ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 6, June 2014

Enhance data security of private cloud using encryption scheme with RBAC

Dimpi Rani[1] , Rajiv Kumar Ranjan[2]
M.Tech (CSE) Student, Arni University, Indora, Kangra , India[1]
Assistant Professor, Dept. of CSE, Arni University, Indora, Kangra,India[2]

Abstract: Cloud computing is a phrase used to describe a variety of computing concepts that involve a large number of computers connected through a real-time communication network such as the Internet. Cloud Computing is an emerging paradigm which has become today's hottest research area due to its ability to reduce the costs associated with computing. Due to the fast development of the Cloud Computing technologies, the rapid increase of cloud services are became very remarkable. Securing data is a challenging issue in today's era. Most of the data travel over the internet and it becomes difficult to make data secure. 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 are using a combination of Blowfish Algorthim, RSA and Digital Signature for improving the Security.

Keywords: Cloud Computing , Internet, Role Back Access Control, Blowfish Algorthim, RSA and Digital Signature.

I. INTRODUCTION

Cloud computing is the long dreamed vision of computing as a utility, where data owners can remotely store their data in the cloud to enjoy on-demand high-quality applications and services from a shared pool of configurable computing resources. Cloud is a new business model wrapped around new technologies such as server virtualization that take advantage of economies of scale and multi-tenancy to reduce the cost of using information technology resources. It also brings new and challenging security threats to the outsourced data. Since cloud service providers (CSP) are separate administrative entities, data outsourcing actually relinquishes the owner's ultimate control over the fate of their data. The term cloud computing probably comes from (at least partly) the use of a cloud image to represent the Internet or some large networked environment. Cloud computing really is accessing resources and services needed to perform functions with dynamically changing needs. An application or service developer requests access from the cloud rather than a specific endpoint or named resource. What goes on in the cloud manages multiple infrastructures across multiple organizations and consists of one or more frameworks overlaid on top of the infrastructures tying them together. Cloud computing platforms are growing very quickly. Organizations can provide hardware for clouds internally (internal clouds), or a third party can provide it externally (hosted clouds). A cloud might be restricted to a single organization or group (private clouds), available to the general public over the

Internet (public clouds), or shared by multiple groups or organizations (hybrid clouds) [1].

II. DATA SECURITY ISSUES IN THE CLOUD

A few years ago, the big issue with Cloud was security. Cloud security issues such as physical security, transmission security, storage security, access security, data security, and application security. In Cloud Computing the user must ensure that their infrastructure is secure [2]. In cloud systems, data is stored in a remote location on servers maintained by a cloud provider. The cloud provider should have provision to ensure that there is no direct snooping into client data. With the cloud model, you lose control over physical security. In a public cloud, you are sharing computing resources with other companies. 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 transaction. perhaps two of the more “hot button” issues surrounding cloud computing relate to storing and securing data, and monitoring the use of the cloud by the service providers. These issues are generally attributed to slowing the deployment of cloud services. for example, by storing the information internal to the organization, but allowing it to be used in the cloud. If the provided cloud storage can be accessed or destroyed by malicious attackers, it causes the leakage of personal data that could effect great damage to each individual user. In Cloud Computing the provider must ensure that their infrastructure is secure and that their clients’ data and application s are protected while the customer must ensure that the provider has taken the proper security measures to protect their information.

III. PROPOSED WORK

In this proposed work we want to secure our data in cloud. Because Security is the major issue which is faced by every user. Consider an organization where their are number of Employees(Users) are working. Each User has its own LOG IN ID and PASSWORD where they can store their data and all the organization is managed and operated by ADMIN. With the help of RBAC Admin restrict the system from unauthorized access because their are number of restriction to downloads the files of cloud with every user **.** If any unauthorized user wants to access the data due to downloading restriction they can effect some files rest of files will be saved**.** RBAC helps to secure our data in Cloud. Secondly, Blowfish helps to encrypted the data and RSA works on these encrypted data and generate the public key and private key.

Public key will be generated with every file and Private key helps to generate the digital signature which is required for downloading time. This Digital Signature will be accessed by user via mail. It also provides a better storage and security technique over Cloud architecture. With the kind of (A combination of Blowfish Algorthim and RSA), it would be more secure to gets hacked. These Algorthims helps to provides security. Here we illustrate the Figure1 which represents the basic design of our proposed work.

