INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

CLOUD COMPUTING WITH PRIVACY MANAGER

MISS. SHRADDHA A. MEHARE[1], PROF. A. R. MUNE[2]

1. Student of Master of Engineering in (CSE), IBSS college of Engineering and Technology, Amravati, India.
2. Assistant professor Department of (CSE), IBSS College of Engineering and Technology, Amravati, India.

Accepted Date: 05/03/2015; Published Date: 01/05/2015

Abstract: Cloud computing is the delivery of computing services over the Internet. Whether they realize it or not, many people use cloud computing services for their own personal needs. For example, many people use social networking sites or webmail, and these are cloud services. Photographs that people once kept on their own computers are now being stored on servers owned by third parties. We describe a privacy manager for cloud computing, which reduces the risk to the cloud computing user of their private data being stolen or misused. And different possible architectures for privacy management in cloud computing [1].

Keywords: Cloud Computing, Privacy

Corresponding Author: MS. SHRADDHA A. MEHARE

Access Online On:

www.ijpret.com

How to Cite This Article:

Shraddha A. Mehare, IJPRET, 2015; Volume 3 (9): 1274-1280

PAPER-QR CODE

INTRODUCTION

Cloud Computing has been one of the most booming technology among the professional of information Technology and also the Business due to its Elasticity in the space occupation and also the better support for the software and the Infrastructure it attracts more technology specialist towards it.

We describe a privacy manager for cloud computing, which reduces the risk to the cloud computing user of their private data being stolen or misused, and also assists the cloud computing provider to conform to privacy law. Cloud computing, in which services are carried out on behalf of customers on hardware that the customers do not own or manage, is an increasingly fashionable business model. The input data for cloud services is uploaded by the user to the cloud, which means that they typically result in users data being present in unencrypted form on a machine that the user does not own or control. This poses some inherent privacy challenges. There is a risk of data theft from machines in the cloud, by rogue employees of cloud service providers or by data thieves breaking into service providers' machines, or even by other customers of the same service if there is inadequate separation of different customers' data in a machine that they share in the cloud.

Service models:-

The cloud computing service models are Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). In a Software as a Service model, a pre-made application, along with any required software, operating system, hardware, and network are provided. In PaaS, an operating system, hardware, and network are provided, and the customer installs or develops its own software and applications. The IaaS model provides just the hardware and network; the customer installs or develops its own operating systems, software and applications.

Deployment of cloud services:- Cloud services are typically made available via a private cloud, community cloud, public cloud or hybrid cloud.

Generally speaking, services provided by a **public cloud** are offered over the Internet and are owned and operated by a cloud provider. Some examples include services aimed at the general public, such as online photo storage services, e-mail services, or social networking sites. However, services for enterprises can also be offered in a public cloud.

In a **private cloud**, the cloud infrastructure is operated solely for a specific organization, and is managed by the organization or a third party.

In a **community cloud**, the service is shared by several organizations and made available only to those groups. The infrastructure may be owned and operated by the organizations or by a cloud service provider. A **hybrid cloud** is a combination of different methods of resource pooling (for example, combining public and community clouds).

Privacy Manager:-

Privacy Manager, which helps the user manage the privacy of their data in the cloud. As a first line of defence, the privacy manager uses a feature called *obfuscation*, where this is possible. The idea is that instead of being present unencrypted in the cloud, the user's private data is sent to the cloud in an encrypted form, and the processing is done on the encrypted data. The result of the processing is de-obfuscated by the privacy manager to reveal the correct result. (We call it obfuscation rather than encryption because some of the information present in the original data is in general still present in the obfuscated data.) The obfuscation method uses a key which is chosen by the user and known by the privacy manager, but which is not communicated to the service provider. Thus the service provider is not able to de-obfuscate the user's data, and this data is not present on the service provider's machines, reducing (or even eliminating) the risks of theft of this data from the cloud and unauthorized uses of this data. Moreover, the obfuscated data is not personally identifiable information, and so the service provider is not subject to the legal restrictions that apply to the processing of the unobfuscated data. Where obfuscation is practical, the principle of data minimization gives a legal impetus to use it. However, it is not practical for all cloud applications to work with obfuscated data. For applications for which users have to upload some private data to the cloud, the privacy manager contains two additional features, called *preferences* and *personae*, which help the users to communicate to service providers their wishes for the use of this personal data, and thus assist the service providers to respect privacy laws requiring users' consent.

