International Journal of Communication and Computer Technologies
Volume 01 – No.12, Issue: 03 January 2013
ISSN NUMBER : 2278-9723

Using encryption Algorithms to enhance the Data Security in Cloud Computing

MANDEEP KAUR[#1], MANISH MAHAJAN[#2]

Department of Information and Technology
Chandigarh Engineering College, Landran
Mohali, India

Abstract Cloud computing is the concept implemented to decipher the Daily Computing Problems. Cloud computing is basically virtual pool of resources and it provides these resources to users via internet. Cloud computing is the internet based development and used in computer technology. The prevalent problem associated with cloud computing is data privacy, security, anonymity and reliability etc. But the most important between them is security and how cloud provider assures it. In this research paper, the proposed work plan is to eliminate the concerns regarding data privacy using encryption algorithms to enhance the security in cloud as per different perspective of cloud customers.

Keywords: Cloud Computing, Algorithms: AES, DSA, Blowfish and RSA, cipher cloud, Eclipse IDE.

1. Introduction

Cloud computing is the concept of using remote services through a network using various resources. It is basically meant to give maximum with the minimum resources i.e. the user end is having the minimum hardware requirement but is using the maximum capability of computing. This is possible only through this technology which requires and utilizes its resources in the best way.

In the cloud, the end user is just using a very light device which is capable of using a network that connects it to a server at some other location. The users do not need to store the data at its end as all the data is stored on the remote server at some other place.

The concept of cloud computing is linked closely with those of IaaS (Infrastructure as a Service); PaaS (Platform as a Service), SaaS (Software as a Service) and collectively *aaS (Everything as a Service) all of which means a service-oriented architecture. Here comes the first benefit of the cloud computing i.e. it reduces cost of hardware that could have been used at user end. As there is no need to store data at user's end because it is already at some other location. So instead of buying the whole infrastructure required to run the processes and save bulk of data you are just renting the assets according to your requirement. The similar idea is behind all cloud networks.

They maintain database and applications for the user(s) at some remote server and provide independence of accessing them from any place through a network.

Cloud computing can deploy, allocate or reallocate computing resources dynamically and monitor the usage of resources at all times. Cloud service providers are incentivized by the profits to be made by charging consumers for accessing these services.

Clouds are of particular commercial interest not only with the growing tendency to outsource IT so as to reduce management overhead and to extend existing, limited IT infrastructures, but even more importantly, they reduce the entrance barrier for new service providers to offer their respective capabilities to a wide market with a minimum of entry costs and infrastructure requirements – in fact, the special capabilities of cloud infrastructures allow providers to experiment with novel service types at the same time reducing the risk of wasting resources. Cloud is not only simple collecting the computer resource, but also provides a management mechanism and can provide services for millions of users simultaneously.

Cloud computing is the broader concept of infrastructure convergence. This type of data centre environment allows enterprises to get their applications up and running faster, with easier manageability and less maintenance to meet business demands. For example-

The smart phones we are seeing in the world today use their internal memory likewise the phones coming nowadays are having their storage capacities like 16gb to 32gb, etc. so it is seen that the memory is required on each mobile phone device to save applications and files of its users and it is also seen that main cost for a mobile phone (especially the smart phones) is of memory storage like- if you buy a phone with memory space of 16gb in 200 US dollars then the same phone (same model) with 32gb internal memory will cost you approximately 300 US dollars which mean you are paying more 100 dollars for some more 16 GB memory i.e. 50% more cost for the device

just for memory space. So instead if you use cloud computing here which means the device with you will be just for communication or interaction between you and the server and all your apps and data is stored at some other location i.e. at server, so you do not require any memory space at your end. This saves your pocket from spending some extra money on getting some extra memory space on your phone; secondly you will be having the option to increase that space on the server by renting it which gives you freedom to use nearly unlimited space to store your data. This also gives the security to your data and applications incase you lost or damage your device, your data will remain safe.

2. Types of Clouds

There are basically four types of clouds, which are described below-

- **Public cloud:** This is the one of the cloud in which cloud services are being available to users via a service provider over the Internet. It provides a control mechanism for them. The services may be free or offered on a pay-per-usage model.
- **Private Cloud:** This provides many of the benefits of public, but the main difference among two is that the data is managed properly within the organization only, without the limits of network bandwidth.
- **Community Cloud:** This type of cloud is basically managed by group of originations that have a common objective to achieve. The members share access to the data in the cloud.
- **Hybrid Cloud:** This is the combination of public as well as private cloud. It can also be defined as multiple cloud systems that are connected in a way that allows programs and data to be moved easily from one system to another.

