Singaporean Journal of Scientific Research

An International Journal (AMIJ)
Singaporean Journal of Scientific Research(SJSR)
Vol.12.No.1 2020 Pp. 1-6
available at:www.sjsronline.com
ISSN: 1205-2421
Paper Received :30-11-2019
Paper Accepted:25-02-2020
Paper Reviewed by: 1. Dr. P. Surya Prakash 2. Basu Reddy
Editor : Dr. R. Velayutha Pandey

Importance of Ethics in Cloud Security

Dr. Pallavi Malhotra
Charles Sturt University

Abstract

This Paper examines the importance of ethics in cloud computing. In the modern society, cloud computing is offering individuals and businesses an unlimited space for storing and processing data or information. Most of the data and information stored in the cloud by various users such as banks, doctors, architects, engineers, lawyers, consulting firms and financial institutions among others require a high level of confidentiality and safeguard. Cloud computing offers centralized storage and processing of data, and this has immensely contributed to the growth of businesses and improved sharing of information over the internet. However, the accessibility and management of data and servers by a third party raise concerns regarding the privacy of clients' information and the possible manipulations of the data by third parties. This document suggests the approaches various stakeholders should take to address various ethical issues involving cloud-computing services. Ethical education and training is key to all stakeholders involved in the handling of data and information stored or being processed in the cloud.

1. Introduction

Information technology is changing rapidly to match the ever-increasing needs of organizations, businesses, governments, and individuals. Individuals, businesses and other organizations require online software to process, synchronize, share, store, and organize data and information to satisfy their needs with as much efficiency and flexibility as possible. The increasing user expectations have led to the growth of cloud computing whereby the computing resources such as software, storage space, maintenance routines and CPU power offered online by the providers who maintain massive data centres for processing and storing files(Chang et al., 2017). As cloud-computing services continue to gain popularity, it raises ethical issues regarding the use and handling of data and information of the clients and users. This document examines the nature of cloud computing services, various ethical issues involved in cloud computing and measures various stakeholders are using or should use to address various ethical issues.

Cloud Computing Technology

Cloud computing involves delivery of computing services such as storage, networking, databases, analytics, software and services over the internet. Cloud providers or third party companies offer the cloud computing services, which are responsible for managing clients' data servers (Chang et al., 2017). Cloud computing technology offers users' enormous benefits of low cost, flexibility and ubiquitous access to data and information using various internets enabled devices and efficient management of IT software by qualified personnel. It offerslow capital expenditure for hardware and software installation, low cost of establishing and running online data centers such as the cost of hiring IT expert, setting up of servers, establishing IT infrastructures, and cost of electricity for powering and cooling the servers (Winkler, 2011; Loske,2015). The cloud computing services are available on-demand hence the services are faster and efficient Also, the cloud computing services are readily accessible to the users everywhere (ubiquitous) regardless of the geographical location or devices used to access the internet (Management Association, Information Resources, 2017).Furthermore, cloud computing has no compatibility issues compatibility which makes it very common among various users.

Ethical Issues in Cloud Computing

Despite several benefits of cloud computing the accessibility and control of clients data and servers by third parties raise various ethical issues regarding the security and confidentiality of clients data and informationstored and exchanged over the internet (Reynolds, 2017).Third parties have access to clients information which they may use for self-gain or to the detriment of the client. For instance, third parties can access clients' emails. The third parties can manipulate or reproduce clients' sensitive data without client's consent, which may have severe legal repercussions to the clients for the breach of customer privacy (Management Association, Information Resources, 2013). Besides, there are concerns about what happens to the client's data and information upon the termination of the contract between cloud service providers and clients. The users of cloud computing services should be aware of the existing policies, and regulations to promote security and confidentiality of the data and client's servers.

Who are the important people involved?

Cloud computing involves many parties. First, there are cloud-computing providers who own and operate datacenters, servers, and hard disks used for storing and processing of data. The hosting companies include Microsoft, Rackspace, Google and Amazon (Dove et al., 2015).The cloud computing service providers are responsible for providing particular online services. Examples include Salesforce, Google Docs, ZoHo Recruit, Dropbox, etc.