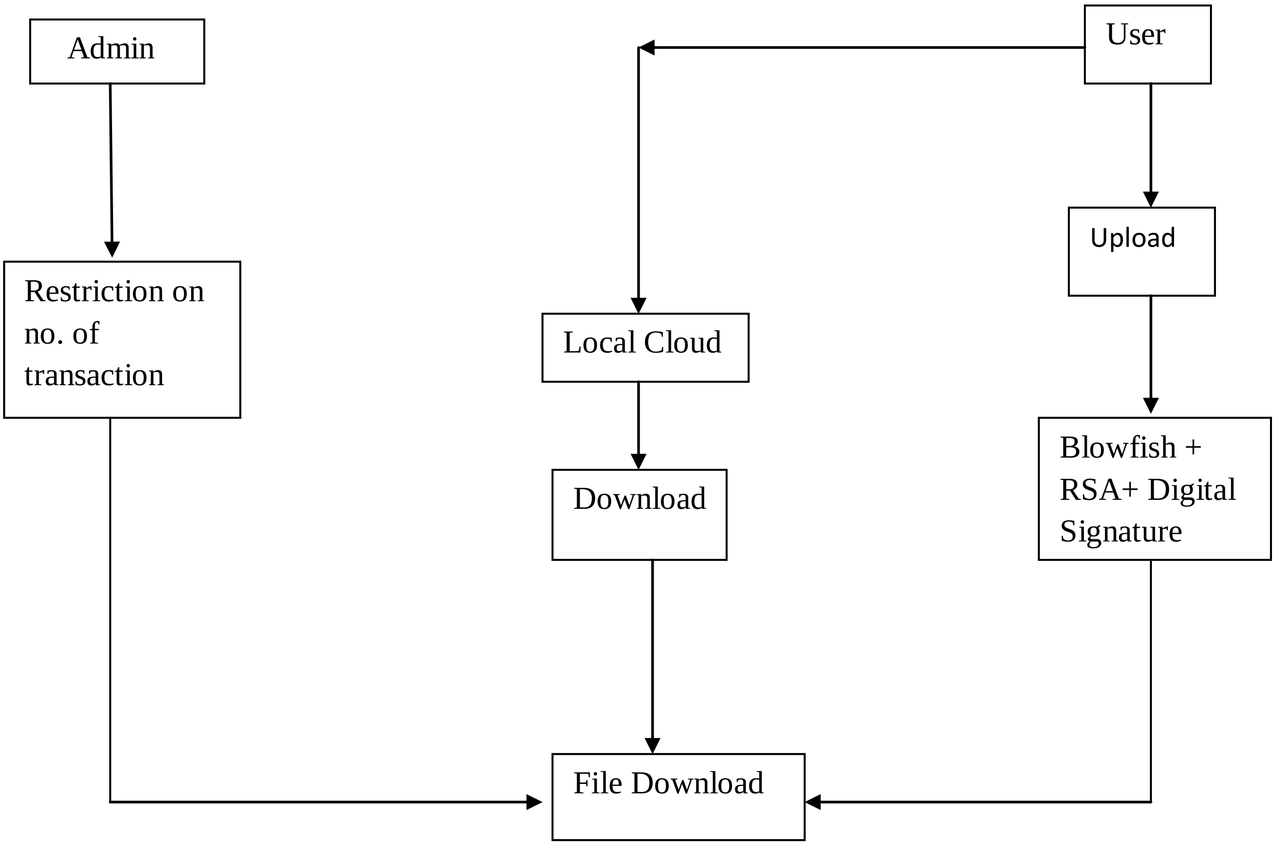

Admin
Restriction on no. of transaction
User
Upload
Blowfish + RSA+ Digital Signature
Local Cloud
Download
File Download

Figure 1 :- Represents the basic design of proposed work

Admin: In an organization, admin create roles for users & also specify the number of transactions per user as per their role.

User: A user can upload/ download file. When uploading file Blowfish, and RSA schemes are used to encrypt data & signature is included to lock that data and when downloading the files inversaly Blowfish and RSA are used to decrypt data & signature is used to unlock the file.

Local Cloud:_Local Cloud is used to store data in the encrypted form.

Below we will explain RBAC , Blowfish Algorthim, RSA and Digital Signature.

A . ROLE- BASED ACCESS CONTROL

RBAC is a rich technology and a great effort in the field of Access control A role represents a specific function within an organization and can be seen as a set of actions or responsibilities associated with this function. Roles are defined by Administrator according to job competency, authority, and responsibility within the organization. [3].In a RBAC model, all grant authorizations deal with roles, rather than being granted to users by Admin.. RBAC ensures that only authorized users are given access to certain data or resources. Roles are defined by Administrator according to job competency, authority, and responsibility within the organization.

