UACEE International Journal of Advances in Computer Networks and its Security – IJCNS
Volume 3 : Issue 2 [ISSN 2250 – 3757]
Publication Date : 05 June 2013

PRIVACY ISSUES IN CLOUD COMPUTING FOR PERSONAL AREA NETWORK

Ankur Chaudhary, Neeti Bisht, Lokesh Kumar, Sachin Choudhary

Abstract: Data security means ensuring that data is kept safe from corruption and that access to it is suitably controlled. It helps in protecting the individual data. This paper focused on cloud data security. Cloud Computing moves the application software and databases to the large data centers, where the management of the data and services are fully trustworthy. The security objectives of an organization are a key factor for decisions about outsourcing information technology services and, in particular, for decisions about transitioning data, applications, and other resources to a public cloud computing environment. The information technology governance practices of the organizations that pertain to the policies, procedures, and standards used for application development and service provisioning, as well as the design, implementation, testing services, should be extended to cloud computing environments. Security and privacy issues are presented in this paper when cloud computing is implemented in personal area networks.

Key words: Cloud computing, Virtualization, Distributed Computing, management System.

I. Introduction

Today security is major challenge of any kind of User. In existing system we have lot of option of protecting our data but all protection comes under client side. If our system is crashed or infected by external virus and our existing tools are not able to handle from these serious issues then we have no option to solve it and all time we fear about our data protection. Therefore our other works are also infected by it. Here we propose security as service by cloud computing. In cloud computing we can use the infrastructure of cloud computing to do our work and also give permission to store and provide protection to our data a long life. In this system all kind of security issues are handled by server side so client is secure. Cloud Computing also provide any ware accessing concept, means that if we use cloud computing then we can give security to our data as well as we can access the data anywhere anytime. This is the influence of cloud computing.

II. Cloud computing

Cloud computing is computing technology that uses the internet and central remote servers to maintain data and applications. It allows consumers and businesses to use applications without installation and access their personal files at any computer with internet access. This technology allows for much more efficient computing by centralizing storage, memory, processing and bandwidth [1].

Cloud computing is a way to increase capacity or add capabilities on the fly without investing in new infrastructure, training new personnel, or licensing new software.

Cloud computing is an extension of old main frame concepts of sharing with the addition of networking and application runs. Cloud has several Advantages like costs, capacity additions, availability, security, experimentation with new technologies, IT management, minimal use of resources etc [2].

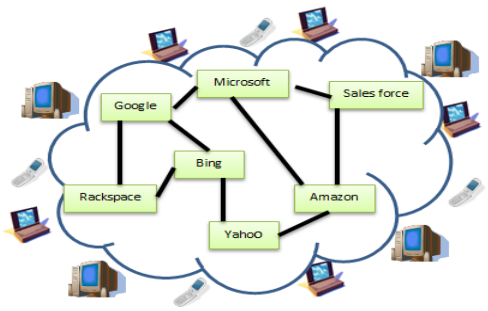

Figure 1 Cloud computing conceptual diagram

The scalability and flexibility are the most important features that drive the emergence of the Cloud computing. Cloud services and computing platforms offered by computing.

Clouds could be scaled across various concerns, such as geographical locations, hardware performance, and software configurations.

III. Cloud service models

- **Platform-as-a-service:** Here, the services provide the entire infrastructure needed to run applications over the Internet just as electricity supply. Further, the services are delivered on the subscription model where the users only pay for what they use [3].

- **Application-as-a-service:** It is also known as Software-as-a-Service (SaaS) or on-demand software. Here, the services offer various application delivered over a network to the end user, for example Google Docs, Gmail, and Google Calendar.

- **Infrastructure-as-a-service:** It is a type of datacenter as a service, where the service provider remotely offers access to its computing resources. Here, the firms hire the whole datacenter or a part of datacenter for all practical purposes [3].

- **Security-as-a-service:** These services refer to the protection against cyber-risk. It provides security applications, which is internet-based service, on-demand, to consumers and businesses. It consists of log management, filtering services and asset tracking including anti-virus, anti-spam and anti-spyware [3].

- **Testing-as-a-service:** This service can test other cloud applications by using testing software and services, which are remotely hosted. Also, these services include various features and functions that are present within traditional EAI technology.

- **Storage-as-a-service:** SaaS is a type of software deployment whereby a provider licenses an application to customers for use as a service on demand and disabling it after use or after the on-demand contract expires. SaaS software vendors may host the application on their own web servers or download the application to the consumer device.

- **Database-as-a-service:** It allows users to access services on the remotely hosted database, which can be easily shared with other users. It can save lots of money in hardware and software licenses.

- **Process-as-a-service:** These services allow users to attach various resources together to create business processes, which can be present within the same cloud computing resource or remote.

- **Integration-as-a-service:** These services were started back in 80s, from the slow evolution of the Business-to-business Integration market. In starting, Value Added Networks, provide such EDI services. But now, these services include integration with applications, semantic mediation, flow control, integration design, etc.

