A Review Paper on

# Enhancing Data Security in Cloud Computing Using 3D Framework & Digital Signature with Encryption

Pradeep Bhosale
Student

Priyanka Deshmukh
Student

Girish Dimbar
Student

Ashwini Deshpande
Student

*Department of Computer Engineering*
*Pimpri Chinchwad College of Engineering, Pune India*

## Abstract

*Cloud Computing is emerging technology which consist of existing techniques combined with new technology paradigms. In this new technology shared resources like software's, hardware's and information is provided to its users and other peoples on internet whenever demanded.*

*Today's world relies on cloud computing to store their public as well as some personal information which is needed by the user itself or some other persons. Cloud service is any service offered to its users by cloud. As cloud computing comes in service there are some drawbacks such as privacy of user's data, security of user data is very important aspects.*

*In this paper we are focusing to enhance the data security in cloud computing using 3 dimensional framework and digital signature with RSA Encryption algorithm. In 3 Dimensional frameworks, at client side user select the parameters reactively between CIA (Confidentiality, Integrity & Availability) and before actual storing the data in cloud a digital signature is created using MD 5 Algorithm and then RSA Encryption algorithm is applied then it stored on cloud.*

**Keywords:** Cloud Computing, 3 Dimensional Framework, Digital Signature, RSA Encryption, MD5 Hashing Algorithm, OTP



## 1. Introduction

Cloud computing is a model for enabling ubiquitous, convenient, on demand access to shared pool of computing resources that can rapidly provisioned and released with minimal management efforts. Cloud computing is a practical approach to experience direct cost benefits and it has potential to transform a data center from a capital intensive set up to a variable priced environment [5]. Nowadays cloud computing has becoming IT buzzword for its implementation in last few years [1]. Cloud computing is a term which is often used with synonyms like grid computing, cluster computing, distributed computing, autonomic computing.

Not only this makes researchers to make some modifications in the existing cloud structure, invent new model cloud computing and much more but also there are some extensible features of cloud computing that make him a super power.

## 1.1. Features of cloud computing

### 1.1.1. Scalability

Cloud computing is scalable. That is whenever we need more resources we can add it to the cloud anytime. That is Cloud computing is infinite pool of resources [6].

### 1.1.2. Environment friendly

Cloud computing makes efficient use of hardware which helps to reduce energy cost [6].

### 1.1.3. Cost efficient

Major feature and advantage of cloud computing is, it is cost efficient. We have to pay that much amount which we used just like electricity bill [6].

### 1.1.4. Up to date

We need not to worry about the updates to the software's and hardware's that we are using in the cloud. The provider is responsible for the overall update process of all the components [6].

### 1.1.5. Improved performance

Whenever we need some high configuration resources it will be available to the user on its demand [6].

Now, we come to know some basics about cloud computing, but we still we don't know how cloud computing works? So let's closer look about cloud computing architecture [15].

## 1.2. Cloud delivery models

Cloud computing basically consists of three service model that are used by any cloud service provider to provide the service to the clients, we called it as cloud delivery models and they are [13]

- SaaS (Software as a Service)
- PaaS (Platform as a Service)
- IaaS (Infrastructure as a Service)

### 1.2.1. Software as a service

Applications that are enabled for the cloud supports an architecture that can run multiple instances of it regardless of locations. Software as a service having stateless application architecture and it is available on monthly subscription base [13].

In this model, a complete application is offered to the customer, as a service on demand. A single instance of the service runs on the cloud & multiple end users are serviced. On the customer's side, there is no need for upfront investment in servers or software licenses, while for the provider, the costs are lowered, since only a single application needs to be hosted & maintained [11].
e.g.: Google Docs, Salesforce.com, Microsoft Azure, Zoho etc.

### 1.2.2. Platform as a service

A platform that enables developers to write applications those run on the cloud. A platform would usually have several applications services available for quick deployment [11].

