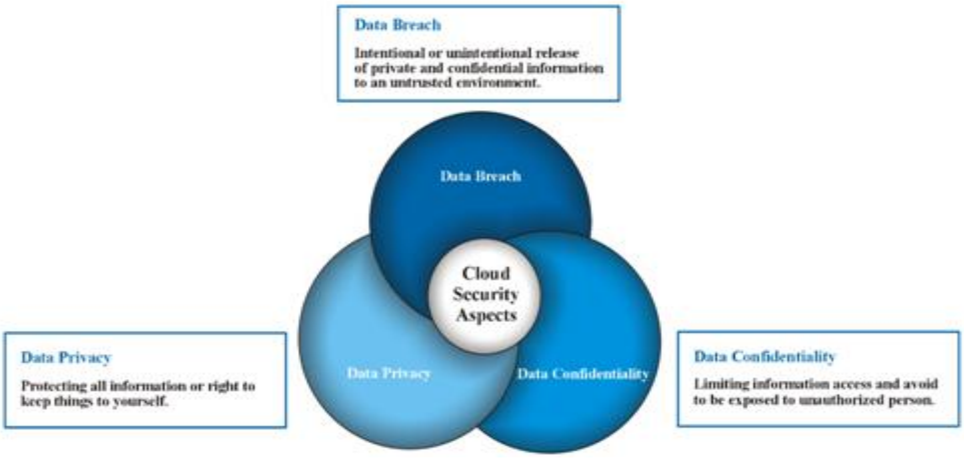
Data Breach
Intentional or unintentional release of private and confidential information to an untrusted environment.
Data Breach
Cloud Security Aspects
Data Privacy
Data Confidentiality
Data Privacy
Protecting all information or right to keep things to yourself.
Data Confidentiality
Limiting information access and avoid to be exposed to unauthorized person.

Fig. 1: Proposed definition of data breach, data confidentiality and data privacy

Figure 1.illustrates the definitions of the data breach, data privacy and data confidentiality that are proposed keeping in view their significance in cloud computing. Figure shows that the relationship between breach of data privacy and data confidentiality is necessarily complicated. In this context, data privacy is the capability to protect all information of individual, data confidentiality is limiting information access and avoiding it to be exposed, and breach is an access of the private and confidential information to an untrusted environment. Thus, an access of the private and confidential data by the unauthorized user leads to the breach of the data in the cloud environment[28].

Therefore, it would not be wrong to say that preserving privacy and confidentiality of data is important as there breaches is one of the most important concerns in today's emerging IT world. A great amount of work has been done by the researchers regarding the issues of breach, privacy and confidentiality of data as these are the leading concerns of security threats to cloud computing.

5. Conclusion

The objective of this paper was to review the existing definitions of data privacy and data confidentiality and their relation to the data breach in order to add to the ongoing discussion of the relation of data breach with data privacy and confidentiality. While cloud computing is taking over the IT world, the rise in research output would suggest that this is an area of growing interest. The review suggested that data privacy and confidentiality aremultidimensional concepts that are viewed from multiple perspectives and includes different factors. Despite several definitions of privacy and confidentiality, mostly are vague and closely related. Such definitions prove to be insufficient because they rely on abstract constructs providing limited guidance in developing security measures. As a result, these terms data privacy and data confidentiality are frequently used interchangeably embodying contradictory ideas. These closely related concepts and shared definitions can lead to incompatible practices.

Moreover, the importance of having a unique definition for both privacy and confidentiality cannot be underestimated. Without clear definition of data privacy and confidentiality, contributions will continue to remain isolated and insular which will lead to ineffective efforts of addressing these concepts. Moreover, the relation of privacy and confidentiality with breach of data leads to the conclusion that focusing on preserving privacy and confidentiality of personal information can ultimately result in the prevention of data breach.

Conclusively, consensus in field of cloud computing has yet to be achieved. A tailored definition is required that can remove ambiguity and complexity of the existing definitions. It should clearly indicate as to whether privacy or confidentiality of data is to be addressed and provides holistic view of cloud environment in which breach of privacy and confidentiality occurs. Importantly, any definition of breach of data privacy and confidentiality must be comprehensible not only by domain scientists but to the layperson also.

6. Future Work

To avoid future inconsistencies, it is essential to propose and implement guidelines that can characterize and classify the existing definitions of privacy and confidentiality as well as their perspective and relevance to the cloud computing. Prospective studies should develop a framework that tends to disambiguate the termsprivacy and confidentiality of data.Moreover, an effective strategies should be developed and implemented to secure data privacy and confidentiality from breaches. It would not only affect cloud providers, in fact, end-users would also be benefitted by this because they have relied on online services and have their credentials compromised. Moreover, data should be specified to the particular entities who are authorized to have access as it ensures that information is disclosed to the right entities.

Acknowledgement

This research is fully supported by University Research Grant from Sultan Idris Education University under the grant number of 2018-0134-109-01.

References

[1] M. Armbrust et al., "A view of cloud computing," Commun. ACM, vol. 53, no. 4, p. 50, Apr. 2010.

[2] D. Gaurav Pal, R. Krishna, P. Srivastava, S. Kumar, M. Bag, and V. Singh, "A Novel Open Security Framework for Cloud Computing," Int. J. Cloud Comput. Serv. Sci., vol. 1, no. 2, pp. 42–52, 2012.

[3] A. Kumar, "World of Cloud Computing and Security," Int. J. Cloud Comput. Serv. Sci., vol. 1, no. 2, pp. 53–58, 2012.