Government is a stakeholder in cloud computing technology because it is involved in setting regulations to promote the security of cloud computing services (Black, 2012). In addition, the government can act as a clouder or provider of cloud computing services. The government policies and practices influence the security and privacy of data and servers stored or processed in the cloud.

Individuals and businesses are using the cloud to store and process data and servers. Individuals and businesses are important stakeholders in cloud computing because they store organizations and client's data in the cloud by other individuals or businesses (Management Association, Information Resources, 2013). They collect personal information from their clients and personal data which they store and process in the cloud. They should handle clients' data responsibly and confidentially.

Major Issues

The majorissue involving cloud computing services is that of clients are entrusting of confidential data and information to a third party. The third parties have established security policies and regulations regarding how they handle clients' data and servers under their control (Ghaznavi-Zadeh, 2015). The clients should review the third party policies and terms of service to determine the extent in which third parties can manipulate the data and information and get the assurance of responsibility in case of breach of security policies by the third party (Samani, Reavis & Honan, 2014). Another concern about cloud computing services involves the possibility of failure of programs operated in the cloud which may undermine the client's access to the data and their inability to resolve the issue (Bruin & Floridi, 2017). Various stakeholders should understand how the cloud computing technology works and ensure adequate policies and regulations regarding the use and management of data and information stored and processed in the cloud.

Opinions

Cloud computing technology offers individuals and organizations great opportunity to improve the efficiency of operations, improved productivity, and business growth cost-effectively and conveniently (Black, 2012). As individuals and businesses focus on enhancing their performance, efficiency, and growth, cloud computing security will become more crucial for individuals and organizations to achieve their goals. The advancing technology increases threats as cybercriminals strive to outsmart individuals and businesses offering Internet-based services (Chang et al., 2017). The main challenges facing information technology involves the people handling the extensive information and data stored and processed in the cloud and other technology-based platforms. Therefore, businesses and organizations should educate and train their employee's matters of ethics to support confidentiality and security of data and information. The ethical education and training should focus on changing people's behavior in the way they handle confidential data and information belonging to their clients (Endicott-Popovsky, 2014). It should also influence the accessibility of data and information by the clients and enable clients to make the required amendments and corrections whenever needed.

Why is this Important

Ethics in cloud computing is very controversial and interesting subject because of the impact it has on individuals, businesses and other stakeholders. The demand for cloud computing services continues to increase as well as efficiency and flexibility, while the cost has decreased significantly (Maurice, Mohamed & Marwan, 2016). Although there are many advantages of using cloud security, there are many issues that need to be addressed to promote confidentiality and security of client's data and servers controlled by third parties (Mather et al., 2009). There are showing that cloud computing is riskier than other Internet-based technologies, but all the same,thereis a need for all stakeholders to take necessary measures to protect client's data and information against manipulations or unauthorized use by third parties.

How has the problem developed?

Most internet users depend on cloud computing services for storage or processing of data and information. Since the1990s the use of the internet has contributed to access to information and business growth (Ghaznavi-Zadeh, 2015). However, there has also growing demand for the internet by individuals and businesses. The development of cloud computing in the recent years has contributed to increased flexibility and accessibility of data and information over the internet. The transfer of data and servers to the control by a third party increased privacy issues and concerns about the ease of accessibility.

In the recent past, there have been issues of cyber-attacks of data and servers targeting large companies. Besides, there has been increasing cases of prosecutions of cybercriminals. In July 2010, the US Army soldier named Bradley Manning was apprehended in connection with the illegal transfer of classified data from national defence information to his personal computer and then WikiLeaks (Dove et al., 2015). The information was sensitive involving the 250,000 U.S. diplomatic cables. In addition, in 2011a computer programmer named Goldman Sachs was sentenced to over eight years in prison for stealing property source code that was used to detect even minute inconsistencies in stock prices. Various stakeholders involved in cloud computing should be aware of how the technology works and act appropriately to protect data and servers involved in the cloud computing (Endicott-Popovsky, 2014). The increasing cases of attacks on data and information stored or shared over the internet have raised ethical issues about the privacy of clients' data, what measure users are taking to enhance the security of data and ensure the data is accessible to the users whenever required.