Here, a layer of software or development environment is encapsulated & offered as a service, upon which other higher levels of service can be built. The customer has the freedom to build his own applications, which run on the provider's infrastructure [11].
e.g.: Microsoft azure service platform, force.com, Google App Engine etc.

### 1.2.3. Infrastructure as a service

A highly scaled redundant and shared computing infrastructure accessible using internet technology consists of servers, storage, security, databases and other peripherals.

IaaS provides basic storage and computing capabilities as standardized services over the network. Servers, storage systems, networking equipment, data centre space etc. are pooled and made available to handle workloads [11].
e.g.: Amazon EC2, S3, Sun's cloud service, GoGrid, 3 Tera etc.

Now take a look at different deployment models of cloud computing;

## 1.3. Cloud deployment models

- Private Cloud
- Public Cloud
- Community Cloud
- Hybrid Cloud

#### 1.3.1. Private cloud

Private clouds are built exclusively for a single enterprise. They aim to address concerns on data security and offer greater control, which is typically lacking in a public cloud. There are two variations to a private cloud [11].

#### 1.3.2. Public cloud

Public clouds are owned and operated by third parties; they deliver superior economies of scale to customers, as the infrastructure costs are spread among a mix of users, giving each individual client an attractive low-cost, "Pay-as-you-go" model. All customers share the same infrastructure pool with limited configuration, security protections, and availability variances. These are managed and supported by the cloud provider. One of the advantages of a Public cloud is that they may be larger than an enterprises cloud, thus providing the ability to scale seamlessly, on demand [11].

#### 1.3.3. Hybrid cloud

Hybrid Clouds combine both public and private cloud models. With a Hybrid Cloud, service providers can utilize 3rd party Cloud Providers in a full or partial manner thus increasing the flexibility of computing. The Hybrid cloud environment is capable of providing on-demand, externally provisioned scale. The ability to augment a private cloud with the resources of a public cloud can be used to manage any unexpected surges in workload [11].

#### 1.3.4. Community cloud

Infrastructure shared by several organizations for a shared cause and may be managed by them or a third party service provider [16].

## 2. Challenges in Cloud Computing

Although virtualization and cloud computing can help companies accomplish more by breaking the physical bonds between an IT infrastructure and its users, heightened security threats must be overcome in order to benefit fully from this new computing paradigm. This is particularly true for the SaaS provider. Some security concerns are worth more discussion [2].

With the cloud model, you lose control over physical security. In a public cloud, you are sharing computing resources with other companies. In a shared pool outside the enterprise, you don't have any knowledge or control of where the resources run. Exposing your data in an environment shared with other companies could give the government "reasonable cause" to seize your assets because another company has violated the law. Simply because you share the environment in the cloud, may put your data at risk of seizure. Storage services provided by one cloud vendor may be incompatible with another vendor's services should you decide to move from one to the other. Data integrity is assurance that the data is consistent and correct. Ensuring the integrity of the data really means that it changes only in response to authorized transactions [16]. Following are the major challenges in the cloud computing:

1) Data Protection
2) Data Recovery and Availability
3) Handling Failures
4) Security and Trust Issues

## 3. 3 Dimensional Framework

Cloud computing is emerged as the modern technology which developed in last few years, and considered as the next big thing, in the years to come. Since it is new, so it requires new security techniques and face new challenges as well to improve its performance. Today cloud growing and gets growing up so it becomes major part of IT industry now. Cloud computing is widely accepted as adoption of virtualization, SOA and utility computing [1].

There are different issue and challenges with each cloud computing technology. The various security concerns and upcoming challenges are addressed in the book named Cloud Computing Security Issues and Challenges by Balchandran Reddy. Until now there is no such standard is available regarding service or operational functioning, and its security is a major concern. There are also the architectural security issues which are changing according to various architectural designs functioning over cloud computing [1].

