Importance of Ethics in Cloud Security

Author- Dr. Pallavi Malhotra,
Research Scholar- Chetanpal Singh

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 the key to all stakeholders involved in the handling of data and information stored or being processed in the cloud.

Index Terms- IT Ethics, Cloud Computing, Cloud Privacy and Security

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 centers 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 internet enabled devices and efficient management of IT software by qualified personnel. It offers low 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.
Cloud security is defined as an approach of protecting valuable data, which is stored online, from any sort of theft, deletion, and leakage to external parties. The various aspects of cloud security fundamentally embrace ‘management’, ‘technology’, and ‘operation.’ In this context, the ‘management’ facet of cloud security covers service integration, administration of cloud safety, updated security policy, strategy of cloud security, and security roles along with responsibilities. Apart from these, the ‘management’ factor also constitutes information technology, in addition to procurement safety requirements, guidelines of cloud security, governance, and continuous assessment. In contrast, the ‘technology’ dimension of cloud security also considers network protection, access control, audits of cloud security, system safeguard, identification, and protection of physical security. Furthermore, the other areas that are covered by the ‘technology’ aspect include authentication, identity as well as key management, backup, recovery along with archive, and protection of core infrastructure. Finally, the ‘operation’ characteristic duly considers ecological protection, personal safety, awareness & training, information integrity, and incident management. Moreover, it covers maintenance, configuration management, system integrity, media protection, and contingency planning (Mitchell & Alcock, 2011).

The importance of cloud computing technology can be better comprehended from certain specific core principles. These principles represent that sharing of data is better to form, expand, and preserve effective communication with the involved parties. Under cloud computing technology, obligations are placed towards sharing valuable data and greater access to the computers is facilitated wherever possible. These identified principles are closely associated with the work ethics of cloud computing security, which eliminates the errors being witnessed while storing and transferring data from one specific place to another (Chance, 2005).

Ethical Issues in Cloud Computing

The significance of ethics in cyber or cloud computing security exists in various developments, which are linked with cloud computing along with information and communications technology (ICT). One of these developments can be identified as the transfer of control, especially from the technology-based users to the third parties who are entitled with the responsibility of servicing the cloud due to offshoring and outsourcing ICT-based functionality to the cloud. Another significant development is data storage in numerous physical locations across several servers throughout the globe. These are possibly owned as well as administered by many distinct business corporations. The interconnection of various services throughout the cloud is the other major development, wherein there lays the need to maintain ethics in cyber security. There are many factors, which are responsible for laying the foundation to determine and preserve ethics in cyber or cloud computing security. These factors typically encompass ‘control’, ‘problem of many hands’, ‘self-determination’, ‘accountability’, ‘ownership’, ‘function creep’, and ‘privacy.’ Furthermore, the other aspects comprise ‘monopoly & lock-in’, ‘cultural imperialism, dealing with diversity’, and ‘privacy across (cultural) borders’ (Timmermans et al., 2010.).

The chief characteristics of cloud computing security are identified as successful exploitation of internet technologies and delivery of cost-effective services to the users. The internet technologies, which are used
under cloud computing security, are deemed as elastic as well as scalable in nature. This eventually
triggers the need to perform certain ethical practices. In this context, these ethical practices may
encourage promoting resource or storage virtualization, measuring elasticity along with scalability and
preserving anonymity as well as accessibility. In addition, the other ethical practices, which can be
included, are determining the competence of resource sharing, fostering usage optimizing, ensuring
speedy information sharing and, delivery as well as control. Based on these identified facets of cloud
computing security, the importance of ethics exists in data off-shoring, wherein valuable data is
accumulated and stored for using it in the future. It is in this context that the concerns of security and
responsibility of the users emerge, which needs to be addressed for generating viable or favorable results.
Therefore, the ethics of ownership and function creep should be highly considered during data off-shoring
under cloud computing security. This would significantly help in maintaining privacy by strengthening the
authentication procedure and ensuring optimum utilization of effective technological resources. Issues of
redundant reliance over the cloud security providers have been apparent and do not promise application,
data, and service portability as per the expectation level. Under this circumstance, standardized data
formats or service interfaces might play a critical function for resolving these issues by a certain level,
which leads towards increased privacy and accountability (Timmermans et al., 2010).

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
information stored 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.

The risks including data corruption, unavailability or outing, unauthorized access, and infrastructure
failure are apparent in cloud computing. In this context, the importance of ethics lies in controlling
outsourcing as well as off-shoring tasks associated with ICT that pass from various technology users to the
third-party service providers. At certain times, cloud computing implements a service oriented architecture
(SOA), wherein all ICT functionalities are aggregated into bigger applications. This may result in creating
difficulty to determine who is liable for accessing the functions and the applications in case if any
undesirable event takes place. In cloud security, the significance of ethics raises the question on
information self-determination. This signifies the right or the capability of the people for exerting personal
control over the collection, execution, and the disclosure of valuable data by others. Information self-
determination is challenged in this present day context, as the organizations and their respective members
share unlimited data to fulfill their own as well as customers’ interests. It must be mentioned that personal
data, which is stored in cloud, are required to manage properly in order to maintain both accountability
and privacy. Thus, in this context, the ethical practices of determining what is being recorded and
identifying for whom the records or the data are made accessible, should be performed and maintained
(Timmermans et al., 2010).
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 cloud user 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 major issue 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, there is a need for all stakeholders to take necessary measures to protect client’s data and information against manipulations or unauthorized use by third parties.

The significance of ethics in cloud security can be better comprehended from two vital factors. This includes ICT governance and precautionary principle. In general, ICT covers several governance arrangements, which comprises professional procedures, technical standardizations, international law, legal provisions, and informal agreements. Correspondingly, governance represents the “manner in which something is governed or regulated; method of management system of regulations” (Timmermans et al., 2010.; p. 6). In relation to the factor concerning ICT governance, the vitality of ethics in cloud security lies in determining the incorporation of moral values into technological advancement and usage. Under ICT governance and cloud security, maintenance of ethics relies on the technology type along with its usage in distinct governance arrangements. With regard to the aspect of precautionary principle, the importance of ethics in cloud security can be determined for preventing harm from any sort of unknown threat without affecting innovation, collaboration, and communication. It is believed that several effects and unwanted results in cloud security are not properly identified due to deficiency in monitoring process. Thus, performing ethical practices of ICT governance and precautionary principle can help in identifying these effects as well as unnecessary consequences, which results in enhanced cloud security functions (Timmermans et al., 2010).

How has the problem developed?

Most internet users depend on cloud computing services for storage or processing of data and information. Since the 1990s 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 defense 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 saves cost 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

Understanding of
the Key Role of Providers’ IT Security Risk Perceptions. UK:


