Computer Engineering and Intelligent Systems
ISSN 2222-1719 (Paper) ISSN 2222-2863 (Online) DOI: 10.7176/CEIS
Vol.10, No.4, 2019
www.iiste.org

Concepts of Cloud Computing and Protection of Data in Cloud Computing

Elifenesh Yitagesu Desta
Lecturer,Department of Computer Science, College of Computing, Madda Walabu University, POBox 247, Bale Robe, Ethiopia

Abstract
The internet has changed the world in a strong way.it has traveled from the concept of parallel computing to distributed computing to grid computing and recently to cloud computing. Cloud computing is a recent trend in Information Technology that moves computing and data away from desktop and portable personal computers into large data center. The main advantage of cloud computing is the user cannot pay for infrastructure, its installation, required man power to handle such infrastructure and maintenance. Cloud computing technology is collecting success stories of savings, ease of use, ease of access and increased flexibility in controlling how resources are used at any given time to deliver computing capability. Cloud providers who can demonstrate that they protect personal information may be more truthful and therefore more attractive to potential Cloud users. The cloud service can be implemented in three different service models, such as Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), and Infrastructure-as-a-Service (IaaS). Data security and privacy protection issues are relevant to both hardware and software in the cloud architecture. This study is to review the concepts of cloud computing and different security techniques and protecting data in the cloud.
Keywords: Cloud computing, Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), Infrastructure-as-a-Service (IaaS).
DOI: 10.7176/CEIS/10-4-01
Publication date:May 31st 2019

Introduction

"Cloud computing" refers to Internet-based computing that allows organizations to access a pool or network of computing resources that are owned and maintained by a third party via the Internet. (Reeta Sony A.L, Prof Sri Krishan Deva Rao, Bhukya Devi Prasad, 2013). The main goal of cloud computing is to make a better use of distributed resources, combine them to achieve higher throughput and be able to solve large scale computation problems. Cloud computing deals with virtualization, scalability, interoperability, quality of service and the delivery models of the cloud, namely private, public and hybrid. (Yashpalsinh Jadeja, Kirit Modi, 2012). As more companies, individuals and even governments place their data in the cloud, both customers and providers of cloud computing services must become acutely aware of the burgeoning laws and regulations restricting the collection, storage, disclosure and movement of certain categories of information. Cloud Computing has been very often portrayed and perceived as a new technology but it is also widely accepted as evolution of technologies such as client server architecture, World Wide Web, and networking. Some even call it mainframe 2.0. In 1960s mainframes were used for computing and transaction processing with users accessing the computing resources through 'dumb terminals'. 1980s saw the advent of protocols for networking and client server architecture. "The ability to connect users to computing and data resources via standardized networks emerged as a key enabler of cloud computing" (The Defense Science Board). The World Wide Web and the Internet followed in the 1990s along with enablers such as web browsers. The decade also saw the emergence of application service providers, offering software packaged as service over the internet. Refer Figure 1 for graphic on evolution of computing. (Trivedi, 2013)

DOI: 10.7176/CEIS

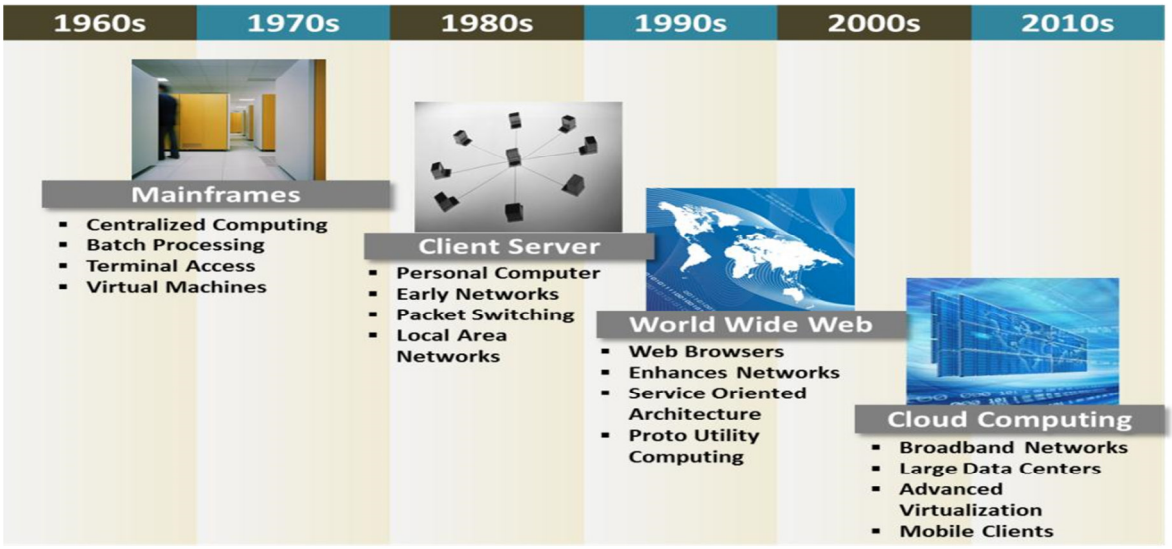

Figure 1: Evolution of Cloud Computing. (Trivedi, 2013)