Cloud computing providing services in layered medium, so there must be some SLA (Service Level Agreement) or service management, must be applied over the layers, which eventually increase the confidence of the user [1]. Data security over the cloud also a major concern and various methodologies are proposed also privacy preserving auditing for the data storage security in cloud computing raising the concern over the privacy related issues in data storage such that no critical information can be intercepted as recently a case happened with Wiki leaks, over the security of the data [1].

### 3.1. Problem description

Today cloud computing make everything flexible and easier but there is another aspect that is what about security of user's data? Is cloud computing in current scenario is providing confidentiality, integrity and being regulated by compliance like Data Protection Act [1]. Through cloud computing the resource are centralized, so the exposure factor proportionally increase which results in risk. So it is necessary to put a countermeasure to mitigate the potential risk.

In 3 Dimensional securities scheme, when client uploads the data over the cloud classifies it on the basis of its security level. The data is classified based on 3 parameters Confidentiality, Integrity & Availability (CIA) [1]. Confidentiality means up to what level data should kept secured on the cloud. Integrity provides assurance that data is not altered but is accurate. Reliability means correct data is given output to valid users. These parameters decide the level of security provided on a particular data. The 3 Dimensional framework is explained with following example.

Suppose a businessman wants to upload his information on the cloud. Thus while giving input as data to the cloud he has to categorize that data on the level of security using parameters of CIA (Confidentiality, Integrity and Availability). The data is of any type. Data for example his contact numbers must be uploaded. He decides to give less security for this data as they are not almost important such data of low level of security goes in protection ring level 3.

Data like his schedule of meeting which has a little more level of security counts in the protection ring 2. While data like his bank account number, PAN card number etc. which has highest level of security are kept in protection ring level 1 [1].

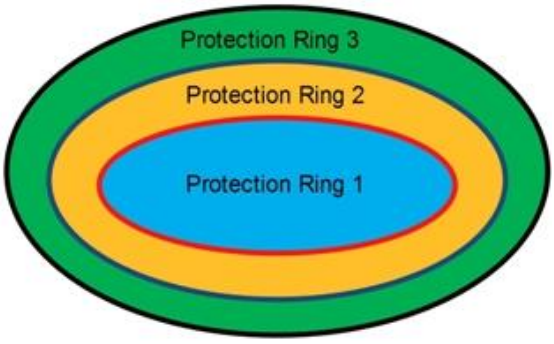


Figure 1. Protection ring structure

3 Dimensional gives facility to the user to categorize data according to its security levels. Thus common data which can be kept public to all users need not require high security schemes. Data categorized thus have increase the level of security of access.

### 3.2. Algorithm

#### 3.2.1. Step 1

Input: User should provide the data as input along with parameters of security levels i.e. CIA. Users have the choice to select the parameters between CIA parameters. User data, protection ring, arrays D, C, I, A, S, R of n integer size [1].

#### 3.2.2. Step 2

Output: Data gets categorized into various rings i.e. ring 1, ring 2, and ring 3. This helps in providing different levels of access to different categories of data. Define data protection ring D [] array of n size.

#### 3.2.3. Step 3

```
for i=1 to n        //input the values of CIA
{
        C[i]    ←value for ith data
        I[i]    ←value for ith data
        A[i]    ← value of ith data
}
```

#### 3.2.4. Step 4

```
For i=1 to n
/*assume rings 3 and protection levels from 1 to 10
selected manually by client while uploading files*/
if (C[i]>6  and I[i]>6) then
Ring level=1 (high)
Else
Calculate new average term CI of both C and I
CI=(C[i] +I[i])/2
Goto step 5
```

#### 3.2.5. Step 5

```
For i=1 to n
If (CI>3 and CI<5 and A[i] <5) then
Ring level 2(Mid)
If (CI>3 and CI<5 and A[i]>5) then
Ring level 3(Low)
If (CI>=1 and CI<3) then
Ring level 3(Low)
```

**Time complexity**

O (n) Best case
O (3n+) Worst case

In above algorithm, the first job of the user is to categorize it on the basis of confidentiality, integrity and availability. Here D [] represents data, now the user have to give the value of C– confidentiality I– integrity and A– availability. After Appling proposed formula the value of Cr criticality raring is calculated. Now allocation of data on the basis of Cr is done in protection ring. This suggests that internal protection ring is very critical and it require more security technique to ensure confidentiality [1].

