INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH & DEVELOPMENT

ISSN 2278 – 0211 (Online)

RSA Public Key Cryptography for Data Protection in Cloud Computing Environments

Vinod Kumar
M.Tech. (C.S.E.) Student, Panchkula Engineering College, Mouli, Panchkula, India
Lalita Devi
M.Tech. (C.S.E.) Student, Panchkula Engineering College, Mouli, Panchkula, India

Abstract:
The name Cloud computing was inspired by the Cloud symbol that's often used to represent the Internet in flow charts and diagrams. The term cloud computing is sometimes used to refer to a new paradigm – some authors even speak of a new technology – that offers IT resources and services over the Internet. The technology analysts at Gartner see cloud computing as a so-called "emerging technology "on its way to the hype[7].When looking at the number of searches for the word pair "cloud computing" undertaken with the Google search engine one can get a feeling of the high interest on the topic. Even terms like "outsourcing", "Software-as-a-Service (SaaS)" or "grid computing" have already been overtaken.
Cloud Computing is becoming a well-known buzzword nowadays. In simple terms Cloud computing is where software applications, processing power, data and potentially even artificial intelligence are accessed over the Internet. Many private individuals now regularly use an online e-mail application such as Gmail, Yahoo Mail or Hotmail. Exchanging messages and sharing photos and video on social networking sites like Face book is now also very common. However, these types of cloud computing activities are just the beginning.

Key words: *Software-as-a-Service (SaaS), Grid computing, Pay-as-you-go, Platform-as-a-Service (PaaS) ,Infrastructure as-a-Service (IaaS) , ERP (Enterprise Resource Planning), application programming interfaces (API), Cloud Security Alliance (CSA) , Common Language Runtime (CLR)*

1. Introduction

The new criterion for service provisions in the Cloud Computing era involves three roles , which are called cloud computing system infrastructure provider (or cloud provider in short), service provider/cloud consumer, and service consumer individually.

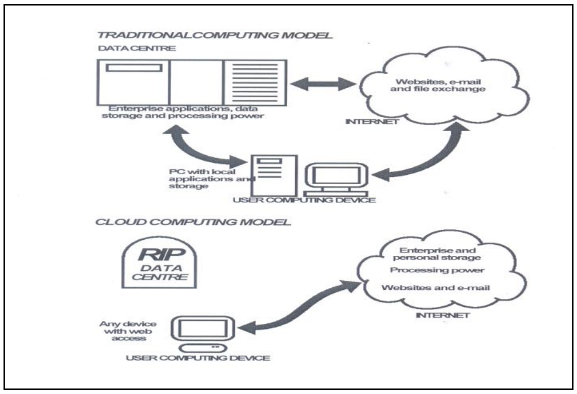
TRADITIONALCOMPUTING MODEL
DATA CENTRE
Enterprise applications, data storage and processing power
Websites, e-mail and file exchange
INTERNET
PC with local applications and storage
USER COMPUTING DEVICE
CLOUD COMPUTING MODEL
RIP
DATA CENTRE
Enterprise and personal storage
Processing power
Websites and e-mail
INTERNET
Any device with web access
USER COMPUTING DEVICE

Figure 1

Cloud computing refers to both the applications delivered as services over the Internet and the hardware and software in the datacenters that provide those services. It is a new computing model where the large computing was run in the various computing resource on network. Based on user requirements, it can dynamically allocate, deploy, redeploy and cancel the cloud services. The aim is to make the "computing power" as the water and electricity to supply for user which allows them to obtain a wide range of functional capabilities on a 'pay-as-you-go' basis. In cloud computing, all of resource on internet is formed a cloud resource pool, then these resource is dynamically allocated to different applications and services. Virtualization technology allows multiple operation systems and applications can be run on a shared computer. Sharing resource makes the hardware performance be used more efficient and provides economic benefits for users to reduce the capital cost and additional expenditure.

2. Service/Delivery Models

There are three common service models for offering cloud computing services. These models are Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) and Infrastructure as-a-Service (IaaS).