The term "cloud" originates from the world of telecommunications when providers began using virtual private network (VPN) services for data communications (John Harauz,Lorti M. Kaufman, Bruce Potter, 2009). Cloud computing deals with computation, software, data access and storage services that may not require end-user knowledge of the physical location and the configuration of the system that is delivering the services. Cloud computing is a recent trend in IT that moves computing and data away from desktop and portable PCs into large data centers (Marios D. Dikaiakos, George Pallis, Dimitrios Katsaros, Pankaj Mehra, Athena Vakali, 2009). The definition of cloud computing provided by National Institute of Standards and Technology (NIST) says that: "Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. (National Institute of Standards and Technology) With the large scale proliferation of the internet around the world, applications can now be delivered as services over the internet.

In the cloud computing environment, consumers of cloud services do not need anything and they can get access to their data and finish their computing tasks just through the Internet connectivity. During the access to the data and computing, the clients do not even know where the data are stored and which machines execute the computing tasks (Yunchuan Sun, Junsheng Zhang, Yongping Xiong, Guangyn Zhu, 2014).

Cloud computing system can be dividing into two sections: the front end and the back end. They both are connected with each other through a network, usually the internet. Front end is what the client (user) sees whereas the back end is the cloud of the system. Front end has the client's computer and the application required to access the cloud and the back end has the cloud computing services like various computers, servers and data storage.

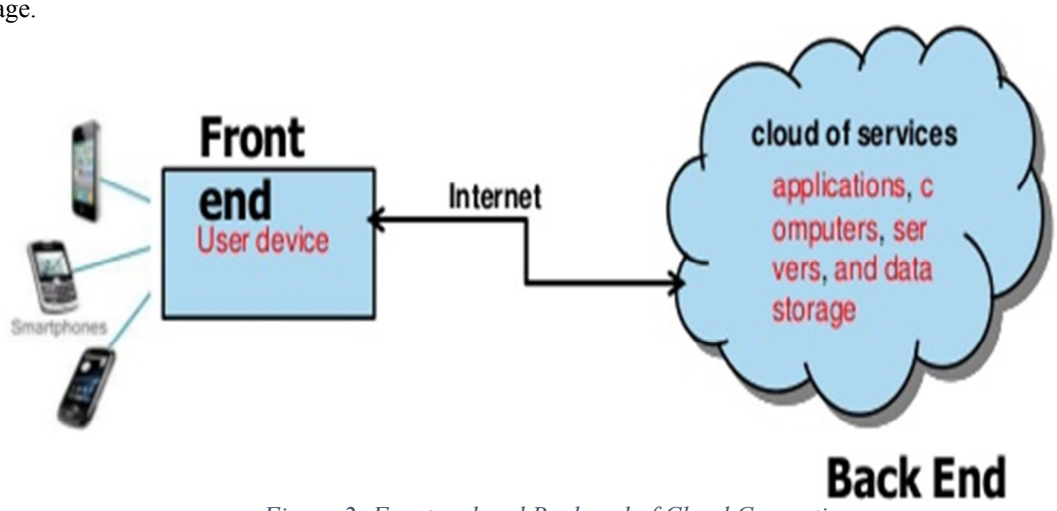

Figure 2: Front end and Back end of Cloud Computing

Monitoring of traffic, administering the system and client demands are administered by a central server. It follows certain rules i.e. protocols and uses a special software called the middleware. Middleware allows

networked computers to communicate with each other (Yashpalsinh Jadeja, Kirit Modi, 2012). The cloud computing model is comprised of a front end and a back end.

The paper is arranged as follows: Section 2 define the environment of cloud computing, cloud providers section 3 define the protection of personal information and in the last section conclude the paper with the summary of cloud computing with the protection of personal data.

Cloud Provider

The central player amongst all in the cloud ecosystem is called cloud provider who provides cloud services. e.g., are Amazon, Microsoft, IBM or Google. This entity provides and operates computing infrastructure both hardware and software to deliver the cloud services to users through the Internet. The role played by the cloud provider will be different depending upon the type of cloud services such as SaaS, PaaS or IaaS (Cloud Computing Architecture).

