Research Article | Impact Factor: 0.621 | ISSN: 2319-507X
Shraddha Gupta, IJPRET, 2014; Volume 2 (9): 252-257 | IJPRET

INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

ADVANCED DATA SECURITY IN CLOUD COMPUTING

MISS SHRADDHA S. GUPTA

M. E. in Computer Science and Engineering, I. B. S. S., College of Engineering, Amravati.

Accepted Date: 27/02/2014 ; Published Date: 01/05/2014

Abstract: The ever-growing computing and networking technologies today are enabling a fundamental paradigm shift in how people deploy and deliver computing services: computing outsourcing. While moving data and computing services to the cloud alike infrastructures promises to provide unprecedented benefits like ubiquitous network access, rapid resource elasticity, minimal management overhead, etc., it simultaneously deprives users of direct control over the systems that manage their data and applications, raising security and privacy the primary obstacles to the public cloud adoption. So Data security is one of the biggest concerns in adopting Cloud computing. In Cloud environment, users remotely store their data and relieve themselves from the hassle of local storage and maintenance. However, in this process, they lose control over their data. Existing approaches do not take all the facets into consideration viz. dynamic nature of Cloud, computation & communication overhead etc. In this paper, we propose Data Storage Security by using Trusted Platform Module to achieve storage correctness incorporating Cloud's dynamic nature while maintaining low computation and communication cost and ensure the security of static data.

Keywords: Cloud Computing ,Security issues, Cloud Service Provider

Corresponding Author: MISS SHRADDHA S. GUPTA

Access Online On:

www.ijpret.com

How to Cite This Article:

Shraddha Gupta, IJPRET, 2014; Volume 2 (9): 252-257

PAPER-QR CODE

INTRODUCTION

Cloud computing has been a concept and a buzz word in the computing industry for many years now, the term has been widely used with many businesses not fully understanding what it actually is and how it will benefit them. The reason why the term was not fully understood was because it was still a concept and the underlying virtualization technology needed and our own networking infrastructure was still in its infancy which meant we could not unlock the full potential of cloud computing, until now. The National Institute of standards & Technology (NIST) defines cloud computing as a model for enabling ubiquitous, 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. cloud computing is not a new technology but rather a new delivery model for computing infrastructure, services and information using many existing technologies that have been harnessed and made available by the cloud service provider's (CSP's). Cloud service providers use the Internet infrastructure to allow communication between client side and server side services/applications [4] and offer the customer/user a pay-per-use model of the CSP's computing resources and infrastructure. Cloud computing can be described as a usage model in which resources are deliveries and, it means to provide resources, such as hardware, software and applications as scalable and "on-demand" services via public network in a multitenant environment.[1]

2. OVERVIEW OF CLOUD COMPUTING

Cloud computing as a delivery model for IT services is defined by the National Institute of Standards and Technology (NIST) as "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.

NIST specify five characteristics of cloud computing that describe and differentiate Cloud services from conventional computing approaches:

2.1.Self Service

Firstly On-demand self-service involves customers using a web site or similar control panel interface to provision computing resources such as additional computers, network bandwidth or user email accounts, without requiring human interaction between customers and the vendor.

2.2. Network Access

Secondly broad network access enables customers to access computing resources over networks such as the Internet from a broad range of computing devices such as laptops and smartphones.

2.3. Resource Pooling

Thirdly Resource pooling involves vendors using shared computing resources to provide cloud services to multiple customers. Virtualization and multi-

tenancy mechanisms are typically used to both segregate and protect each customer and their data from other customers, and to make it appear to customers that they are the only user of a shared computer or software application.

2.4. Rapid elasticity

Rapid elasticity enables the fast and automatic increase and decrease to the amount of available computer processing, storage and network bandwidth as required by customer demand.

2.5. Pay-per-use

Lastly Pay-per-use measured service involves customers only paying for the computing resources that they actually use, and being able to monitor their usage. This is analogous to household use of utilities such as electricity.[2]

3. INCREASING THE CLOUD SECURITY

Public and private cloud services, also known as multi-tenant infrastructure, are used increasingly in the enterprise and by government agencies. With their popularity come security issues that are now high priority. A number of TCG technologies and standards, including the Trusted Platform Module (TPM), network security, and self-encrypting drives can be used to provide security for systems, networks, and data. TCG also is addressing how to interface various technical standards to create an end-to-end enterprise solution that is tailored to meet mission and business needs and comply with security policies within public and private cloud networks. TPM (Trusted Platform Module) is a computer chip (microcontroller) that can securely store artifacts used to authenticate the platform (your PC or laptop). These artifacts can include passwords, certificates, or encryption keys. A TPM can also be used to store platform measurements that help ensure that the platform remains trustworthy. Authentication (ensuring that the platform can prove that it is what it claims to be) and

attestation (a process helping to prove that a platform is trustworthy and has not been breached) are necessary steps to ensure safer computing in all environments[3].

4.TRUSTED ARCHITECTURE OF CLOUD.