[4] A. Sarwar and M. N. Khan, "A Review of Trust Aspects in Cloud Computing Security," Int. J. Cloud Comput. Serv. Sci., vol. 2, no. 2, pp. 116–122, 2013.

[5] M. Theoharidou, N. Papanikolaou, S. Pearson, and D. Gritzalis, "Privacy Risk, Security, Accountability in the Cloud," in 2013 IEEE 5th International Conference on Cloud Computing Technology and Science, 2013, pp. 177–184.

[6] D. Svantesson and R. Clarke, "Privacy and consumer risks in cloud computing," Comput. Law Secur. Rev., vol. 26, no. 4, pp. 391–397, Jul. 2010.

[7] M. F. Mokbel, C.-Y. Chow, and W. G. Aref, "The New Casper: A Privacy-Aware Location-Based Database Server," in 2007 IEEE 23rd International Conference on Data Engineering, 2007, pp. 1499–1500.

[8] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," J. Netw. Comput. Appl., vol. 34, no. 1, pp. 1–11, Jan. 2011.

[9] R. Cheng, Y. Zhang, E. Bertino, and S. Prabhakar, "Preserving User Location Privacy in Mobile Data Management Infrastructures," Springer, Berlin, Heidelberg, 2006, pp. 393–412.

[10] F. Rocha, S. Abreu, and M. Correia, "The Final Frontier: Confidentiality and Privacy in the Cloud," Computer (Long. Beach. Calif)., vol. 44, no. 9, pp. 44–50, Sep. 2011.

[11] R. Gellman, "Privacy in the clouds: risks to privacy and confidentiality from cloud computing," Proc. World Priv. forum, pp. 1–26, 2009.

[12] Cloud Security Alliance, "Top Threats to Cloud Computing V1.0," Cloud Security Alliance., 2010. [Online]. Available: http://www.cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf.

[13] Cloud Security Alliance, "The Notorious Nine. Cloud Computing Top Threats in 2013," Security, 2013. [Online]. Available: http://www.cloudsecurityalliance.org/topthreats.%5Cnhttp://www.cloudsecurityalliance.org.

[14] Cloud Security Alliance, "The Treacherous 12 Cloud Computing Top Threats in 2016," Security, no. February, pp. 1–34, 2016.

[15] C. A. Ardagna, R. Asal, E. Damiani, and Q. H. Vu, "From Security to Assurance in the Cloud," ACM Comput. Surv., vol. 48, no. 1, pp. 1–50, Jul. 2015.

[16] X. Ma, "Security Concerns in Cloud Computing," in 2012 Fourth International Conference on Computational and Information Sciences, 2012, pp. 1069–1072.

[17] T. Mather, S. Kumaraswamy, and S. Latif, Cloud security and privacy: An Enterprise Perspective on Risks and Compliance. O'Reilly, 2009.

[18] D. Chen and H. Zhao, "Data Security and Privacy Protection Issues in Cloud Computing," in 2012 International Conference on Computer Science and Electronics Engineering, 2012, pp. 647–651.

[19] S. Pearson and A. Charlesworth, "Accountability as a Way Forward for Privacy Protection in the Cloud," Springer, Berlin, Heidelberg, 2009, pp. 131–144.

[20] Y. Chou, O. Levina, and J. Oetting, "Enforcing confidentiality in a SaaS cloud environment," in 2011 19thTelecommunications Forum (TELFOR) Proceedings of Papers, 2011, pp. 90–93.

[21] M. Zhou, R. Zhang, W. Xie, W. Qian, and A. Zhou, "Security and Privacy in Cloud Computing: A Survey," in 2010 Sixth International Conference on Semantics, Knowledge and Grids, 2010, pp. 105–112.

[22] Z. Xiao and Y. Xiao, "Security and Privacy in Cloud Computing," IEEE Commun. Surv. Tutorials, vol. 15, no. 2, pp. 843–859, 2013.

[23] D. Zissis and D. Lekkas, "Addressing cloud computing security issues," Futur. Gener. Comput. Syst., vol. 28, no. 3, pp. 583–592, Mar. 2012.

[24] S. Pearson and A. Benameur, "Privacy, Security and Trust Issues Arising from Cloud Computing," in 2010 IEEE Second International Conference on Cloud Computing Technology and Science, 2010, pp. 693–702.

[25] S. Pearson and G. Yee, Privacy and Security for Cloud Computing. London: Springer London, 2013.

[26] V. Shandilya and S. Shiva, "Security in the cloud based systems: Structure and breaches," in 8th International Conference for Internet Technology and Secured Transactions (ICITST-2013), 2013, pp. 542–547.

[27] D. Chandramohan, T. Vengattaraman, D. Rajaguru, R. Baskaran, and P. Dhavachelvan, "A novel framework to prevent privacy breach in cloud data storage area service," in 2013 International Conference on Green High Performance Computing (ICGHPC), 2013, pp. 1–4.

[28] M. Jouini and L. B. A. Rabai, "Surveying and Analyzing Security Problems in Cloud Computing Environments," in 2014 Tenth International Conference on Computational Intelligence and Security, 2014, pp. 689–693.

[29] D. A. B. Fernandes, L. F. B. Soares, J. V. Gomes, M. M. Freire, and P. R. M. Inácio, "Security issues in cloud environments: a survey," Int. J. Inf. Secur., vol. 13, no. 2, pp. 113–170, Apr. 2014.

[30] D. Kolevski and K. Michael, "Cloud computing data breaches a socio-technical review of literature," in 2015 International Conference on Green Computing and Internet of Things (ICGCIoT), 2015, pp. 1486–1495.