After applying above the user are required to register itself. And whenever the user access the data he / she have to give username if it matches then it redirected to company for authentication. Now here the user is required to give password for corresponding password. If the user get validated, it redirect to cloud to access resource [1].

This technique provides a new way to authenticate in 3 dimensional approaches. It provides availability of data by overcoming many existing problem like denial of services, data leakage. As additional it also provides more flexibility and capability to meet the new demand of today's complex and diverse network [2].

## 4. Digital Signatures with RSA Encryption Algorithm

In cloud computing where resources are shared and provided to the users. Security plays an important role in cloud paradigm. In case of IT infrastructure public cloud leads to the sharing of computing resources with other companies as well. Here is the risk of data or any other important asset, the risk of seizure. Cloud computing makes use of virtualization where data and resources are stored in a virtual environment. Users will not know exact location of data or other source of data. To ensure data storage safety Confidentiality Integrity and Availability (CIA) should be provided. To extend further safeguards of data and its access encryption schema should be provided along with backup and auditing [2].

### 4.1. Digital signatures

A digital signature or digital signature scheme is a mathematical scheme for demonstrating the authenticity of a digital message or document. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, and that it was not altered in transit. Digital signatures are commonly used for software distribution, financial transactions, and in other cases where it is important to detect forgery or tampering. In some countries, including the United States, India, and members of the European Union, electronic signatures have legal significance [2] [17].

Digital signatures employ a type of asymmetric cryptography. For messages sent through a non secure channel, a properly implemented digital signature gives the receiver reason to believe the message was sent by the claimed sender. Digital signatures are equivalent to traditional handwritten signatures in many respects, but properly implemented digital signatures are more difficult to forge than the handwritten type. Digital signatures can also provide non-repudiation, meaning that the signer cannot successfully claim they did not sign a message, while also claiming their private key remains secret; further, some non-repudiation schemes offer a time stamp for the digital signature, so that even if the private key is exposed, the signature is valid nonetheless. Digitally signed messages may be anything represent able as a bit string: examples include electronic mail, contracts, or a message sent via some other cryptographic protocol [17].

### 4.2. RSA algorithm

RSA is a public key algorithm invented in 1977 by 3 scientists Ron Rivest, Adi Shamir, Leonard Adleman (RSA). RSA is most widely used public key algorithm over internet RSA is capable of supporting encryption and digital signatures. RSA gets its security by integer factorization problem. RSA is relatively very easy to understand and implement [10].

Today RSA is used worldwide to encrypt the data which is confidential and RSA gives best security policy that's why all the service providers such as gmail, hotmail, mediafire etc. are using RSA algorithm to ensure their users full of confidentiality. RSA is also used in some security protocols to ensure security and the protocols are 10]:

- IPSEC/IKE: IP Data Security
- TLS/SSL: Transport Layer Security
- PGP: Email Security
- SSH: Terminal Connection Security
- SILC: Conferencing Service Security

### 4.3. Proposed algorithm

**Step 1. Key Generation**

Declare e as encryption exponent and d as decryption exponent.

p,q ← Integer numbers.
n ←Modulus for keys.
Ø (n) ← Euler's Totient.
e ← Public key exponent.