3.Characteristics of Cloud Computing

There are several characteristics of cloud computing, which are described below-

- **Virtualization:** Through Cloud computing, user is able to get service anywhere through any kind of terminal. User can attain or share it safely anytime.
- **High Reliability:** Cloud uses data fault tolerant to ensure the high reliability of the service.
- **Versatility:** Cloud computing can produce various applications supported by cloud, and one cloud can support different applications running it at the same time.
- **On Demand Service:** Cloud is a large resource pool that a user can buy according to his/her need; cloud is just like running water, and gas that can be charged by the amount that user used.
- **Extremely Inexpensive:** The centered management of cloud make the enterprise needn't undertake the management cost of data center that increase very fast. The versatility can increase the utilization rate of the available resources compared with traditional system, so users can fully take advantage of low cost. Some advantages are listed below-
  - Cloud computing do not need high quality equipment for user and it is easy to use.
  - Cloud computing can realize data sharing between different equipments.
  - Cloud computing provides dependable and secure data storage center. You don't worry the problems such as data loss or virus.

4. Background Study

Cloud computing is basically broken down into three segments: "application" "storage" and "connectivity." Each segment serves a different purpose and offers different products for businesses around the world. The services themselves have long been referred to as Software as a Service (SaaS) [1]. There is an increasingly perceived vision that computing will one day be the 5th utility (after water, electricity, telephony). To deliver this vision, architecture was made for creating cloud [2].

Cloud Computing is associated with a new paradigm for the provision of computing infrastructure. This paradigm shifts the location of this infrastructure to the network to reduce the costs associated with the management of hardware and software resources [4].

Cloud computing provides computation, software, data access and storage resources without requiring cloud to know the location and other details of the computing infrastructure. End-users access cloud based applications through a web browser or a light weight desktop or mobile application while the business

software and data are stored on servers at a remote location [6].

Cloud computing is the concept implemented to decipher the Daily Computing Problems, likes of Hardware, Software and Resource Availability unhurried by Computer users. The cloud Computing provides an undemanding and non ineffectual Solution for Daily Computing. The prevalent Problem associated with Cloud Computing is the Cloud security and the appropriate Implementation of Cloud over the Network and how digital signature is implemented using RSA algorithm[7].

Among the many IT giants driven by trends in cloud computing has not doubtful. It gives .almost everyone has brought good news. For enterprises, cloud computing is worthy of consideration and try to build business systems as a way for businesses in this way can undoubtedly bring about lower costs, higher profits and more choice; for large scale industry, After the financial turmoil will be the cost of infrastructure for large-scale compression seems likely; developers, when in the face of cloud computing, through the PaaS model can effectively improve their own capacity, Therefore, the impact of cloud computing on the ISV is the largest of the many roles; for engineers and developers are concerned. There is the advent of cloud computing is bound to birth a number of new jobs. The clouds will grow in size as soon as available bandwidth and the corresponding service model mature enough, cloud computing will bring a revolutionary change in the Internet. Cloud computing announced a low-cost supercomputing services to provide the possibility, while there are a large number of manufacturers behind, there is no doubt that cloud computing has a bright future[7].

5. Problem Formulation

In Cloud computing technology there are a set of important policy issues, which include issues of privacy, security, anonymity, telecommunications capacity, government surveillance, reliability among others. But the most important between them is security and how cloud provider assures it. Generally, Cloud computing has several customers such as ordinary users, academia, and enterprises who have different motivation to move to cloud. If cloud clients are academia, security effect is on performance of computing and for them cloud provides a way to combine security and performance. For enterprises the most important problem is also security but with different vision. For them high performance may be not as critical as academia. So, as per the perspective of different users, the security point of view is different.

6. Proposed Work Plan

To access a cloud based web application that will try to eliminate the concerns regarding data privacy, segregation.

We proposed different encryption algorithms like - AES, DES, RSA and Blowfish to ensure the security of data in cloud. For the perspective of different users, we proposed these algorithms. DES is developed in early 1970s; Blowfish is developed by Bruce Schneier, in 1993. AES is developed by NIST in 2001.All of these algorithms are symmetric key, in which a single key is used for encryption/decryption purposes. RSA is asymmetric key algorithm, created by Ron Rivest, Adi Shamir and Lenard Adleman in 1978. This algorithm is used for public key cryptography. In this, two public/private keys are used for encryption/decryption.

The key-size of algorithms is different. Like- Key size of Blowfish algorithm is 128-448 bits and AES algorithm is 128,192,256 bits. The key length of AES is less than Blowfish. 2048 bits of asymmetric key is equivalent to 112 bits of symmetric key.