1. ***Software-as-a-Service (SaaS)***. The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a web browser, or program interface. The consumer does not manage or control the underlying cloud infrastructure, including network, servers, operating systems, storage, or even individual application capabilities (Denys, 2012). In SaaS the role played by the cloud provider is to take complete ownership of application and infrastructure and make it available to the end-user. In this case the cloud provider would install, maintain and upgrade applications and will ensure uptime, response time and security aspects of the application software. In this case the cloud user has practically no administrative control on the management of application (Cloud Computing Architecture).
2. ***Platform-as-a-Service (PaaS)***. The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created, or acquired applications, created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure (including network, servers, operating systems, or storage), but has control over the deployed applications and possibly configuration settings for the application-hosting environment (Denys, 2012). In PaaS, the cloud provider limits its responsibility to look after the infrastructure platform. In addition it creates and enables an environment in such a way that the cloud user can develop and deploy its application. The cloud provider creates integrated development environments (IDEs), software development kits (SDKs), and deployment and management tools. While the end-user manages the application parameters and controls the balance responsibility of underlying infrastructure such as OS, storage, network etc. are managed by the cloud provider (Cloud Computing Architecture).
3. ***Infrastructure-as-a-Service (IaaS)***. The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources, where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications which may have limited control of select networking components (e.g., host firewalls) (Denys, 2012). In the most basic of cloud services i.e., IaaS the cloud provider just manages the hardware, host OS, storage and network and hosting infrastructure. The only services run by the service provider are a set of services such as virtual machines and virtual network interfaces. The rest of the overlaying layers are run, managed and controlled by the cloud user. The IaaS user has far greater control on software, application and also the OS. The cloud provider's responsibility includes deployment, combination, management, security, and privacy of the cloud services (Cloud Computing Architecture).

DOI: 10.7176/CEIS

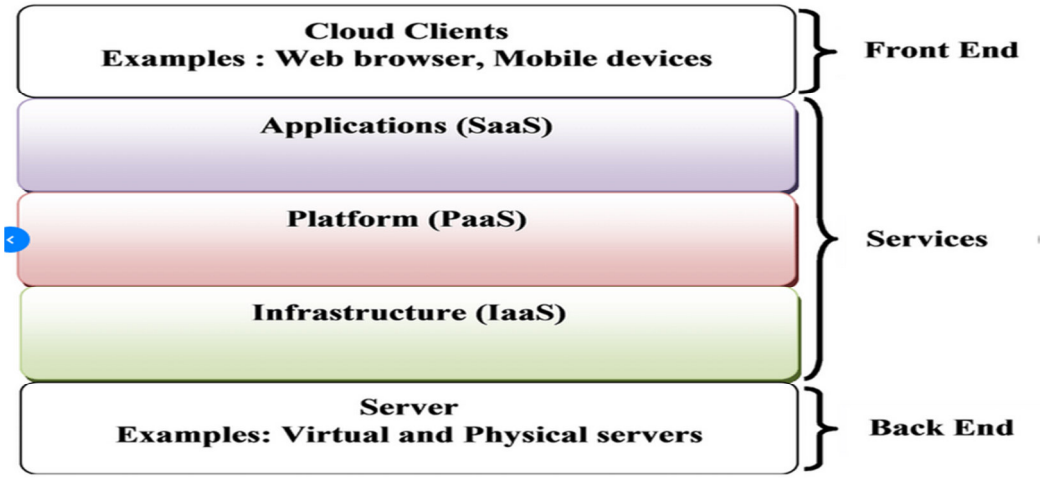

Figure 3: Services of cloud computing with the front and back end of cloud computing

The user or the client of cloud computing services would be in the role of a data controller, and the cloud provider in the role of its contractual data processor, performing certain tasks regarding data processing, such as storage, copying, transferring, etc. A reminder – any handling of personal data is regarded as data processing, and personal data are any information related to an identified or identifiable individual. Be cautious, even if you cannot tell by yourself, who the data is relating to, others may be able to identify the person, without disproportionate effort or means. Identifiability of an individual should be interpreted broadly and not only through the capabilities of a certain entity, and through the presence of the exact data that enable direct identification of an individual.

Certain aspects of data protection, such as the proportionality principle, the purpose of data processing, and retention periods are, of course, an integral part of the framework for data protection. However, in the context of cloud computing they do not present any specificity. The areas that are exposed the most are contractual personal data processing, data security, and transfer of data to third countries (Personal Data Protection and Cloud Computing, 2012).