**Step 2. Compute Values**

2.1 Choose two distinct large prime numbers p &q (Random prime no generation algorithm).
2.2 Compute n=p*q
2.3 Compute Ø(n)=(p-1)(q-1)
2.4 Choose e such that 1<e< Ø(n)
2.5 Compute d*e=1
2.6 Public key is (n,e),private key is (n,d)

**Step 3. Digital signing**

3.1 Sender A create message digest of information using hash function (MD5)
3.2 *Hash Function:*
3.2.1 Declare character 'str' of unsigned long type.
3.2.2 Declare & initialize hash of unsigned integer type.
3.2.3 Unsigned int hash=0

```
int q.
while (q=str+1)
hash=hash+q;
```

3.3 Represent this digest as integer m& it is having value between 0 to n-1
3.4 Uses private key (n,d) to compute the signature
$S=m^d \bmod n$
3.5 Send signature S to the recipients

**Step 4. Encryption**

4.1 Sender A obtain receiver B's public key (n,e)
4.2 Plaintext message as integer m
4.3 Compute ciphertext $c=m^e \bmod n$
4.4 Sends this message (ciphertext) to B

**Step 5. Decryption**

5.1 Uses his private key (n,d) to compute $m=c^d \bmod n$
5.2 Extract plain text

***Step 6.* Signature verification**

6.1 Receiver uses senders public key (n,e) to compute $V=S^e \bmod n$
6.2 Extract message digest from integer V
6.3 Independently computes the message digest of the information that has been signed
6.4 If both are identical the signature is valid

**Time Complexity**

Best Case: O (n)
Worst Case: $O(n^2)$

## 5. One Time Passwords (OTP)

A onetime password (OTP) is generated without connecting the client to the server [3]. The mobile phone will act as a token and use certain factors unique to it among other factors to generate a one-time password locally. The server will have all the required factors including the ones unique to each mobile phone in order to generate the same password at the server side and compare it to the password submitted by the client. The client may submit the password online or through a device such as an ATM machine. A program will be installed on the client's mobile phone to generate the OTP [3].

In order to secure the system, the generated OTP must be hard to guess, retrieve, or trace by hackers. Therefore, it's very important to develop a secure OTP generating algorithm. Several factors can be used by the OTP algorithm to generate a difficult-to-guess password. Users seem to be willing to use simple factors such as their mobile number and a PIN for services such as authorizing mobile micropayments [3].

### 5.1. OTP parameters

#### 5.1.1. IMEI number

The term stands for International Mobile Equipment Identity which is unique to each mobile phone allowing each user to be identified by his device. This is accessible on the mobile phone and will be stored in the server's database for each client [3].

#### 5.1.2. IMSI number

The term stands for International Mobile Subscriber Identity which is a unique number associated with all GSM and Universal Mobile Telecommunications System (UMTS) network mobile phone users. It is stored in the Subscriber Identity Module (SIM) card in the mobile phone. This number will also be stored in the server's database for each client [3].

#### 5.1.3. Username

Although no longer required because the IMEI will uniquely identify the user anyway. This is used together with the PIN to protect the user in case the mobile phone is stolen [3].

#### 5.1.4. PIN

This is required to verify that no one other than the user is using the phone to generate the user's OTP. The PIN together with the username is data that only the user knows so even if the mobile phone is stolen the OTP cannot be generated correctly without knowing the user's PIN. Note that the username and the PIN are never stored in the mobile's memory. They are just used to generate the OTP and discarded immediately after that [3].

#### 5.1.5. Hour

This allows the OTP generated each hour to be unique [5].

#### 5.1.6. Minute

This would make the OTP generated each minute to be unique; hence the OTP would be valid for one minute only and might be inconvenient to the user. An alternative solution is to only use the first digit of the minute which will make the password valid for ten minutes and will be more convenient for the users, since some users need more than a minute to read and enter the OTP. Note that, the software can be modified to allow the administrators to select their preferred OTP validity interval [5].

#### 5.1.7. Day

Makes the OTP set unique to each day of the week.

#### 5.1.8. Year/Month/Date

Using the last two digits of the year and the date and month makes the OTP unique for that particular date [3].