Privacy Manager in the Client

The architecture of our solution is illustrated in fig. Privacy Manager Software on the client helps users to protect their privacy when accessing cloud services. A central feature of the Privacy Manager is that it can provide an obfuscation and de-obfuscation service, to reduce the amount of sensitive information held within the cloud. In addition, the Privacy Manager allows the user to express privacy preferences about the treatment of their personal information, including the degree and type of obfuscation used. Personae – in the form of icons that correspond to sets of privacy preferences – can be used to simplify this process and make it more intuitive to the user. So for example, there could be an icon with a mask over a face that corresponds to maximal privacy settings, and other icons that relate to a lower level of protection of certain types of personal data in a given context. The user's personae will be defined by the cloud service interaction context.

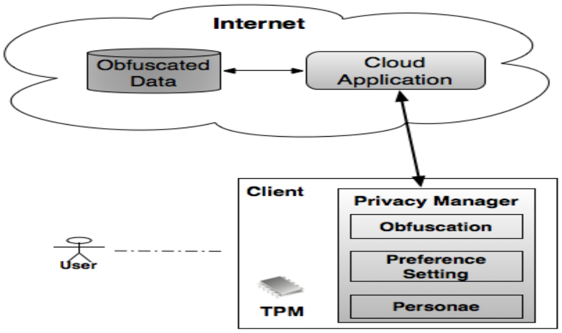

Figure 1. Client-Based Privacy Manager

Privacy Manager in a Hybrid Cloud:

As an alternative, as illustrated in Figure 2, the Privacy Manager may be deployed in a local network or a private cloud, to protect information relating to multiple parties. This would be suitable in environments, such as enterprise environments, where local protection of information is controlled in an adequate manner and its principal use would be to control personal information passing to a public cloud. The Privacy Manager can itself be virtualized within the internal cloud. Note that the TPM could also be virtualized, within the private cloud.

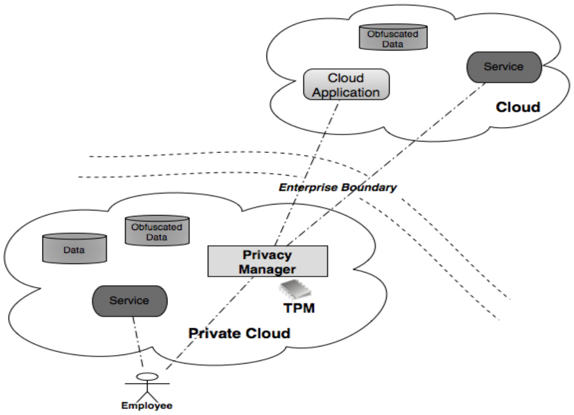

Figure:-Enterprise-focused Privacy Manager

Advantages to this approach include that the benefits of the cloud can be reaped within the private cloud, including the most efficient provision of the Privacy Manager functionality. It can provide enterprise control over dissemination of sensitive information, and local compliance. A significant issue however is scalability, in the sense that the Privacy Manager might slow down traffic, provide a bottleneck and may not be able to adequately manage information exposed between composed services. There are various different options with respect to this type of architecture. For example, the proxy capability could be combined, even in a distributed way, with other functionalities, including identity management. Another example is that trusted virtual machines could be used within the privacy cloud to support strong enforcement of integrity and security policy controls over a virtual entity (a guest operating system or virtual appliance running on a virtualized platform). It would be possible to define within the Privacy Manager different personae corresponding to different groups of cloud services, using different virtualized environments on each end user device. In this way, virtualization is used to push control from the cloud back to the client platform. As with the previous architecture, there could be mutual attestation of the platforms, including integrity checking.