IV. Types of cloud computing

Public Cloud -A public cloud sells services to anyone on the Internet. (Currently, Amazon Web Services is the largest public cloud provider.) [4]

Private Cloud -A private cloud is a proprietary network or a data center that supplies hosted services to a limited number of people. [4]

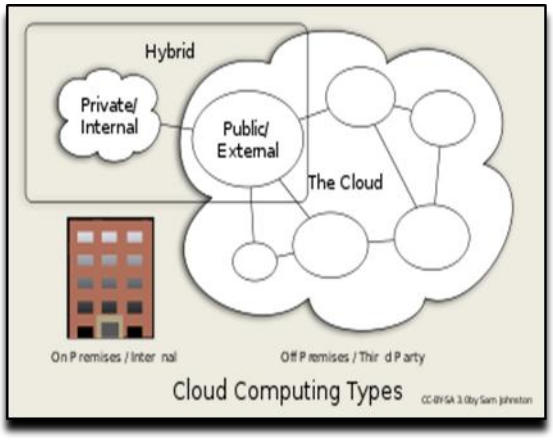

Figure 2 Types of Cloud Computing

When a service provider uses public cloud resources to create their private cloud, the result is called a virtual private cloud.

V. Security and privacy issues

Governance: Governance implies control and oversight over policies, procedures, and standards for application development, as well as the design, implementation, testing, and monitoring of deployed services. With the wide availability of cloud computing services, lack of organizational controls over employees engaging such services arbitrarily can be a source of problems. While cloud computing simplifies platform acquisition, it doesn't alleviate the need for governance; instead, it has the opposite effect, amplifying that need.

Compliance: Compliance involves conformance with an established specification, standard, regulation, or law. Various types of security and privacy laws and regulations exist within different countries at the

national, state, and local levels, making compliance a potentially complicated issue for cloud computing [4].

Trust: Under the cloud computing paradigm, an organization relinquishes direct control over many aspects of security and, in doing so, confers an unprecedented level of trust onto the cloud provider [4].

Architecture: The architecture of the software systems used to deliver cloud services comprises hardware and software residing in the cloud. The physical location of the infrastructure is determined by the cloud provider as is the implementation of the reliability and scalability logic of the underlying support framework. Virtual machines often serve as the abstract unit of deployment and are loosely coupled with the cloud storage architecture [4].

Applications are built on the programming interfaces of Internet-accessible services, which typically involve multiple cloud components communicating with each other over application programming interfaces. Many of the simplified interfaces and service abstractions belie the inherent complexity that affects security.

***Identity and Access Management*:** One recurring issue is that the organizational identification and authentication framework may not naturally extend into the cloud and extending or changing the existing framework to support cloud services may be difficult. The alternative of employing two different authentication systems, one for the internal organizational systems and another for external cloud-based systems, is a complication that can become unworkable over time. Identity federation, popularized with the introduction of service oriented architectures, is one solution that can be accomplished in a number of ways, such as with the Security Assertion Markup Language (SAML) standard or the OpenID standard [4].

Software Isolation: High degrees of multi-tenancy over large numbers of platforms are needed for cloud computing to achieve the envisioned flexibility of on-demand provisioning of reliable services and the cost benefits and efficiencies due to economies of scale. To reach the high scales of consumption desired, cloud providers have to ensure dynamic flexible delivery of service and isolation of subscriber resources. It is important to note that applications deployed on guest virtual machines remain susceptible to attack and compromise, much the same as their non-virtualized counterparts [4].

Data Protection: Data stored in the cloud typically resides in a shared environment collocated with data from other customers. Organizations moving sensitive and regulated data into the cloud, therefore, must account for the means by which access to the data is controlled and the data is kept secure [4].

Availability: availability is the extent to which an organization's full set of computational resources is accessible and usable. Availability can be affected temporarily or permanently, and a loss can be partial or complete. Denial of service attacks, equipment outages, and natural disasters are all threats to availability. The concern is that most downtime is unplanned and can impact the mission of the organization [4].

Incident Response: As the name implies, incident response involves an organized method for dealing with the consequences of an attack against the security of a computer system. The cloud provider's role is vital in performing incident response activities, including incident verification, attack analysis, containment, data collection and preservation, problem remediation, and service restoration. Revising an organization's incident response plan to address differences between the organizational computing environment and a cloud computing environment is an important, but easy-to-overlook prerequisite to transitioning applications and data [4].

VI. Security benefits of cloud computing

Staff Specialization: Cloud providers, just as organizations with large-scale computing facilities, have an opportunity for staff to specialize in security, privacy, and other areas of high interest and concern to the organization. Through increased specialization, there is an opportunity for staff members gain in-depth experience, take remedial actions, and make security improvements more readily than otherwise would be possible with a diverse set of duties [5].

Platform Strength: The structure of cloud computing platforms is typically more uniform than that of most traditional computing centers. Greater uniformity and homogeneity facilitate platform hardening and enable better automation of security management activities like configuration control, vulnerability testing, security audits, and security patching of platform components.