For the vast majority of cloud storage, the security and privacy options provided are perfectly acceptable. The fact is that most people just don't care about privacy. For those of us that do, however, there is a relatively easy solution that can allow you to continue using cloud storage and keep your data secure, Using Trusted Cloud; you can create encrypted folders within your cloud storage, which gets synched like any other file from the Trusted Cloud. You probably have data stored in multiple clouds - Sales force, Box.net, Gmail, Amazon, and many others. Trusted Cloud provides you with the ability to create a unified data protection policy across all clouds. As an in-line security gateway that sits between your users and your cloud applications, Trusted Cloud applies encryption on the fly before sensitive data leaves the enterprise. By applying encryption in a cloud security gateway, Cipher Cloud eliminates the inherent security and privacy risks of cloud computing. Your business never loses control of its sensitive data, yet you can achieve the full benefits of cloud computing. Mostly data stored in cloud are not in protected format. There is a big concern of security in cloud storage. The Trusted Gateway provides a way to encrypt sensitive information to the enterprises as it moves to any cloud application and then decrypt it again as data is delivered to end users. This protects the data from being accessed by others. This revolutionary technology maintains the cloud application user experience, with near zero latency, and without making any changes to the cloud application itself. Trusted Gateway takes a revolutionary approach to protecting sensitive data before it leaves an organization's secure enterprise network. As illustrated in the fig. 3 the Trusted Gateway examines all outgoing cloud requests, in real time, to identify sensitive data, encrypt that data using TPM, and then forward the modified request to the cloud application. Similarly, encrypted data returning from the cloud application is converted, again in real time, into clear text prior to being displayed to the end user.

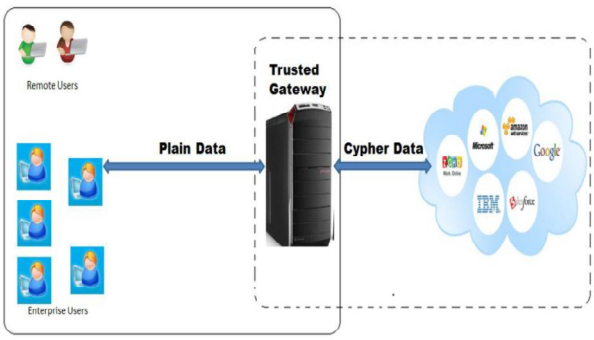

Fig: Trusted Cloud Storage Architecture

There also may be possible that in the internal network some intruder gain access pretend to be another genuine user. So it is necessary to authenticate the user to retain security. For authenticate the users we use the famous Kerberos authentication service [2]. The entities of the authentication service are as follows:

4.1. End User (U): User, who aims to stores encrypted credentials to the cloud storage. So to encrypt data user should authenticate itself to the Trusted Gateway.

4.2. Remote User: Remote User, who access the cloud storage outside the internal enterprise network.

4.3. Trusted Gateway (TG): Trusted gateway is the work station having TPM which maintains the data to be encrypted comes from end users and encrypt them and store to the cloud storage and vice versa.

4.4.AuthenticationServer (AS): Authentication Server verifies user's access right in database; create ticket granting ticket and session key.

4.5.Ticket Granting Server (TGS): Ticket Granting Server issues ticket to request the Trusted Gateway.

4.6. Database: The Kerberos service must have a database to store user id (ID) and hashed passwords.[4]

5.CONCLUSION

Cloud Computing is an emerging commercial infrastructure paradigm that promises to eliminate the need for maintaining expensive computing hardware. As market grows the threat on data also grows. In this paper we have proposed a model which helps to use trusted platform module widely for the security of cloud storage. We have design a new trust model which uses TPM store encrypted data to the cloud, which is unprofitable to the other users. The data will be safe in the public cloud also. Kerberos is the secure method to authenticating requests for any service, is used to authenticate users to the trusted gateway. In TPM access to keys, data or systems is often protected and requires authentication by presenting a password.[5]

6. REFERENCES

1. K. Valli Madhavi, R. Tamilkodi and R. Bala Dinakar, "Data Storage Security in Cloud Computing for Ensuring Effective and Flexible Distributed System," International Journal of Electronics Communication and Computer Engineering, Vol 3.

2. Mehdi Hojabr, "Ensuring data storage security in cloud computing with effect of kerberos," International Journal of Engineering Research & Technology (IJERT),ISSN-2278-0181, Vol. 1.

3. Qian Wang and Cong Wang and KuiRen, Wenjing Lou, Jin Li "Enabling Public Auditability And Data Dynamics For Storage Security in Cloud Computing" in IEEE transactions on parallel and distributed systems, vol. 22.

4. Nashaat el-Khameesy and Hossam Abdel Rahman, "A Proposed Model for Enhancing Data Storage Security in Cloud Computing Systems," Journal of Emerging Trends in Computing and Information Sciences, ISSN 2079-8407, Vol. 3

5. Ravi Kant Sahu and Abhishek Mohta, L.K. Awasthi "Robust Data Integration While Using Third Party Auditor For Cloud Data Storage Services", conf. IJARCSSE, Volume 2.