Privacy Infomediary within the Cloud :-

Figure shows how the Privacy Manager may be deployed as (part of) a privacy infomediary , mediating data transfer between different trust domains. The Privacy Manager would act on behalf of the user and decide the degree of data transfer allowed, based upon transferred user policies and the service context, and preferably also an assessment of the trustworthiness of the service provision environment. Notification and feedback by the Privacy Manager to the user would also be preferable here, in order to increase transparency and accountability.

The infomediary could be a consumer organization or other entity that is trusted by the users. It might alternatively be an entity that already exists within the cloud in order to provide an alternative function, such as an identity provider or auditor, and the functionality could be an extension of that. For example, the open source project Otemba implements key management and user management, separating cryptographic keys from the cloud infrastructure. A key management role might be extended to a general infomediary role.The infomediary may also play a role in checking that the user preferences are satisfied before providing a decryption key for decrypting any data that needs to be decrypted in order for the cloud service to be provided (for example, it could be a Trust Authority in order to provide IBE decryption keys). Again, trusted infrastructure could be useful in ensuring that the infrastructural building blocks of the cloud are secure, trustworthy and compliant with security best practice[2].

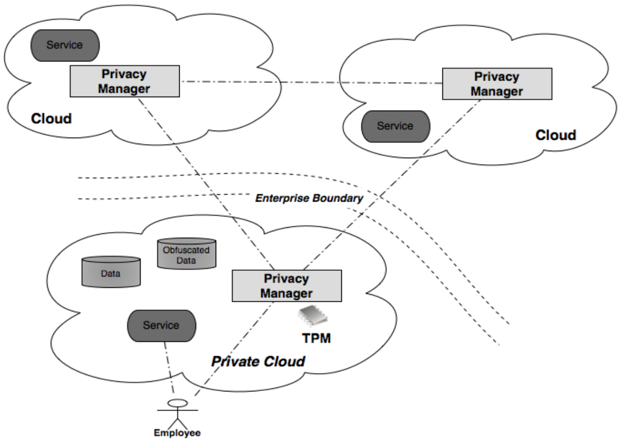

Figure 3. Privacy Manager within the Cloud

Features of Cloud Services:-

Cloud services are popular because they can reduce the cost and complexity of owning and operating computers and networks. Since cloud users do not have to invest in information technology infrastructure, purchase hardware, or buy software licences, the benefits are low up-front costs, rapid return on investment, rapid deployment, customization, flexible use, and solutions that can make use of new innovations. In addition, cloud providers that have specialized in a particular area (such as e-mail) can bring advanced services that a single company might not be able to afford or develop.

Some other benefits to users include scalability, reliability, and efficiency. Scalability means that cloud computing offers unlimited processing and storage capacity. The cloud is reliable in that it enables access to applications and documents anywhere in the world via the Internet. Cloud computing is often considered efficient because it allows organizations to free up resources to focus on innovation and product development [2].

CONCLUSION:-

In conclusion, we have described cloud computing with privacy manager. In cloud computing characteristic there are two type: Service Models and Deployment of Cloud services, Features of cloud services. And we have also explored how the architecture would vary for different scenarios.

REFERENCES:-

1. Mowbray, M., Pearson, S.: A client-based privacy manager for cloud computing.In COMSWARE '09. ACM

2. World Wide Web Consortium (W3C): Platform for Privacy Preferences (P3P) Project

3. Mowbray, M.: The Fog over the Grimpen Mire: Cloud Computing and the Law. Scripted Journal of Law, Technology and Society, Volume 6, no.1, April (2009)

4. Pearson, S. (Ed.): Trusted Computing Platforms.

5. Organization for Economic Co-operation and Development (OECD): Guidelines Governing the Protection of Privacy and Transborder Flow of Personal Data. OECD, Geneva (1980)

6. Salmon, J.: Clouded in uncertainty – the legal pitfalls of cloud computing. Computing magazine (24 Sept 2008).

7. Mowbray, M.: The Fog over the Grimpen Mire: Cloud Computing and the Law. Scripted Journal of Law, Technology and Society

8. Pearson, S. (Ed.): Trusted Computing Platforms

9. Linux kernel. Wikipedia.

10. Jerome H.Saltzer. Protection and the control of information sharing in multics. *Commun. ACM*, 17(7):388–402, 1974.