3. Characteristics of SaaS

- Web access to commercial software.
- Software is managed from a central location.
- Software delivered in a "one to many" model.
- Users not required handling software upgrades and patches.
- Application Programming Interfaces (APIs) allow for integration between different pieces of software.

4. Characteristics of IaaS

IaaS is generally accepted to comply with the following:

- Resources are distributed as a service
- Allows for dynamic scaling
- Has a variable cost, utility pricing model
- Generally includes multiple users on a single piece of hardware

5. Characteristics of PaaS

- Services to develop, test, deploy, host and maintain applications in the same integrated development environment. All the varying services needed to fulfill the application development process.
- Web based user interface creation tools help to create, modify, test and deploy different UI scenarios.

6. Cloud Computing Security

Wikipedia defines Cloud Computing Security as "Cloud computing security (sometimes referred to simply as "cloud security") is an evolving sub-domain of computer security, network security, and, more broadly, information security. It refers to a broad set of policies, technologies, and controls deployed to protect data, applications, and the associated infrastructure of cloud computing." Note that cloud computing security referred to here is not cloud-based security software products such as cloud-based anti-virus, anti-spam, anti-DDoS, and so on.

The vulnerabilities and threats that cloud computing need to address among others are as follows [13]

- Poor authentication, authorization and accounting system.
- User provisioning and de-provisioning; the ability of customer to control the process.
- Remote access to management interface.
- Hypervisor vulnerabilities such as virtual machine based root kit.
- Lack or weak key encryption.
- Lack of standard technologies and solutions.
- Poor key management procedures.
- Inaccurate modeling of resource allocation.
- Mis-configuration.
- Lack of control in vulnerability assessment process.
- Possibility of internal network probing in the cloud.
- Service level agreements with excessive business risks, conflicting promises to stakeholders.
- Possibility of co-residency checks occurring.
- Lack of audit or certification on part of cloud service provider.
- Lack of forensic readiness, sanitization of sensitive data.

Alliance has identified what it calls the top threats to cloud as follows:

- Abuse and nefarious use of cloud computing.
- Insecure interfaces and application programming interfaces (API).
- Malicious insider.
- Shared technology issues.

- Data loss or leakage
- Account or service hijacking.
- Unknown risk profile.
- Though the threats identified are representative of all the possible threats that can occur in the cloud, nevertheless they portray the necessity of security to appeal to the feelings of the clients. This is because without security addressing the reality of these risks and providing for mitigation plans, clients trust for cloud services will be hard to build.

7. Data Security in Cloud

Many new companies often lack the protection measures to weather off an attack on their servers due to the shortage of resources poor programming that explores software vulnerabilities (PHP, JavaScript, etc) .

8. Critical Areas for Cloud Computing

The Cloud Security Alliance (CSA) has developed a 76-page security guide (Security Guidance for Critical Areas of focus in Cloud Computing) that identifies many areas for concern in cloud computing. This environment is a new model which cannot be well protected by traditional "perimeter" security approaches. From this document six specific areas of the cloud computing environment where equipment and software implementing TCG specifications can provide substantial security.

9. Components

The proposed system has following components:

9.1. Remote Access

The Cloud, by nature, is inherently a `public place'. Services are exposed over HTTP, a public medium. Access to these services need to be controlled and access kept to authorized personnel. Moreover as the data is held remotely, trust needs to be established with the service and with the security provided by the service over the data itself. Access to the data needs to be regulated.

9.2. Data Integrity

Data integrity is one of the issues that we consider during the development phase of our secured application. The task is to make files secure by completely denying unauthorized access to the files while at the same time make sure that the files should not be modified only by the authors. It can only be modified by the cloud server administrator.