## 6. Proposed System Architecture

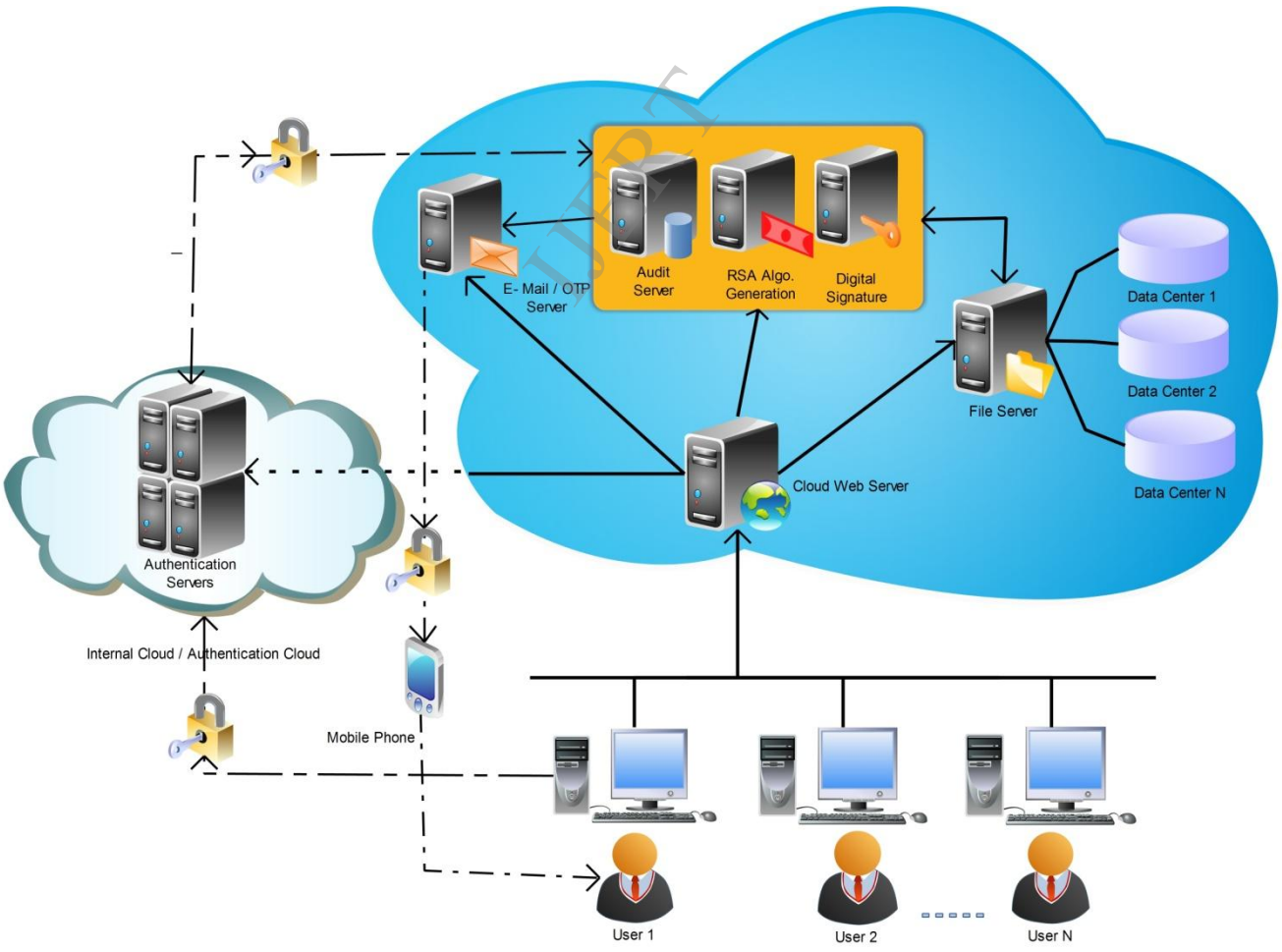


Figure 2. Proposed System Architecture

Above figure is our system's architecture that we are implementing. In this system two techniques are used 3 dimensional framework and digital signature with RSA encryption algorithm. Basic aim is to create a private cloud and in that cloud itself an internal cloud is to be created for the authentication purpose, so multiple users connects to cloud using web services like SOAP and XML. Then the web server is responsible for overall operation in the cloud. For different operations in the cloud different internal servers are used for particular purposes such as Audit server for auditing in the cloud, RSA Generator for algorithm execution, Digital Signature for signature generation. Also Key Generation Center (KGC) helps to generate keys for the algorithm. For ultra secure download mechanism two factor authentication is used in which OTP's are generated and send to client's E-Mail or Mobile and then client is authorized for the downloading the data.

## 7. Performance Evaluation

Models for delivering information technology services in which resources are retrieved from the internet through web based tools and applications, rather than a direct connection to a server. Data and software packages are stored in servers. However, cloud computing structure allows access to information as long as an electronic device has access to the web [18]. In cloud computing technology data and resources are shared; hence there is a threat of accessing of data by invalid users. Initially, the access to the cloud was not secure because credentials such as username and password were required to access. Any invalid user tries to make login to the system using other's account then he is able to access the data [14].

Security policies like 3 dimensional framework enables to categorize data into different security levels. Digital signature is very strong authentication scheme for verifying that only valid user who is liable to access can access the file. RSA is strongest public key encryption algorithm used over the internet now a day. RSA is one of the algorithms having asymmetric key encryption policy. Any invalid user accessing encrypted data then it is hard to interpret [10]. Security of cloud is enhanced by using 3 Dimensional Framework, Digital Signature, RSA Encryption Algorithm and Two Factor Authentication Schemes.