Protection of Personal Information

One of the most challenging issues arising from cloud computing is protection of personal data. Various cloud aspects pose issues for privacy. Jurisdiction is one of the foremost issues affecting privacy and personal data protection in cloud computing. Within cloud computing, there are no borders. Within this environment, data can be broken up and stored in multiple data centers across multiple jurisdictions. Security becomes the second most important issue. Personal data is processed and stored outside the infrastructure in a data warehouse, which makes it vulnerable to hackers and other forms of data breaches. This vulnerability can result in lost, destroyed or improperly disseminated data. (Reeta Sony A.L, Prof Sri Krishan Deva Rao, Bhukya Devi Prasad, 2013). Data security has regularly been a major issue in IT. Data security becomes particularly serious in the cloud computing environment, because data are distributed in different machines and storage devices including servers, Personal Computers, and various mobile devices such as wireless sensor networks and smart phones. Data security in the cloud computing is more complicated than data security in the traditional information systems (Yunchuan Sun, Junsheng Zhang, Yongping Xiong, Guangyn Zhu, 2014). Data protection and security comprise one of the major challenges in cloud computing. Most organizations adopt network centric and perimeter security, which are normally based on firewalls and intrusion detection systems and which are very much the traditional security systems. This type of data and security protection does not provide sufficient protection against, privileged users, or other insidious types of security attacks, whereas in cloud computing services, the provider may benefit from a data centric approach with encryption, key management, strong access controls, and security intelligence to provide security for the data. Data which is collected from users or consumers for its intended collection purpose and onward transfer or third party use of the data must occur only when authorized by law, as stipulated by the terms of the privacy policy, or according to customer preference. If cloud computing providers fail to manage these challenges, they will be unable to maintain the trust and confidence of their users or consumers.

(Reeta Sony A.L, Prof Sri Krishan Deva Rao, Bhukya Devi Prasad, 2013).

Conclusion

Cloud computing deals with computation, software, data access and storage services that may not require end-user knowledge of the physical location and the configuration of the system that is delivering the services. Cloud

 DOI: 10.7176/CEIS

computing is a recent trend in IT that moves computing and data away from desktop and portable PCs into large data centers (Marios D. Dikaiakos, George Pallis, Dimitrios Katsaros, Pankaj Mehra, Athena Vakali, 2009). The barrier and hurdles toward the rapid growth of cloud computing are data security and privacy issues. Reducing data storage and processing cost is a mandatory requirement of any organization, while analysis of data and information is always the most important tasks in all the organizations for decision making. So no organizations will transfer their data or information to the cloud until the trust is built between the cloud service providers and consumers (Yunchuan Sun, Junsheng Zhang, Yongping Xiong, Guangyn Zhu, 2014). Information security is a fundamental part and one of the essential principles of all the legal acts regulating the field of data protection. As a *narrower part of personal data protection* it refers to the protection of integrity, confidentiality and accessibility of personal data. (Personal Data Protection and Cloud Computing, 2012). Data security becomes particularly serious in the cloud computing environment, because data are distributed in different machines and storage devices including servers, Personal Computers, and various mobile devices such as wireless sensor networks and smart phones. Data security in the cloud computing is more complicated than data security in the traditional information systems. Data protection and security comprise one of the major challenges in cloud computing. Most organizations adopt network centric and perimeter security, which are normally based on firewalls and intrusion detection systems and which are very much the traditional security systems. This type of data and security protection does not provide sufficient protection against, privileged users, or other insidious types of security attacks, whereas in cloud computing services, the provider may benefit from a data centric approach with encryption, key management, strong access controls, and security intelligence to provide security for the data.

References

Cloud Computing Architecture. (n.d.).

Denys, P. (2012, October 12). Security of Personal Information in Cloud Computing.

John Harauz,Lorti M. Kaufman, Bruce Potter. (2009, July/Auguest). Data Security in the world of Cloud Computing. *IEEE Security and Privacy*.

Marios D. Dikaiakos, George Pallis, Dimitrios Katsaros, Pankaj Mehra, Athena Vakali. (2009, Sep/Oct). Cloud Computing: Distributed Internet Computing for IT and Scientific Research. *IEEE Internet Computing*.

National Institute of Standards and Technology. (n.d.). Retrieved from Computer Security Resource Center: www.csrc.nist.gov

Personal Data Protection and Cloud Computing. (2012). Information Commissioner and Cloud Security Alliance Slovenia Chapter.

Reeta Sony A.L, Prof Sri Krishan Deva Rao, Bhukya Devi Prasad. (2013). Implications of Cloud Computing for personal data protection and privacy in the era of the cloud: an Indian perspective. *Law, Journal of the higher school of economics*, 64-80.

Trivedi, H. (2013, may 10). Cloud Computing Adoption Model for Governments and Large Enterprises.

Yashpalsinh Jadeja, Kirit Modi. (2012). Cloud Computing-concepts, Architecture and Challenges. *International Conference on Computing, Electronics and Electrical Technology.*

Yunchuan Sun, Junsheng Zhang, Yongping Xiong, Guangyn Zhu. (2014). Data Security and Privacy in Cloud Computing. *International Journal of Distributed Sensor Networks*. Retrieved from http://dx.doi.org/10.1155/2014/190903