ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology
Volume 1, Issue 4, June 2012

Secure Data Storage in the Cloud using Digital Signature Mechanism

Shobha Rajak, Ashok Verma

***Abstract*— Cloud computing services need to address the security during the transmission of sensitive data and critical applications to shared and public cloud environments. The cloud environments are scaling large for data processing and storage needs. Cloud computing environment have various advantages as well as disadvantages on the data security of service consumers. In Cloud computing environment data protection as the most important security issue. In this issue, it concerns Include the way in which data is accessed and stored, audit requirements, compliance, and notification Requirements, issues involving the cost of data breach, and damage to brand value. In the cloud storage infrastructure, regulated and sensitive data needs to be properly segregated. It is very new Concept which is use for Data securing with the Help of Digital Signature in the cloud computing. In the service provider's data center, protecting data privacy and managing compliance are critical by using encrypting and managing encryption keys of data in transfer to the cloud.In this Research Paper, we have tried to assess Cloud Storage Methodology and Data Security in cloud by the Implementation of digital signature with CFX_MF algorithm.**

Index Terms— **Cloud computing, Data security, Internet, Key, cloud server, digital signature and encryption.**

INTRODUCTION

Cloud computing is a very important computing epitome in which services to assign to a Network connection, software & also services using over a network. This network of servers &connections is collectively known as "the cloud".[2] SaaS stands for Software as a service(SaaS), sometimes it is called "on-demand software "because is a used by need to customer according to their responsibility.[3] Like an iphone, Blackberry or Laptop they are using service by thin client or other access point .[2]By users using a thin client, normally using a web browser over the Internet.[3]By releasing the need to install & run the application of cloud on the customer's own computer.[4] Cloud computing is archive its position in the IT Companies. When we adopting cloud technology can be an affordable way to get access to a dynamically scalable, virtual-ized computing environment. Optimal IT hardware, software, expertise and infrastructure management resources that may not otherwise be available from a cost perspective can be rapidly deployed and easily scaled.[1] Processes, applications and services can be available on demand, regard-less of the user location or device. Cloud computing can be contrasted with the traditional desktop computing model, where the resources of a single desktop computer are used to complete tasks, and an expansion of the client/server model. To paraphrase Sun Microsystems, famous adage, in cloud computing the network becomes the supercomputer.[2-4]

In addition to the different cloud computing models, there are distinctions among the most common cloud service models as shown in Figure 1. Available to anyone with Internet access, cloud service models include:[1]

●Software as a Service (SaaS) cloud model—Enables software to be delivered from a host source over a network as opposed to installations or implementations

●Platform as a Service (PaaS) cloud model—Enables operating systems and middleware services to be delivered from a man-aged source over a network

●Infrastructure as a Service (IaaS) cloud model—Enables theentire infrastructure to be delivered as a service over a net-work, including storage, routers, virtual systems, hardware and servers.

In this paper we will focus on the IaaS cloud computing models.

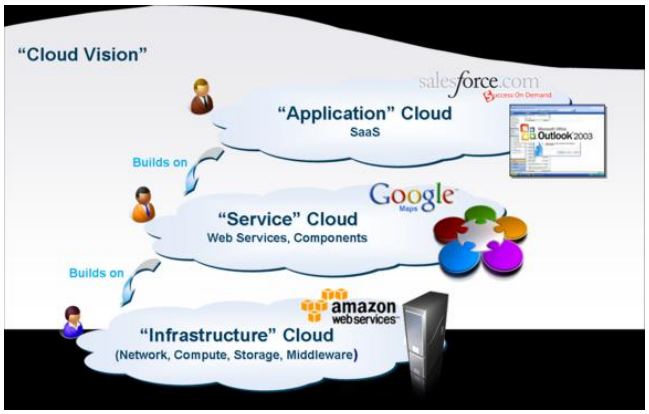
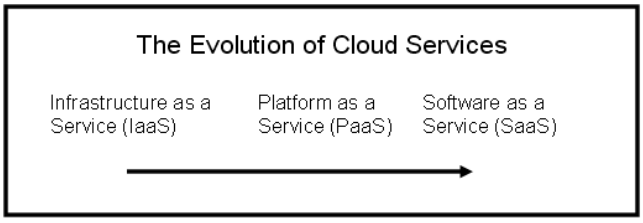