B. Blowfish Algorithm

Blowfish is a symmetric block cipher algorithm. It uses the same secret key to both encryption and decryption of messages. The block size for Blowfish is 64 bits; messages that aren't a multiple of 64-bits in size have to be padded. It uses a variable –length key, from 32 bits to 448 bits. [4].It is appropriate for applications where the key is not changed frequently. It is considerably faster than most encryption algorithms when executed in 32-bit microprocessors with huge data caches. Data encryption happens via a 16-round Feistel network as shown in figure 3.

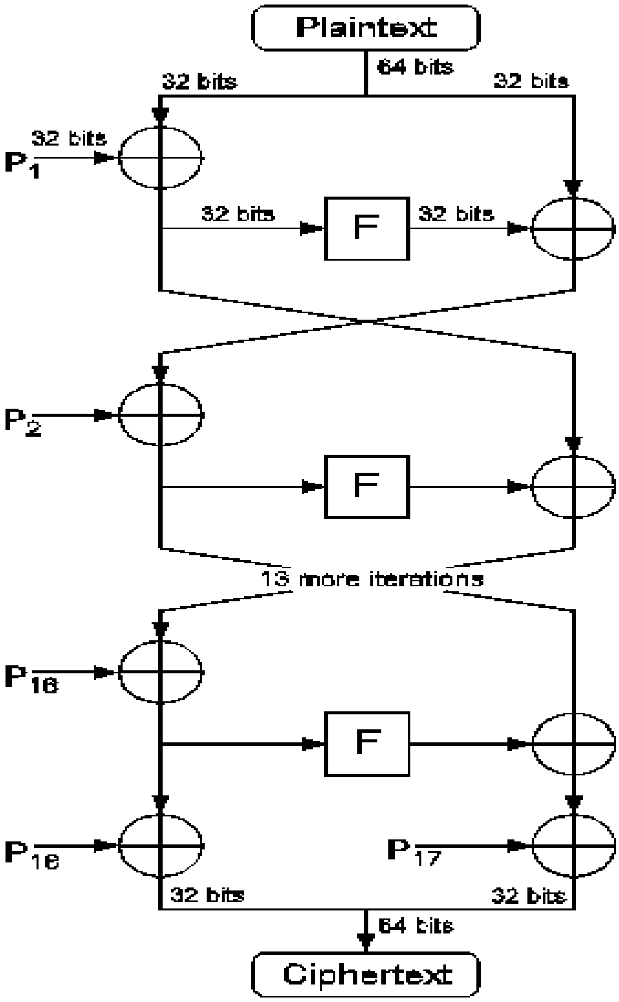


Figure 2. Encryption with Blowfish

C. RSA

RSA is widely used Public-Key algorithm. RSA stands for Ron Rivest, Adi Shamir and Len Adleman, who first publicly described it in 1977. In our proposed work, we are using RSA algorithm to encrypt the data to provide security so that only the concerned user can access it. [5].Here we explain RSA algorthim.

RSA algorithm involves three steps:

1. Key Generation
2. Encryption
3. Decryption

An RSA algorithm is the genetic algorithms in the security system in the cryptography[6]. In RSA algorithms first we choose the two integer values.

Let P and Q are the integer values. Then we find the value
of N.

$N = P \times Q$ … (3.1)

$\emptyset(N) = (P - 1) \times (Q - 1)$ … (3.2)

Then we choose the value of e, which is not factor of $\emptyset(N)$

And also we find the value of d, which is related the expectation value (e).

$ed = 1 \bmod \emptyset(N)$ … (3.3)

Or $d = \frac{1}{e} \bmod \emptyset(N)$ … (3.4)

Or $d = e^{-1} \bmod \emptyset(N)$ … (3.5)

By Euclidian theorem the value of d depends upon $|\emptyset(N)|$.

The value of d has the modulus values 1, 2…n.

$d = 1 + |\emptyset(N)|$ … (3.6)

RSA algorithms are also used in the encryption and decryption.

Encryption key = (e, N).

Decryption key = (d, N).

If the message M so the value of M <N.

Encrypt = $E = M^e \bmod N$ ... (3.7)

Decrypt => $M = E^d \bmod N$ … (3.8)

In equations (3.1), (3.2) and (3.6) are using for the key generation but the equation (3.7), (3.8) are using encryption and decryption.