## 8. Conclusion

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 [2].

As cloud is a emerging technology there are some areas where we have to make improvement. Security is most important aspect today, without proper security policies no one can keep their data on the cloud safeguarded. So we have to improve security area of cloud to assure user about his privacy regarding his data on the cloud. To achieve this we implement the technique of 3 dimensional framework along with Digital signature and RSA Encryption Algorithm to improve security one step ahead [1][2].

## 9. References

[1] Parikshit Prasad, Badrinath Ojha, Rajeev Ranjan shahi, Ratan Lal, "3 Dimensional Security in Cloud Computing", IEEE, 2011
[2] Uma Somani, Kanika Lakhani, Manish Mundra, "Implementing Digital Signature with RSA Encryption to Enhance Data Security of Cloud in Cloud Computing", IEEE, 2010
[3] Fadi Aloul, Syed Zahidi, Wassim El-Hajj, "Two Factor Authentication Using Mobile Phones", 2008
[4] Balachandran Reddy, Cloud computing security issues and challenges, 2009
[5] Special Publications 800-145 "National Institute of Standard and Technology (NIST)"
[6] http://en.wikipedia.org/wiki/Cloud_computing
[7] http://cloudcomputing.sys-con.com/node/1744132
[8] Zhidong Shen, Qiang Tong, "The Security of Cloud Computing System enabled by Trusted Computing Technology", 2010
[9] http://www.cloudcomputingchina.cn/Article/ /200909/306.html
[10] Pekka Riikonen, "RSA Algorithm", 2002
[11] Torry Harris, "Cloud Computing An Overview"
[12] Takuya Suzuki, Masayuki Okuhara, "Security Architectures for Cloud Computing", 2010
[13] Anthony T. Velte, Toby J. Velte, "Cloud Computing: A Practical Approach", Tata McGraw Hill Publications.
[14] Gautam Shroff, "Enterprize Cloud Computing", Cambridge University Press
[15] http://www.linuxhowto.in/2011/02/cloud-computing-architecture.html.
[16] Rohit Bhadauria, Rituparna Chaki, Sugata Sanyal, "A Survey on Security Issues in Cloud Computing", 2011
[17] http://en.wikipedia.org/wiki/Digital_signature
[18] http://www.investopedia.com/terms/c/cloud-computing.asp#axzz282pxqmcJ