Figure 1. Cloud computing models



Benefits of Cloud Computing

Manuscript received May, 2012.
***Shobha Rajak**, CSE, GGITS Jabalpur (e-mail:Shobha_2808@yahoo.co.in). Jabalpur , India, +919981784920*
***Ashok Verma** , CSE GGITS Jabalpur, India(e-mail: ashokverma@ggits.org).*

According to International Data Corporation (IDC), "The proliferation of devices, compliance, improved systems performance, online commerce and increased replication to secondary or backup sites is contributing to an annual doubling of the amount of information transmitted over the Internet." The cost of dealing with this amount of data is something that companies must address. In today's economy, companies are looking at any cost saving measures, and the bottom line is that cloud computing provides much greater flexibility than previous computing models.[12]In this time Data security is the very main issues in the cloud it is very important that how to secure data in the cloud. Hackers and Malware virus would be attack on data. These are concerns about the security issues.

I. PROBLEM STATEMENT

The problem is that when cloud service providers provide service that time might be hacker hacked username and Password. For Prevent this problem we implement the concept of digital Signature. Digital signatures enable the "authentication" and "non-repudiation" of digital messages, assuring the recipient of a digital message of both the identity of the sender and the integrity of the message.

II. RELATED WORKS

Yuh-Min Tseng a,*, Jinn-Ke Jan b, Hung-Yu Chien b[5]-proposed a digital signature scheme using self-certified public keys in the ISP era. It provides the message recovery property. The authenticated encryption scheme only allows a specified receiver to verify and recover the message. The authenticated encryption scheme with message linkages is suitable for transmission of large message, while providing the linkages among signature blocks.

YANG Xiaoyuan1, ZHU Shuaishuai, PAN Xiaozhong[6]-proposed a new quick data verification scheme (Light PoR), with considering not only the secure public data verification but also the communication and computing costs. Once the verification fails, our scheme can automatically maintain the data availability of CCS clusters at a relatively high level.

Cong Wang et al. [7] stated that data security is a problem in cloud data storage, which is essentially a distributed storage system. And explained their proposed scheme to ensure the correctness of user's data in cloud data storage, an effective and flexible distributed scheme with explicit dynamic data support, including block update, delete, and append relying on erasure correcting code in the file distribution preparation to provide redundancy parity vectors and guarantee the data dependability.

John Harauz et al. [8], described the Security Content automation protocol (SCAP) and benefits it can provide with latest cloud computing paradigm with reference to the latest report released by NIST, giving insight as to what SCAP is trying to do, It states that many tools for system security, such as patch management and vulnerability management software, use proprietary formats, nomenclatures, measurements, terminology, and content. Their example states that, when vulnerability scanners do not use standardized names for vulnerabilities, it might not be clear to security staff whether multiple scanners are referencing the same vulnerabilities in their reports.

Siani Pearson, et al. [9], described the overview of privacy issues within cloud computing and a detailed analysis on privacy threat based on different type of cloud scenario was explained, the level of threat seem to vary according to the application area. Their work has stated the basic guidelines for software engineers when designing cloud services in particular to ensure that privacy are not mitigated.

Meiko Jensen et al. [10], described a selection of issues of Cloud Computing security and the Web Services security frameworks (attacking the Cloud Computing system itself), stating the importance and capabilities of browser security in the Cloud computing context, and sketched the threat of flooding attacks on Cloud systems. Showed, the threats to Cloud Computing security are numerous, and each of them requires an in-depth analysis on their potential impact and relevance to real-world Cloud Computing scenarios.