D. Digital Signatures

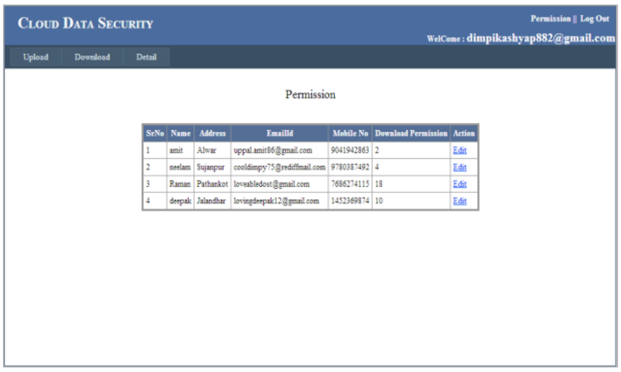
Digital signature is a mathematical scheme for demonstrating the authenticity of a digital message or document. Digital signatures are commonly used for software distribution, financial transactions, and in other cases where it is important to detect forgery or tampering.. A key generation algorithm that selects a private key uniformly at random from a set of possible

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

private keys. The algorithm outputs the private key and a corresponding public key. 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. Digitally signed messages may be anything able as a bit string: examples include electronic mail, contracts, or a message sent via some other cryptographic protocol .

IV. IMPLEMENTATION AND RESULT

1. The described work is implemented in ASP.NET. Firstly we show the snapshot where admin restricts all the users to the number of downloads. This snapshot represents the list of employees who are working in an organization and restriction in no. of download which is granted by Admin. Figure 3. Represents the permission taken. . This restriction provides the security with the help of RBAC. because an unauthorized user cannot download the files without admin permission.

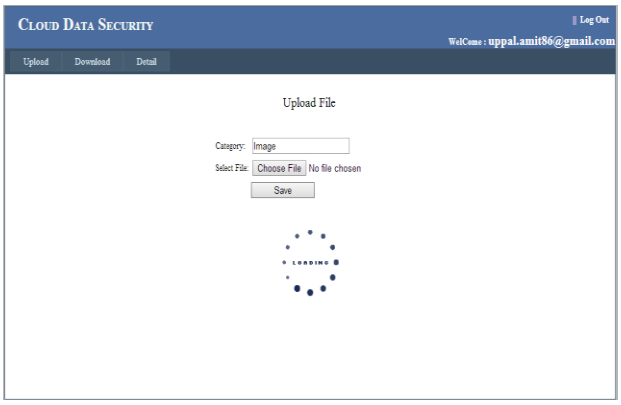


Permission

SrNo	Name	Address	EmailId	Mobile No	Download Permission	Action
1	amit	Alwar	uppal.amit86@gmail.com	9041942863	2	Edit
2	neelam	Sujanpur	cooldimpy75@rediffmail.com	9780387492	4	Edit
3	Raman	Pathankot	loveabledost@gmail.com	7686274115	18	Edit
4	deepak	Jalandhar	lovingdeepak12@gmail.com	1452369874	10	Edit

Fig. 3: Representation for permission taken

2. Figure 4. represents the uploading page where Employee upload the file and the processing can take place. When Employee upload a file Firstly Blowfish Algorthim applied on the file which encrypt the data.Within the help of Blowfish a ciphertext is generated. Then Secondly, RSA is applied on it. And RSA generate a public and private key with every file. Public key is shown within each file and helps to generate a new session and private key with the help of Digital Signature Algorthim generate a Digital Signature which is send to e-mail of Employee.



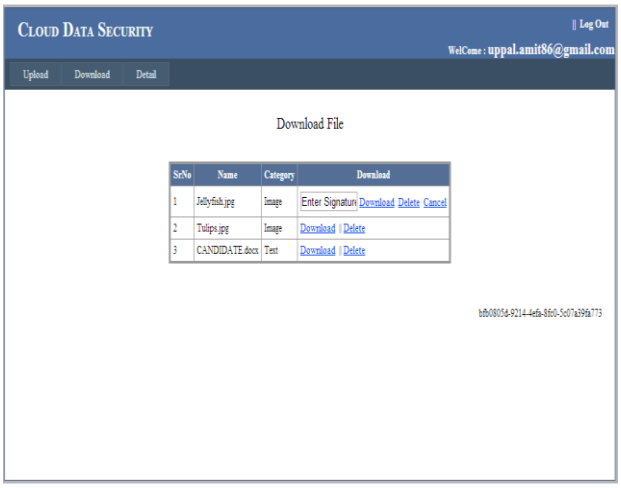
Upload File

Category: Image

Select File: No file chosen

Figure4. Represents the uploading procedure

3. Figure 5. represents the downloading procedure where Employee wants to download the file. but during downloading a file a Digital Signature is required which can be accessed by via e-mail of Employee. And their Right side a public key is shown.