Resource Availability: The scalability of cloud computing facilities allows for greater availability. Redundancy and disaster recovery capabilities are built into cloud computing environments and on-demand resource capacity can be used for better resilience when facing increased service demands or distributed denial of service attacks, and for quicker recovery from serious incidents.

Backup and Recovery: The backup and recovery policies and procedures of a cloud service may be superior to those of the organization and, if copies are maintained in diverse geographic locations, may be more robust. Cloud services could also serve as a means for offsite backup storage for an organization's data center, in lieu of more traditional tape-based offsite storage.

Mobile Endpoints: The architecture of a cloud solution extends to the client at the service endpoint, used to access hosted applications. Cloud clients can be browser-based applications-based. Since the main computational resources needed are held by the cloud provider, clients are generally lightweight computationally and easily supported on laptops, notebooks, as well as embedded devices such as smart phones, tablets, and personal digital assistants [8].

Data Concentration: Data maintained and processed in the cloud can present less of a risk to an organization with a mobile workforce than having that data dispersed on portable computers or removable media out in the field, where theft and loss of devices routinely occur.

Cloud Oriented: Cloud services are available to improve the security of other cloud environments. For example, reverse proxy products are available that enable unfettered access to a SaaS environment, yet maintain the data stored in that environment in encrypted form. Cloud-based identity management services also exist, which can be used to augment or replace an organization's directory service for identification and authentication of users to a cloud.

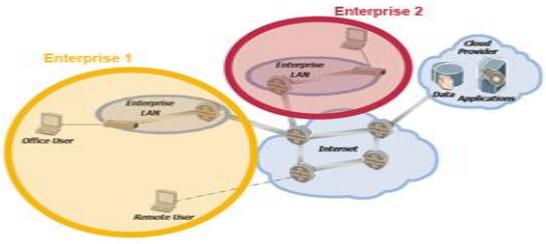

Figure 2: Cloud Computing Providers

Data Center Oriented: Cloud services can be used to improve the security of data centers. For example, electronic mail can be redirected to a cloud provider via mail exchange (MX) records, examined and analyzed collectively with similar transactions from other data centers to discover widespread spam, phishing, and malware campaigns, and to carry out remedial action (e.g., quarantining suspect messages and content) more comprehensively than a single organization would be able to do.

VII. Conclusion

While the biggest obstacle facing public cloud computing is security, the cloud computing paradigm provides opportunities for innovation in provisioning security services that hold the prospect of improving the overall security of some organizations. The biggest beneficiaries are likely to be smaller organizations that have limited numbers of information technology administrators and security personnel, and lack the economies of scale available to larger organizations with sizeable data centers. Here we propose a way by which we can ensure the correctness of user's data in the cloud, we propose an effective and flexible distributed scheme. Cloud Computing moves the application software and databases to the large data centers, where the management of the data and services are fully trustworthy. We can use the concept of cloud computing for privacy and security without increasing cost and infrastructure. Here all the responsibility is going through server side then user have no fear about it.

References

[1] Pastaki rad, m., Sajedi badashian, a., Meydanipour, g., Ashurzad delcheh, m., Alipour, m. and Afzali, h, "A Survey of Cloud Platforms and Their Future", Springer-Verlag Berlin Heidelberg, 2009

[2] Plummer, d.c., Bittman , t.j., Austin, t., cearley, d.w., and Smith d.m., "Cloud Computing: Defining and Describing an Emerging Phenomenon" , 2008 .

[3] SEDAYAO, J. "Implementing and operating an internet scale distributed application using service oriented architecture principles and cloud computing infrastructure" in iiWAS '08: Proceedings of the 10th International Conference on Information Integration and Web-based Applications & Services,2008

[4] www.wikipedia.org

[5] Birman, K., Chockler, G., and van Renesse, R. "Toward a cloud computing research agenda", SIGACT News, 40, 2, 68-80,2008

Ankur Chaudhary completed his B.Tech in Computer Science and Engineering from RIT, Roorkee. Presently he is doing M.Tech in Computer Science and Engineering from Tula's Institute, Dehradun. His research interest is in cloud computing, VANET's, wireless networking.

Neeti Bisht is a Ph.D. scholar at Sharda University, Greater Noida, India and is currently working as an Assistant Professor in the Tula's Institute, Dehradun (The Engineering & Management College) Uttarakhand India, facilitating the MTech & BTech students academically and in their Research Work as well. She had presented their Research Papers in various International and National Conferences and Journals and attended various workshops as well. Her specialization and research work is in Wireless Communication and Networking. And her research interest includes sensor networks, ad-hoc networks, cloud computing and security issues.

Lokesh Kumar completed his B.Tech in Computer Science and Engineering from RIT, Roorkee. Presently he is doing M.Tech in Computer Science and Engineering from Tula's Institute, Dehradun. His research interest is in sensor networks, cloud computing, automata, computer architecture.

Sachin Choudhary completed his B.Tech in Computer Science and Engineering from RIT, Roorkee. Presently he is doing M.Tech in Computer Science and Engineering from Tula's Institute, Dehradun. His research interest is in wireless networking, cloud computing, graph theory.