III . REQUIREMENTS SPECIFICATION

3.1 Hardware Requirements

The system running the application should have following Requirements:
1. Intel I3 Core to dual
2. RAM Size 4GB
3. Processor 64bit Upper limit 7400E

3.2 Software Requirements

The system running the application must have the following:
1. Supporting OS: Windows 2008 Server, Windows XP, Windows7.
2. Java Development Kit - jdk1.6.0_02.
3. Java Runtime Environment - jre1.6.0_06.
4. Web Browser with Java Plug-in installed
5. Wireless connectivity driver.
6. Virtual Machine

3.3 Network Support

This project can be used to run on both Wireless and LAN Networks. It supports following network architectures:
1. Local Area Network (using network cables)
2. Wireless Network (Wi-Fi)
3. Ad-Hoc Network
4. Dial-up or VPN network to a workplace.

3.4 Technology Specific Tools used

In this work we use following tools:
1. Eclipse3.3
2. Tomcat server v_6
3. Java.awt package for layout of the applet.
4. Oracle 10G

IV. IMPLEMENTATION

4.1 Module 1: Study of the System

This proposed system can be mainly divided into two parts:
1.Server
2.Client

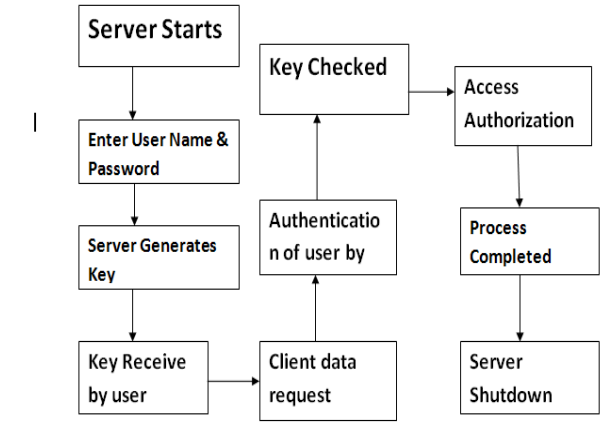


Figure.1 Design Framework – The High Level Design

This project is mainly depended on client/server model. The client requests the server and server responses by granting the clients request. The proposed system should provide both of the above Features along with the followed ones:

a) Server - The server should be able to perform the Following features:
The first and foremost problem is to find the server. We should identify the program in the server which processes the client's request. Authentication of users' generation of keys encryption of data files

b) Client: The client should be able to perform the Following features:
Authenticate itself from server request for keys decrypt data files

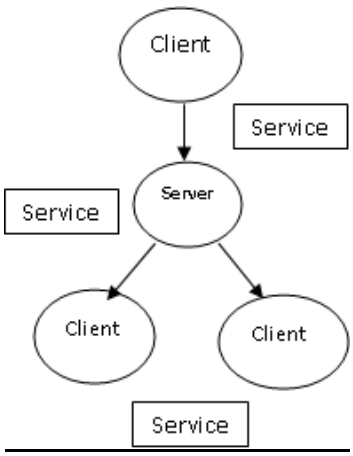


Figure 2:-Context Diagram – The Low level Design

RSA DIGITAL SIGNATURE ALGORITHM

The RSA Digital Signature algorithm is a FIPS approved cryptographic algorithm for digital signature generation and verification.

A PROOF THAT v = r IN THE DSA [4]

This appendix is for informational purposes only and is not required to meet the standard.

The purpose of this appendix is to show that in the DSA, if M′ = M, r′ = r and s′ = s in the signature Verification then v = r′. We need the following easy result.

LEMMA. Let p and q be primes so that q divides p - 1, h a positive integer less than p, and $g = h^{(p-1)/q} \bmod p$. Then $g^q \bmod p = 1$, and if m mod q = n mod q, then $g^m \bmod p = g^n \bmod p$.