Download File

SrNo	Name	Category	Download
1	Jellyfish.jpg	Image	Enter Signature Download Delete Cancel
2	Tulips.jpg	Image	Download | Delete
3	CANDIDATE.docx	Text	Download | Delete

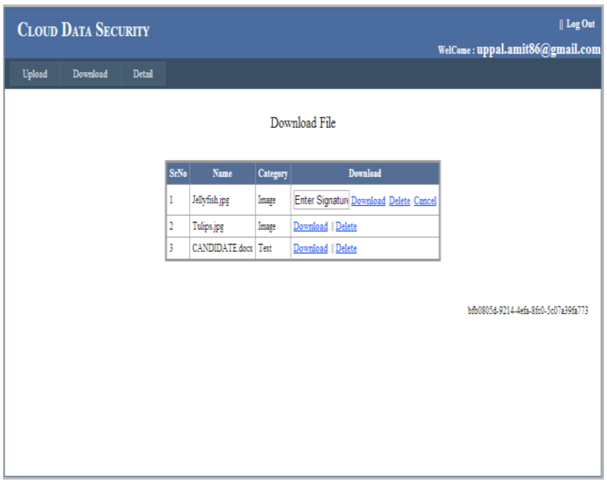
bfb0805d-9214-4efa-8fc0-5c07a39fa773

Figure 5. Represents the downloading procedure

4. This Snapshot Figure 6. represents the Signature key which is required for downloading the files.

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

When user wants to download a file Signature is required And the Signature is accessed by user via mail.



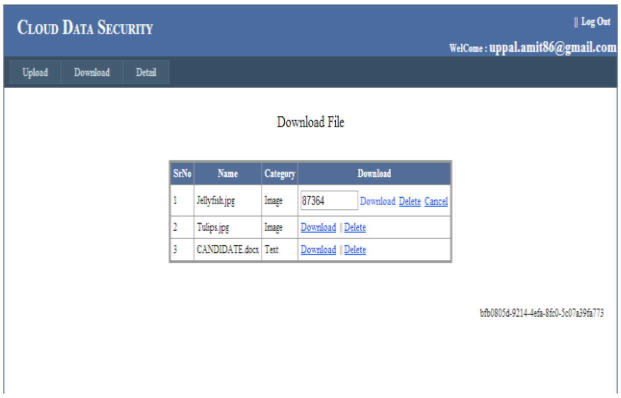
Download File

SrNo	Name	Category	Download
1	Jellyfish.jpg	Image	Enter Signatur Download Delete Cancel
2	Tulips.jpg	Image	Download | Delete
3	CANDIDATE.docx	Text	Download | Delete

bfb0805d-9214-4efa-8fc0-5c07a39fa773

Figure 6. Represents the Signature key

5. Figure 7. represent the downloading a file within Signature. An Employee enter the Signature and accessed the file.. When an Employee enter an Signature file is downloaded. Similarly second file is downloaded by using Signature.



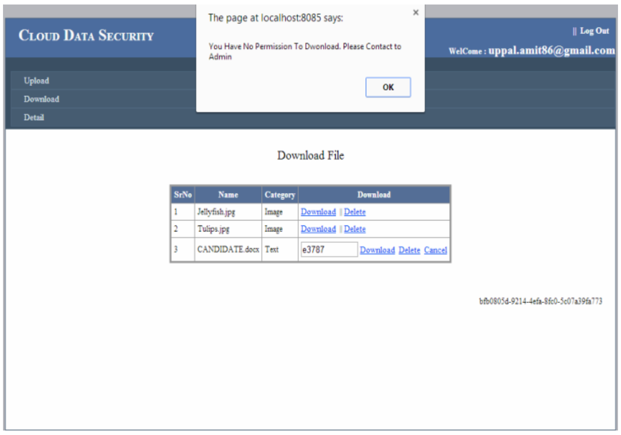
Download File

SrNo	Name	Category	Download
1	Jellyfish.jpg	Image	87364 Download Delete Cancel
2	Tulips.jpg	Image	Download | Delete
3	CANDIDATE.docx	Text	Download | Delete

bfb0805d-9214-4efa-8fc0-5c07a39fa773

Figure7. Downloading a file within Signature.

3. Figure 8.represents the downloading a page within No Permission To Download Message. Because an Employee have restricted only two files have downloaded. Because Employee is restricted by an admin. After accessing two files when Employee wants to download a third file a message is generated that Contact to admin.



