INTERNATIONAL JOURNAL OF
RESEARCH AND CURRENT DEVELOPMENT
Available Online at http://www.journalijrcd.com
VOL. 1, ISSUE, 1, PP.17-19, NOVEMBER, 2016

IJRCD

ISSN: XXX-XXXX

RESEARCH ARTICLE

SECURITY CHALLENGES AND EFFICIENT DATA PROTECTION IN TRUSTED CLOUD ENVIRONMENT

Saranya S*

Department of CSE Velammal Engineering College Chennai, India

ARTICLE INFO

Article History:

Received 15th September, 2016
Received in revised form 25th October, 2016
Accepted 23rd November, 2016
Published online 28th December, 2016

Keywords:

TCCP, Cloud Environment, Private Data Protection

ABSTRACT

Cloud computing transforms the way information technology (IT) is consumed and managed, promising improved cost efficiencies, accelerated innovation, faster time-to-market, and the ability to scale applications on demand. While the great thing about the cloud is that you can access it from anywhere, the downside is you may never know exactly where your data is being stored. Therefore several security models and trust establishing techniques have been deployed and are been in execution for providing more security to the data, especially the sensitive data. To address this problem we propose the design of a trusted cloud computing platform (TCCP). Moreover, it allows users to determine whether or not the service is secure before they launch in Cloud Environment

INTRODUCTION

The term "cloud", appears to have its origins in network diagrams that represented the internet, or various parts of it, as schematic clouds. "Cloud computing" was coined for what happens when applications and services are moved into the internet "cloud." Cloud computing is not something that suddenly appeared overnight; in some form it may trace back to a time when computer systems remotely time-shared computing resources and applications. More currently though, cloud computing refers to the many different types of services and applications being delivered in the internet cloud, and the fact that, in many cases, the devices used to access these services and applications do not require any special applications.

Cloud computing has a variety of characteristics, with the main ones being:

- Shared Infrastructure — Uses a virtualized software model, enabling the sharing of physical services, storage, and networking capabilities. The cloud infrastructure, regardless of deployment model, seeks to make the most of the available infrastructure across a number of users.
- Dynamic Provisioning — Allows for the provision of services based on current demand requirements. This is done automatically using software automation, enabling the expansion and contraction of service capability, as needed. This dynamic scaling needs to be done while maintaining high levels of reliability and security.
- Network Access — Needs to be accessed across the internet from a broad range of devices such as PCs, laptops, and mobile devices,
- using standards-based APIs (for example, ones based on HTTP). Deployments of services in the cloud include everything from using business applications to the latest application on the newest Smartphone's.
- Managed Metering — uses metering for managing and optimizing the service and to provide reporting and billing information. In this way, consumers are billed for services according to how much they have actually used during the billing period.

Pursuant to the provisions of the PDPA normally 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. Identifiably 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 the following: contractual personal data processing, data security, and transfer of data to third countries.

This paper proposes a trusted cloud computing platform (TCCP) for ensuring the confidentiality and integrity of computations that are outsourced to IaaS services. The TCCP provides the abstraction of a closed box execution

Corresponding author:* **Saranya S
Department of CSE Velammal Engineering College Chennai, India

environment for a customer's VM, guaranteeing that no cloud provider's privileged administrator can inspect or tamper with its content. Moreover, before requesting the service to launch a VM, the TCCP allows a customer to reliably and remotely determine whether the service backend is running a trusted TCCP implementation. This capability extends the notion of attestation to the entire service, and thus allows a customer to verify if its computation will run securely. In this paper we show how to leverage the advances of trusted computing technologies to design the TCCP. Section 2 introduces data protection in cloud environment. Section 3 security challenges of private data in cloud environment. Section 4 describes User Satisfaction in Trusted Environment.

Data Protection in Cloud Environment

Open Issues on Data Protection

No borders with in the cloud the concept of cloud computing is globalized, and within the cloud there are no borders. The customer's data then remains within the selected zone. Regarding data protection, cloud computing raises a number of interesting issues. Data protection law is based on the premise that it is always clear where personal data is located, by whom it is processed and who is responsible for data processing. Cloud computing appears to fundamentally conflict with this evidence. For example, if a customer uses an e-mail service based on cloud computing, the customer's data can be stored anywhere in the world, depending on where the servers on which the necessary storage capacity is available are located. Different services supplied by a wide range of providers are regularly bundled to produce an end-user proposal, for example, if the mail service provider obtains the storage capacity required to store its customers' data from other providers. Therefore, with cloud computing it is no longer possible to say where the data is at a certain moment and by whom and how it is being processed. This means that it is doubtful whether those responsible for data processing, in accordance with data-protection regulations, are in a position to effectively assume their responsibility at all. If the data circulates freely around the globe via the internet, it is also no longer clear which data-protection authorities at which location are responsible for ensuring the observance of the principles of data Protection.

Cloud computing can be deployed using a number of different models.

- Private cloud – The cloud customer is the sole user of the cloud service. The underlying hardware may be managed and maintained by a cloud provider under an outsourcing contract. Access to the cloud service may be restricted to a local or wide area network.
- Community cloud – A group of cloud customers access the resources of the same cloud service. Typically the cloud customers will share specific requirements such as a need for legal compliance or high security which the cloud service provides. Access to the cloud service may be restricted to a wide area network.
- Public cloud – The infrastructure, platform or software is managed by the cloud provider and made available to the general public (cloud customers or cloud end-users). Access to the cloud service is likely to be over the public internet
- Therefore we are enhancing data in the cloud environment and also preserve such data in private cloud storage. Private cloud storage, also called internal cloud storage, is a service delivery model for storage within a large enterprise. Internal cloud storage runs on a dedicated infrastructure in the data center, offering the same scalability benefits of public cloud storage to corporate departments and partners while addressing security and performance concerns.