9.3. User Authentication and Authorization

The secure application is certainly required to employ a strong mechanism to authenticate the users. The most frequently used strategy is asking for a user name and password to authenticate he user. Some key points that we should consider in the design of authentication mechanism are: transmitting the password in clear (i.e., we may use SSL to protect the user privacy and to safe the application by being played in the hand of some intruder after he capture the network traffic and thus get the password). Also, it is required that the secure application provides secure storage of the user names and passwords along with a method to manage them, including resetting or revoking the passwords or user accounts. Our another important concern during the preliminary design of secure application is whether to store the password in some hash format or storing it in the plain text format as the user entered

9.4. Centralized Approach

Resources and data security are controlled by the cloud sever administrator. Only Administrator should have the authority for uploading files and key generation. Clients can't be able to download file without admin permission. It offers more security then decentralized system because all the processing is controlled in a central location.

10. Principal Design Features

- Interoperability
- Common Runtime Engine
- Language Independence
- Base Class Library
- Simplified Deployment
- Security
- Portability

11. Advantages of the System

- Security & Backup
- Easily accessible
- Quality of Service

12. Results

The encryption and decryption time is measured while uploading and downloading.

13. Conclusion

As stated above data protection is a critical issue in cloud computing environments. Clouds have no borders and the data can be physically located anywhere in the world. So this phenomenon raises serious issues regarding user authentication and data confidentiality. Hence this study proposed service cloud architecture. One of the major objectives of the targeted secure application is to provide secure storage at the server as maintaining authorized access to the documents for the authorized users. Another important concern is to maintain integrity of customer i.e. correctness of his data in the cloud. The security system addressed following minimum key security-elements: User authentication and Authorization, Data encryption and decryption, Data integrity.

14. References

1. Aderemi A. Atayero , Oluwaseyi Feyisetan,” Security Issues in Cloud Computing: The Potentials of Homomorphic Encryption”, Journal of Emerging Trends in Computing and Information Sciences, VOL. 2, NO. 10, October 2011
2. Brantner, M., D. Florescu,” Building a database on S3”. ,ACM SIGMOD international conference on Management of data.2008
3. Brunette, G., & Mogull, R.”Security guidance for critical areas of focus in cloud computing”
4. Cloud Security Alliance “Top Threats to Cloud Computing” Version 1.0 (2010)
5. Cloud Security Alliance” Security Guidance for Critical Areas of Focus in Cloud Computing” version 2.1 (2009)
6. Cong Wang, Qian Wang, Kui Ren, and Wenjing Lou, "Ensuring Data Storage Security in Cloud Computing", The 17th IEEE International Workshop on Quality of Service (IWQoS'09), Charleston, South Carolina, July 13-15, 2009
7. Fenn, Jackie, Nikos Drakos, Whit Andrews, “Hype Cycle for Emerging Technologies”, edited by Gartner: Gartner
8. Frank Gens “Enterprise IT in the Cloud Computing Era”, IDC's QuickLook Survey, IDC's Enterprise Panel 2008
9. Gilliam, D. P,”Managing information technology security risk. Software Security Theories and Systems”, 3233, 296-317. doi: 10.1007/978-3-540-37621-7_16
10. Greene, S. S. “Security policies and procedures: Principles and practices”, Upper Saddle River, N.J.: Pearson Prentice Hall
11. Habib, S. M., Ries, S., & Muhlhauser, M.”Cloud computing landscape and research challenges regarding trust and reputation”, Ubiquitous Intelligence & Computing and 7th International Conference on Autonomic & Trusted Computing, Oct 2010
12. Hewitt, C. (2008). "ORGsfor scalable, robust, privacy-friendly client cloud computing." IEEE Internet Computing 12(5): 96-99.
13. Hogben, G. and Catteddu, D. “Cloud Computing: benefits, risks and recommendations for information security”, Technical Report,European Network and Information Security Agency.
14. Hongwei Li, Yuanshun Dai1, Ling Tian, and Haomiao Yang “Identity-Based Authentication for Cloud Computing” in Springer-Verlag Berlin Heidelberg 2009.
15. H. Rhee, J. Park, W. Susulo, and D. Lee, “Trapdoor security in a searchable public-key encryption scheme with a designated tester,” Journal of Systems and Software, vol. 83, no. 5, pp. 766–771, May 2010