The page at localhost:8085 says:

You Have No Permission To Dwonload. Please Contact to Admin

Download File

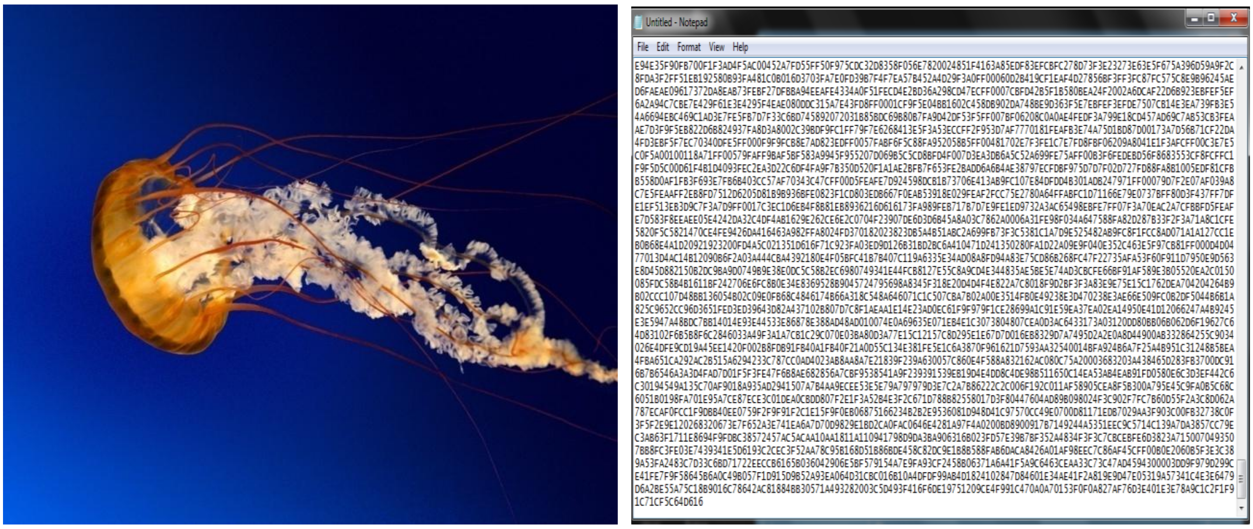
SrNo	Name	Category	Download
1	Jellyfish.jpg	Image	Download | Delete
2	Tulips.jpg	Image	Download | Delete
3	CANDIDATE.docx	Text	e3787 Download Delete Cancel