Proof: We have

$g^q \bmod p = (h^{(p-1)/q} \bmod p)^q \bmod p$

$= h^{(p-1)} \bmod p$

$= 1$

By Fermat's Little Theorem. Now let m mod q = n mod q, i.e., m = n + kq for some integer k. Then

$g^m \bmod p = g^{n+kq} \bmod p$

$= (g^n g^{kq}) \bmod p$

$= ((g^n \bmod p)(g^q \bmod p)^k) \bmod p$

$= g^n \bmod p$

Since $g^q \bmod p = 1$. ■

We are now ready to prove the main result.

THEOREM. If M′ = M, r′ = r, and s′ = s in the signature verification, then v = r′.

Proof: We have

$w = (s')^{-1} \bmod q = s^{-1} \bmod q$

u1 = ((SHA-1(M′)) w) mod q = ((SHA-1(M))w) mod q

u2 = ((r′)w) mod q = (rw) mod q.

10

Now $y = g^x \bmod p$, so that by the lemma,

$v = ((g^{u1} y^{u2}) \bmod p) \bmod q$

$= ((g^{SHA\text{-}1(M)w} y^{rw}) \bmod p) \bmod q$

$= ((g^{SHA\text{-}1(M)w} g^{xrw}) \bmod p) \bmod q$

$= ((g^{(SHA\text{-}1(M)+xr)w}) \bmod p) \bmod q.$

Also

$s = (k^{-1}(SHA\text{-}1(M) + xr)) \bmod q.$

Hence

$w = (k(SHA\text{-}1(M) + xr)^{-1}) \bmod q$

$(SHA\text{-}1(M) + xr)w \bmod q = k \bmod q.$

Thus by the lemma,

$v = (g^k \bmod p) \bmod q$

$= r$

$= r'$. ■

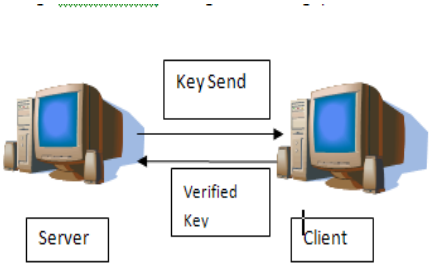


Figure 3:- Key Request and Response Design

Client requests for services to server & server grants the request to a user. Client has to first register himself in the server starts. Server stores the username, password. Then at the time of login client enter username & password then click to submit button & user that time server generate key by using digital algorithm & simulteausly user go to another page where username, password & key three fields are there & key block are also there. Client submits the key then Server

check the key or verified key which key user was entered. Then go through next page & show message that you have successfully login.

ALGORITHM FOR COMPUTING m VALUES OF x [4]

Let x be the signer's private key. The following may be used to generate m values of x:

Step 1. Choose a new, secret value for the seed-key, XKEY.

Step 2. In hexadecimal notation let

t = 67452301 EFCDAB89 98BADCFE 10325476 C3D2E1F0.

This is the initial value for $H_0 \| H_1 \| H_2 \| H_3 \| H_4$ in the SHS.

Step 3. For j = 0 to m - 1 do

15

a. $XSEED_j$ = optional user input.

b. $XVAL = (XKEY + XSEED_j) \bmod 2^b$.

c. $x_j = G(t, XVAL) \bmod q$.

d. $XKEY = (1 + XKEY + x_j) \bmod 2^b$.

1- User: who uses and relay on the verification of the cloud to store a large data files with a secure way.

2- Cloud Server (CS): who is managed by CSP, which has a huge storing space and flexible recourses to keep up the client data.

When user first time open website register profile to him then register in the data base which save in the server. Then user enters your username and password then click on submit button. after that digital signature algorithm perform on the server and generate key which is shown to user then user type that key it is more important visible key n entered key are same then server respond to verified key message to user and user successfully login to their profile and access your data.

To implement our design, we need to achieve some goals in our model by allowing the Server to verify the Key over the cloud Environment in the virtual machine. Additionally, we need to ensure that the cloud server does not manipulate or alter the user data in the cloud. Furthermore, the model is achieved using the digital signature technique. The digital signature works by taking the user data first, then perform a hash function over it using RSA Algorithm (RSA) Digital Signature Algorithm. After that, computes the signature for the generated hash value by encrypting it with the private key. In the other side, the decryption is done by the public key but the result will be a hash value, and the hash value is not reversible to its original data.

