Cloud Computing Based Services

Dimple patil, Madhuri Walse, Jagruti Warkhede, Priya Gawande

Under Guidance of Prof. L.J.Sankpal

Department of Computer Engineering Sinhgad Academy of Engineering, Pune

Email: madhuwalse1992@gmail.com dimpal.patil26@gmail.com warkhede.jagruti@gmail.com priyagawande@gmail.com

Abstract - The cloud is a next generation platform that provides dynamic resource pools, virtualization, and high availability. Today, we have the ability to utilize scalable, distributed computing environments within the confines of the Internet, a practice known as cloud computing. The project is designed to eliminating the need to install and run the software on the customer's own computers and simplifying maintenance and support. In this project we shall provide access to Cryptography services to user on demand through Internet as cloud. The prevalent Problem associated with cloud computing is the cloud security and the appropriate Implementation of Cloud over the Network. In this Research Paper, we have tried to assess Cloud Storage Methodology and Data Security in cloud by the Implementation of digital signature with RSA algorithm.

Keywords - Internet, impaired people, web browser, services

INTRODUCTION

Cloud computing is the Internet based development and is used in computer technology. It has become an IT buzzword for the past a few years. Cloud computing has been often used with synonymous terms such as software as a service (SaaS), grid computing, cluster computing, autonomic computing, and utility computing. SaaS is only a special form of services that cloud computing provides. Grid computing and cluster computing are two types of underlying computer technologies for the development of cloud computing. It is often difficult to define the cloud computing. Computing is a virtual pool of computing resources. It provides computing resources in the pool for users through internet. It provides a mandatory application programming environment. It can deploy, allocate or reallocate computing resource dynamically and monitor the usage of resources at all times Cloud computing collects all the computing resources and
manages them automatically through software. In the process of data analysis, it integrates the history data and present data to make the collected information more accurate and provide more intelligent service for users and enterprises. The users need not care how to buy servers, software solutions and so on. Users can buy the computing resource through internet according to their own needs.

**MOTIVATION**

In this model, cloud providers install and operate application software in the cloud and cloud users access the software from cloud clients. The cloud users do not manage the cloud infrastructure and platform on which the application is running. This eliminates the need to install and run the application on the cloud user's own computers simplifying maintenance and support. What makes a cloud application different from other applications is its elasticity. This can be achieved by cloning tasks onto multiple virtual machines at run-time to meet the changing work demand. Load balancers distribute the work over the set of virtual machines.

**MODULES OF THE SYSTEM**

The proposed system i.e., Software has following modules:

1. Register user (Assume user have valid Gmail id)
2. Login user
3. User profile : users basic details with his public key(if he had)
4. Mail alerts
5. User Role – a. Admin (Required to activate/deactivate registered user)
   b. User who is going to use above services

**PROJECT WORK**

How does it work?

After installing the application you need to create an account and fill up the details. After registration server will accept your request and make activation of user account. After verification user can access the services using public and private key which is provided by server.

**PROJECT PLAN**

The project plan for proposed system i.e., Software gives step by step flow of the system implementation plan. It includes the requirements gathering and analysis, design of project, GUI development, coding, testing, modification and deployment phases.
The above figure depicts the project plan. It describes the activity plan of the project. The activities will be carried out in the same order.

We are implementing the proposed system on the basis of object oriented concepts. It means dividing whole system into different modules.

**SYSTEM REQUIREMENTS**
This application is directed to two user profiles, the client and the server to be tracked. The server side requires availability of internet connection. The client side requires valid email id and internet connection. If there is any error in sending the message from the operator, there won’t be any message sends to the operator by the application, instead no action takes place at the server side.

**APPLICATION FEATURES**

Encryption Decryption techniques:
In cloud computing, it is frequent for the entities to communicate manually. To achieve the security in the communication, it is important to impose an encryption and signature schemes. Therefore, the following encryption techniques are proposed:

IBE is a form of public key cryptography in which a third party server uses a simple identifier, such as an e-mail address, to generate a public key that can be used for encrypting and decrypting electronic messages.
Compared with typical public key cryptography, this greatly reduces the complexity of the encryption process for both users and administrators. An added advantage is that a message recipient doesn’t need advance preparation or specialized software to read the communication.

Digital signature

A digital signature scheme typically consists of three algorithms:

- A key generation algorithm that selects a private key uniformly at random from a set of possible private keys. The algorithm outputs the private key and a corresponding public key.
- A signing algorithm that, given a message and a private key, produces a signature.
- A signature verifying algorithm that, given a message, public key and a signature, either accepts or rejects the message's claim to authenticity.

Two main properties are required. First, a signature generated from a fixed message and fixed private key should verify the authenticity of that message by using the corresponding public key. Secondly, it should be computationally infeasible to generate a valid signature for a party who does not possess the private key.

CONCLUSION

In this paper, we investigated the problem of data security in cloud data storage, which is essentially a distributed storage system. To ensure the correctness of users’ data in cloud data storage, we proposed an effective and flexible distributed scheme with explicit dynamic data support.

The purpose of a digital signature is the same as your handwritten signature. Instead of using pen and paper, a digital signature uses digital keys (public-key cryptology). Like the pen and paper method, a digital signature attaches the identity of the signer to the document and records a binding commitment to the document. Unlike a handwritten signature, it is considered impossible to forge a digital signature the way a written signature might be. Digital signatures cryptographically bind an electronic identity to an electronic document thus making the document authorized.

ACKNOWLEDGEMENT

The authors would like to thank Department of Computer Engineering and indebted to our guide Prof. L.J. Sankpal for her guidance and sagacity without which this IEEEpaper would not have been designed. She provided us with valuable advice which helped us to accomplish the design of IEEE paper. We are also thankful to our HOD Prof. B. B. Gite (Department of Computer Engineering) for his constant encouragement and moral support.

Also we would like to appreciate the support and encouragement of our colleagues who helped us in correcting our mistakes and proceeding further to produce the paper with the required standards.
REFERENCES


[5] Java Speech API By Jarkko Enden, Department of Computer Science, University of Helsinki, Finland.