bfb0805d-9214-4efa-8fc0-5c07a39fa773

Figure 8. Represents the downloading files

within Restriction

6. Blowfish and RSA helps to encrypted the data which converts an Image into an Encrypted form of data. Below Fig.9. Represents the Encryption by using Blowfish Algorithm and RSA.



```
E94E35F90FB700F1F3AD4F5AC00452A7FD55FF50F975CDC32D8358F056E7820024851F4163A85EDF83EFCBFC278D73F3E23273E63E5F675A396D59A9F2C
8FDA3F2FF51EB192580B93FA481C0B016D3703FA7E0FD39B7F4F7EA57B452A4D29F3A0FF00060D2B419CF1EAF4D27856BF3FF3FC87FC575C8E9B96245AE
D6FAEAE09617372DA8EAB73FEBF27DFBBA94EEAFE4334A0F51FECD4E2BD36A298CD47ECFF0007CBFD42B5F1B580BEA24F2002A6DCAF22D6B923EBFEF5EF
6A2A94C7CBE7E429F61E3E4295F4EAE080DDC315A7E43FD8FF0001CF9F5E04BB1602C458DB902DA748BE9D363F5E7EBFEF3EFDE7507CB14E3EA739FB3E5
4A6694EBC469C1AD3E7FE5FB7D7F33C6BD745892072031B85BDC69B80B7FA9D42DF53F5FF007BF06208C0A0AE4FEDF3A799E18CD457AD69C7AB53CB3FEA
AE7D3F9F5EB822D6B824937FA8D3A8002C39BDF9FC1FF79F7E6268413E5F3A53ECCFF2F953D7AF7770181FEAFB3E74A75D1BD87D00173A7D56B71CF22DA
4FD3EBF5F7EC70340DFE5FF000F9F9FCB8E7AD823EDFF0057FABF6F5C88FA952058B5FF00481702E7F3FE1C7E7FD8FBF06209A8041E1F3AFCFF00C3E7E5
C0F5A00100118A71FF00579FAFF9BAF5BF583A9945F955207D069B5C5CD8BFD4F007D3EA3DB6A5C52A699FE75AFF00B3F6FEDEBD56F8683553CF8FCFFC1
F9F5D5C00D61F4B1D4093FEC2EA3D22C6DF4FA9F7B350D520F1A1AE2BFB7F653FE2BADD6A6B4AE38797ECFDBF975D7D7F02D727FD88FA8B1005EDF81CFB
B558D0AF1FB3F693E7FB6B403CC57AF70343C47CFF00D5FEAFE7D924598DCB1B73706E413AB9FC107E84DFDD4B301ADB247971FF00079D7F2E07AF039A8
C7E5FEAAFF2EB8FD7512D6205D81B9B936BFE0823F1CD803EDB667F0EAB53918E029FEAF2FCC75E2780A64FFABFC1D71166E79E0737BFF80D3F437FF7DF
E1EF513EB3D9C7F3A7D9FF0017C3EC1D6EB4F8B81EB8936216D616173FA989FEB717B7D7E9FE1ED9732A3AC65498EBFE7FF07F3A70EAC2A7CFBBFD5FEAF
E7D583F8EEAEE05E4242DA32C4DF4AB1629E262CE6E2C0704F23907DE6D3D6B45A8A03C7862A0006A31FE98F034A647588FA82D287B33F2F3A71A8C1CFE
5820F5C5821470CE4FE9426DA416463A982FFA8024FD370182023823DB5A4B51ABC2A699FB73F3C5381C1A7D9E525482AB9FC8F1FCC8AD071A1A127CC1E
B0B68E4A1D20921923200FD4A5C021351D616F71C923FA03ED9D126B31BD2BC6A410471D241350280FA1D22A09E9F040E352C463E5F97CB81FF000D4D04
77013D4AC14B12090B6F2A03A444CBA4392180E4F05BFC41B7B407C119A6335E34AD08A8FD94A83E75CD86B268FC47F22735AFA53F60F911D7950E9D563
E8D45D882150B2DC9BA9D0749B9E38E0DC5C58B2EC6980749341E44FCB8127E55C8A9CD4E344835AE5BE5E74AD3CBCFE66BF91AF589E3B05520EA2C0150
085FDC58B4B1611BF242706E6FC8B0E34E8369528B9045724795698A8345F318E20D4D4F4E822A7C8018F9D2BF3F3A83E9E75E15C1762DEA704204264B9
B02CCC107D48BB136054B02C09E0FB68C4846174B66A318C548A646071C1C507CBA7B02A00E3514FB0E49238E3D470238E3AE66E509FC0B2DF5044B6B1A
825C9652CC96D3651FED3ED39643D82A437102B807D7C8F1AEAA1E14E23AD0EC61F9F979F1CE28699A1C91E59EA37EA02EA14950E41D12066247A4B9245
E3E5947A48BDC7BB14014E93E44533E86878E388AD48AD010074E0A69635E071EB4E1C3073804807CEA0D3AC6433173A03120DD80BB06B062D6F19627C6
4D83102F6B5B8F6C2846033A49F3A1A7CB1C29C070E03BA80D3A77E15C12157C8D295E1E67D7D016EB8329D7A7495D2A2E0A8D44900AB332864255C9034
026E4DFE9CD19A45EE1420F002B8FDB91FB40A1FB40F21A0D55C134E381FE5E1C6A3870F961621D7593AA32540014BFA924B6A7F25A4B951C31248B5BEA
4FBA651CA292AC2B515A6294233C787CC0AD4023AB8AA8A7E21839F239A630057C860E4F588A832162AC080C75A20003683203A438465D283FB3700DC91
6B7B6546A3A3D4FAD7D01F5F3FE47F6B8AE682856A7CBF9538541A9F239391539EB19D4E4DD8C4DE98B511650C14EA53AB4EAB91FD0580E6C3D3EF442C6
C30194549A135C70AF9018A935AD2941507A7B4AA9ECEE53E5E79A797979D3E7C2A7B86222C2C006F192C011AF58905CEA8F5B300A795E45C9FA0B5C68C
6051B0198FA701E95A7CE87ECE3C01DEA0CBDD807F2E1F3A52B4E3F2C671D788B82558017D3F80447604AD89B098024F3C902F7FC7B60D55F2A3C8D062A
787ECAF0FCC1F9DBB40EE0759F2F9F91F2C1E15F9F0EB06875166234B2B2E9536081D948D41C97570CC49E0700D81171EDB7029AA3F903C00FB32738C0F
3F5F2E9E120268320673E7F652A3E741EA6A7D70D9829E1BD2CA0FAC0646E4281A97F4A0200BD8900917B7149244A5351EEC9C5714C139A7DA3857CC79E
C3AB63F1711E8694F9FDBC38572457AC5ACAA10AA1811A110941798D9DA3BA906316B023FD57E39B7BF352A4834F3F3C7CBCEBFE6D3823A715007049350
7BB8FC3FE03E7439341E5D6193C2CEC3F52AA78C95B168D51B86BDE458C82DC9E1B8B588FAB6DACA8426A01AF98EEC7C86AF45CFF00B0E2060B5F3E3C38
9A53FA2483C7D33C6BD71722EECCB6165B036042906E5BF579154A7E9FA93CF2458B06371A6A41F5A9C6463CEAA33C73C47AD4594300003DD9F979D299C
E41FE7F9F58645B6A0C49B057F1D915D9B52A93EA064D31CBC016B10A4DFDF99AB4D1824102847D84601E34AE41F2A819E9D47E05319A57341C4E3E6479
D6A2BE55A75C18B9016C78642AC81884BB30571A493282003C5D493F416F6DE19751209CE4F991C470A0A70153F0F0A827AF76D3E401E3E78A9C1C2F1F9
1C71CF5C64D616
```