There are three procedures in our model to satisfy the integrity concept:

1- Digital signature part will be done by the user.

2- The CS verifies over the user data in the cloud to check over the manipulation or intrusions in the cloud data.

In next the paragraphs explanation for each entity function in the proposed model:

1- User: User first chose a random parameter to construct the public and the private keys then he\she will sign the data using the private key to be uploaded to the cloud, then he\she send the signed data to the cloud server.

2- CS: CS will compute a hash value from the original data to send it to the user, and then takes this hash value entered in the web page cloud for verification using the public key. At the end, the CS will inform the user if the key is not verified or any error regarding this concept.

V Result

Consequently, we found that our model provides us a well-defined and efficient result depends on each situation we assumed. With the pages which have been created, we make the system easy to use by the user that does not have background in the digital sign technique. After discussing the situations for the attacking as shown earlier and the forms that were built using windows Azure application make the cloud able to reach the client data integrity and availability.

VI Conclusion & Future Work

In this paper, we proposed a model for the integrity check over the cloud computing and we utilize the TPA and digital signature to achieve the integrity concept, in such a way to help the user to verify and examine the data from unauthorized people that manipulate with the cloud or extract from the data. Moreover, we are able to evaluate our work using a windows azure project that involves digital signature coding. As results, we found that our model worked well according to our claims. In future it can be enhancing in the server side updating and data modification. In our paper we decided to concern about the client data storing service in the cloud. The main objective was to study the ability to verify the client data with the absent of the editing and the deleting. The approach used for the encryption in the verification process was the digital signature. In the implementation we used as an example of the client data in the cloud a text entered by the client, this research is not covering other various kinds of client data. In this paper we have a future work to modification in the data

VII .REFERENCES

[1] "Security and high availability in cloud computing environments", IBM Global Technology Services Technical White Paper ,IBM ,June 2011

[2] M. Sudha, Dr.Bandaru Rama Krishna Rao, M. Monica--- A Comprehensive Approach to Ensure Secure Data Communication in Cloud Environment */International Journal of Computer Applications (0975 – 8887)Volume 12– No.8, December 2010*

[3] Ms. Rashmi A. Akojwar, Ms. Reshma V. Kothari, Mr. Sandip A. Kahate,Ms. Ruchika D. Ganvir-
Software As A Service With Cloud Computing International Journal of Electronics Communication and Computer Engineering Volume 3, Issue 1, ISSN: 2249 –071X

[4] U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology-DIGITAL SIGNATURE STANDARD (DSS)

[5] Digital signature with message recovery
Using self-certified public keys and its variantsYuh-Min Tseng, Jinn-Ke Jan, Hung-Yu Chien

[6] YANG Xiaoyuan1, ZHU Shuaishuai, PAN Xiaozhong-

[7] Cong Wang, Qian Wang and Kui Ren. ―Ensuring Data Storage Security in Cloud computing‖ 978-1-4244-3876-1/2009 IEEE.
[8] John Harauz, Lori M. Kaufman and Bruce Potter, ―Data security in the world of cloud computing ―,2009 IEEE CO Published by the IEEE Computer and Reliability Societies.

[9] Siani Pearson, ―Taking account of Privacy when Designing Cloud computing Services‖ *CLOUD'09*, May 23, 2009, Vancouver, Canada, 2009 IEEE.

[10] Meiko Jensen, Jörg Schwenk, Nils Gruschka, Luigi Lo Iacono, "On Technical Security Issues in Cloud Computing", 2009 IEEE
International Conference on Cloud Computing

[11] Erica Brasher-Sims, "SaaS Software as a Service", 2008

[12] Michael Gregg, "10 Security Concerns for Cloud Computing", Expert Reference Series of White Papers, Global Knowledge, 010