The research will be conducted using Java runtime of Google App Engine, i.e. JDK 1.6. Eclipse IDE.Google App Engine SDK 1.6.0 or higher. Below are the steps for proposed work plan-

6.1. Steps for Proposed Work plan

- User should not require any third party software/program to encrypt data on the client side.
- Every bit of data read/written to/from the cloud database must go through an encryption framework.
- User must be authorized using passwords, to access the data saved on Cipher Cloud.
- Encryption keys used must be generated instantly and should never be stored on cloud storage framework in any form.
- Give the user a choice to select the encryption algorithm they wish to use.
- Provide an efficient mechanism of encryption over the cloud.

7. Report Analysis

During the literature review, three concepts were distilled that were related to the cloud computing paradigm in the form of dimensions. These dimensions relate to *how* data *is used*, *where* data *is located* in relation to the data owner, and *how* data *is protected*. Cipher Cloud encrypts the data, making its ownership

exclusive to its owner and makes it independent from the facts of where the data might be stored or who manages it. Even in cases of take over and change of ownership, only the user will be able to decrypt the given data. Additionally the data is kept safe during transit using HTTPS TLS 1.0 standard making it difficult for anyone to sniff the data.

8. Future Work plan

As discussed, cloud computing is a very promising deployment model that can cope with the security limitations occurring in a public cloud environment, while still being able to support many of the economic advantages of public cloud computing.

Further using these encryption algorithms, two public/private keys are used for encryption/decryption. We provide the options to the users to choose any algorithm according to him/her need and accordingly encrypt/decrypt the data on cloud. For this further, we need Google plug-ins for eclipse for creating, debugging and testing the application. An interface can be provided to the users to select the various encryption algorithms as per their own choice. And, the further steps can be followed-

Step1. User log into Cipher cloud and then he/ she will be getting choices of encryption algorithms.
Step2. Then, after selecting any algorithm as per user's choice, he/ she will be able to encrypt the particular data which he/she wants to.
Step3. After selecting algorithm, user will be getting options to upload the files and encrypt it accordingly.

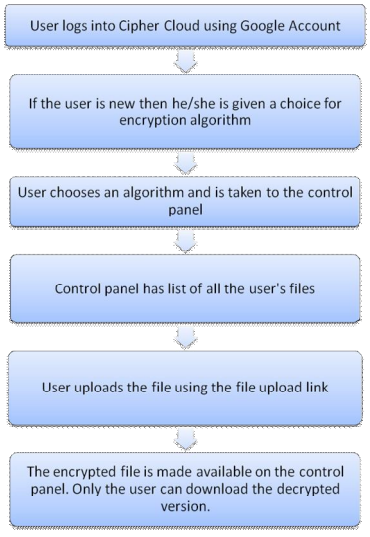

Figure 8.1. Flow of Cipher cloud from a user's perspective

Step4. After sending request to server, server generates the symmetric key and decrypts the request and again encrypts it with RSA and transmits the file to user.

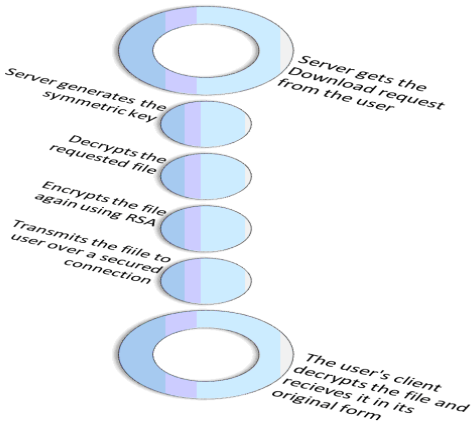

Figure 8.2. Framework flow of download request

References

[1] Armbrust, Fox, Griffith, Joseph, "*Above the clouds: A Berkeley view of cloud computing*"[2009].
[2] Buyya, Venugo, "*Cloud Computing and emerging IT platforms: Vision, hype, and reality for delivering Computing as the 5th Utility*", [2008].
[3] Caceres, Lindner, Vaquero, "*A break in the clouds: towards a cloud definition*", [2008].
[4] Keahey, Fortes, Freeman, "*Science Clouds:Early Experiences in Cloud Computing for scientific applications*" [2008].
[5] Moretti, Thain, Flynn, "*All-pairs: An abstraction for data inexpensive cloud computing*", [2008].
[6] Nurmi, Woloski, Obertelli, "*The Eucalyptus Open-source Cloud computing*" [2009].
[7] Uma Somani, Kanika Lakhani, Manish Mundra **, "***Implementing digital signature with RSA Encryption Algorithm to enhance the data security of cloud in Cloud Computing*" [2010].
[8] YouSeff, Butrico, Da Silva "*Toward a Unified Ontology of cloud computing*" [2009].

[9]http://en.wikipedia.org/wiki/Cloud_computing

[10]http://aws.typepad.com/aws/2008/07/white-paper-on.html

[11]https://cloudsecurityalliance.org/

[12]http://www.mytestbox.com/miscellaneous/cloud-computing-grid-computing-utility-computing-list-top-providers/