Fig.9. Encryption by using Blowfish Algorithm and RSA

CONCLUSION AND FUTURE SCOPE

Cloud Computing is still a new and evolving paradigm where computing is regarded as on-demand service. Once the organization takes the decision to move to the cloud, it loses control over the data. Security of the Cloud relies on trusted computing and cryptography. Thus, in our proposed work, only the authorized user can access the data. Even if some intruder (unauthorized user) gets the data accidentally or intentionally if he captures the data also, he can't decrypt it and accessed it due to encryption techniques. With the help of RBAC we will restrict the system from unauthorized access. With the kind of (A combination of Blowfish Algorthim and RSA),it would be more secure to gets hacked. It also provides a better storage and security technique using Digital Signature over Cloud architecture.

In future My proposed work is very help full to increase the security on cloud in cloud computing As the Security need increases so, reliable authentication systems are required which can help to minimize the unauthorized access & helps for safeguarding of data .

ACKNOWLEDGMENT

Author would like to give her sincere gratitude to guide Mr. Rajiv Kumar Ranjan who encouraged and guided her throughout this paper.

REFERENCES

[1]. Uma Somani, "Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing," 2010 1st International Conference on Parallel, Distributed and Grid Computing (PDGC - 2010). Volume 64, pp.211-216

[2]. Leena Khanna " Cloud Computing: Security Issues And Description Of Encryption Based Algorithms To Overcome Them" International Journal of Advanced Research in Computer Science and Software Engineering,Volume 3 March - 2013, pp. 279-283.

[3]. Wei-Tek Tsai "Role-Based Access-Control Using Reference Ontology in Clouds"978-0-7695-4349-9/11 $26.00 © 2011 IEEE DOI 10.1109/ISADS.2011.21

[4].Ajit Singh, "Securing Data by Using CryptographywithSteganography""International Journal of Advanced Research in Computer Science and Software Engineering"Volume 3, Issue 5, May 2013 ,pp.404-402

[5].Rashmi Nigoti "A Survey of Cryptographic Algorithms for Cloud Computing" IJETCAS 13-123; March-May 2013, pp.141-146

[6]. Parsi Kalpana "Data Security in Cloud Computing using RSA Algorithm" International Journal of Research in Computer and Communication technology, IJRCCT, ISSN 2278-5841, Vol 1, Issue 4, September 2012.

[7]. Esh Narayan" To Enhance the data security of cloud in cloud computing using RSA Algorthim", Bookman International Journal of Software Engineering, Vol. 1 No. 1 Sep. 2012 ,ISSN No. 2319-4278

[8] Pradeep Bhosale" Enhancing Data Security in Cloud Computing Using 3D Framework & Digital Signature with Encryption", International Journal of Engineering Research & Technology (IJERT) Vol. 1 Issue 8, October – 2012 ,ISSN: 2278-0181

[9]. Vishakha Lokhande" Efficient Encryption and Decryption Services for Cloud Computing", International Journal of Societal Applications of Computer Science,Vol 1 Issue 2 December 2012 ISSN 2319 – 8443.

[10]. RuWei Huang, Si Yu, Wei Zhuang and XiaoLin Gui, "Design of Privacy-Preserving Cloud Storage Framework" 2010 Ninth International Conference on Grid and Cloud Computing.

[11]. Farzad Sabahi, “Cloud Computing Security Threats and Responses," IEEE Trans. on Cloud Computing., vol. 11, no. 6, pp. 670 { 684, 2002.}

[12]. Mohammed Achemlal, Sa¨ıd Gharout and Chrystel Gaber “Trusted Platform Module as an Enabler for Security in Cloud Computing” Vol 978-1-4577-0737-7/11/$26.00 ©2011 IEEE.

[13]. Jianfeng Yang, Zhibin Chen “Cloud Computing Research and Security Issues” Vol 978-1-4244-5392-4/10/$26.00 ©2010 IEEE.

[14]. Victor Echeverr´ıa, Lorie M. Liebrock, and Dongwan Shin “Permission Management System: Permission as a Service in Cloud Computing” 2010 34th Annual IEEE Computer Software and Applications Conference Workshops.