Security Challenges of Private Data in Cloud Environment

As a designer of a private cloud solution, you should design access control for the services hosted in the cloud. You should also determine who can request services and how much they can request. This section describes how these capabilities relate to the on- demand self-service attribute of private clouds. The on-demand, self-service characteristic of a public cloud implies that anyone with a credit card can purchase the resources they need as and when they require them. For the private cloud, you must determine who within the enterprise should have the authority to request resources from your private cloud (and who has the authority to release those resources when they are no longer required). The key issues associated with the on-demand self-service attribute of the private cloud are therefore:

- Authentication, authorization, and role-based access controls that control who, within the organization, may provision and manage cloud-based resources.
- Monitoring and auditing the use of a provisioning portal to ensure that controls are applied effectively.

In a private cloud, the client who requests the resources may not be a separate business unit within the organization but can be the IT department itself, acquiring resources from the cloud on behalf of a client business unit. In this scenario, one of the benefits derived by the organization is the ability of the IT department to make new infrastructure resources available much faster than in a more traditional architecture.

Infrastructure Security

Apart from being able to initiate requests to provision and de-provision cloud resources, tenants should have no access to the private cloud physical infrastructure. If your private cloud supports the IaaS service delivery model, then your self-service provisioning portal should enable clients to request virtual infrastructure resources.

Platform Security

Although from the perspective of the tenant the request for a resource such as a virtual machine to host a departmental application may appear to be a single operation, the provisioning process is more complex.

ISSN:XXXX-XXXX

User Satisfaction in Trusted Environment

Trust refers to a belief on reliability, security, dependability and ability of an entity that acts in particular environment. The ultimate goal of trust evaluation in the network is not completely eliminate incredibility, but rather to help system administrators to balance "providing services" and "credible assurance". It is an active testing before the attack. Creation and updating of trust for cloud users are based on the evidence of various acts directly or indirectly. User behaviour is the basic evidence used to quantitatively assess the trust value. The service provider may obtain objective evidence directly from the hardware. Access Control Process by User Behaviour

The cloud service provider can refuse to provide services for untrustworthy users to prevent unauthorized users from misuse or destruction of resources in cloud. Service providers also take punishment for these users, for example, blacklisting.

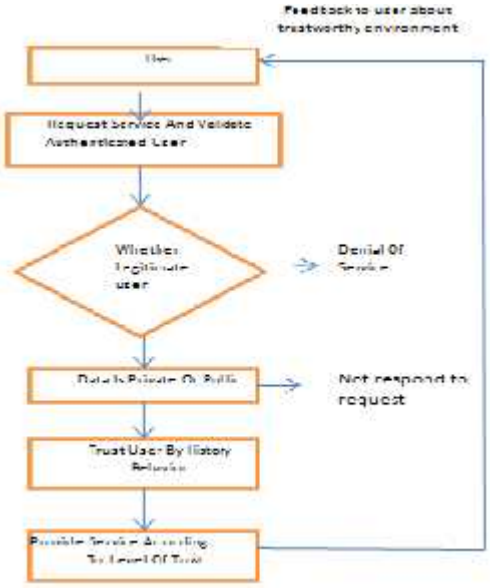

Figure1 Control Flow analysis of trusted environment

For users who have a certain level of trust, cloud service providers can take access policies to limit them. For example, cloud service providers only give a very low privilege to users; only let them take limited operation and take no impact on providers; and warn users to avoid continue to take mistrust behaviour.

Therefore, the purpose of dividing the trust into different level is to use different measures for different users. Trust value feedback on the user, can guide the user to take a more trustworthy behaviour, and to improve the safety awareness of terminal user. Fig. 1 shows a control flowchart of the process.

CONCLUSION

This paper describes about trust worthy environment of user and security provided to data in cloud environment. Cloud Environment has lot of security issues and issues are resolved in the proposed system. This trusted environment considers only private data. In future, we focus and implement the same for public data

References

C. M. Rong, Son T. Nguyen and Martin Gilje Jaatun. Beyond Lightning: a Survey on Security Challenges in Cloud Computing, Computers & Electrical Engineering, Vol. 39, No. 1, 2013, pp. 47-54

A. K. Rao, "Centralized Database Security in Cloud," *International Journal of Advanced Research in Computer and Communication Engineering* (IJARCCE), vol.1, pp.544-549, 2012.

S. Berger, R. C´aceres, K. A. Goldman, R. Perez, R. Sailer and L. van Doorn. vTPM: virtualizing the trusted platform module. In Proc. Of USENIX-SS'06, Berkeley, CA, USA, 2006.

T. Garfinkel, B. Pfaff, J. Chow, M. Rosenblum and D. Boneh. Terra: A Virtual Machine-Based Platform for Trusted Computing. In Proc. of SOSP'03, 2003 [4]

How to cite this article:
Saranya S. 2016, Security Challenges and Efficient Data Protection in Trusted Cloud Environment. *International Journal of Research and Current Development*; 1(1): 17-19.