Individuals and businesses have the responsibility for protecting client's information and data and should apply specific practices that ensure such data and information is secure (Mather Kumaraswamy& Latif, 2009). Businesses and individuals involved in handling client's information should be aware of the practices and technologies utilized to ensure security and privacy of client's property and information (Bruin & Floridi, 2017). The approaches and practices for providing client's data and the information is secure include data encryption, server security, password security, and client security.

Conclusion

Cloud computing technology is crucial in the modern world because it supports ubiquitous access of data and files over the internet using any internet enabled devices. Also, it savescost and enhances performance and efficiency of operations. Furthermore, cloud computing offers a more secure and secure means of computing, unlike the traditional computer-and-server-based technology. However, there are various ethical issues involving cloud computing technology which includes access and control of clients data by a third party as well and the inability of cloud computing users to access and resolve issues whenever they occur. There is a need for all the people involved in cloud computing to observe ethical standards to avoid compromising the security of data and servers stored and processed in the cloud.The providers and users of cloud computing services should establish necessary procedures to promote the security and confidentiality of the cloud computing services.

References

[1] Black, N.(2012). The ethics of cloud computing for lawyers; American bar association,*GPSolo e-reportVol. 2(2).*Available at;https://www.americanbar.org/groups/gpsolo/publications/gpsolo_ereport/2012/september_2012/ethics_cloud_computing_lawyers.html

[2] Bruin,B. &Floridi, L. (2017). *The Ethics of Cloud Computing: Sci Eng Ethics*, 23(1): 21–39. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC523607/

[3] Chang, V., Ramachandran, M., Walters, R.J. & Wills, G. (2017). *Enterprise Security: Second International Workshop, ES 2015, Vancouver, BC, Canada, November 30 – December 3, 2015, Revised Selected Papers*. Switzerland: Springer.

[4] Dobrick, F.M., Fischer, J. & Hagen, L.M. (2017). *Research Ethics in the Digital Age: Ethics for the Social Sciences and Humanities in Times of Mediatization and Digitization***.**USA:Springer.

[5] Dove,E.S., Joly,Y., Tassé, A. & Knoppers, B.M (2015).Genomic cloud computing: legal and ethical points to consider;*Eur J Hum Genet, Vol.*23(10): 1271–1278.Available at; https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4592072/

[6] Endicott-Popovsky, B. (Ed) (2014). *ICCSM2014-Proceedings of the International Conference on Cloud Security Management ICCSM-2014:* ICCSM2014. UK: Academic Conferences Limited.

[7] Ghaznavi-Zadeh,R. (2015). *Enterprise Security Architecture: A guide to Infosec management*. USA: Primedia E-launch LLC.

[8] Loske,A. (2015). *IT Security Risk Management in the Context of Cloud Computing: Towards an Understanding of the Key Role of Providers' IT Security Risk Perceptions*. UK: Springer.

[9] Management Association, Information Resources (Ed) (2017). *Mobile Commerce: Concepts, Methodologies, Tools, and Applications: Concepts, Methodologies, Tools, and Applications*. USA: IGI Global.

[10] Management Association, Information Resources, (2013). *IT Policy and Ethics: Concepts, Methodologies, Tools, and Applications: Concepts, Methodologies, Tools, and Applications*. USA: IGI Global.

[11] Mather, T., Kumaraswamy, S. & Latif, S. (2009). *Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance*."O'Reilly Media, Inc."

[12] Maurice, D., Mohamed, E. & Marwan, O. (2016). *Security Solutions for Hyperconnectivity and the Internet of Things*. USA: IGI Global.

[13] Reynolds, G. (2017). Ethics and information technology, 6th Ed. USA: Cengage Learning.

[14] Samani, R., Reavis,J. & Honan, B. (2014). *CSA Guide to Cloud Computing: Implementing Cloud Privacy and Security*.USA: Elsevier Science.

[15] Winkler, V. (2011). *Securing the Cloud: Cloud Computer Security Techniques and Tactics*. USA: Elsevier.