Volume 3, Issue 11, November 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Third Party Auditing (TPA) for Data Storage Security in Cloud with RC5 Algorithm

Miss. Nupoor M. Yawale
M.E. Second year CSE
P R Patil COET, Amravati. INDIA.

Prof. V. B. Gadichha
P R Patil COET
Amravati. INDIA.

Abstract-- Cloud computing is an internet based computing which enables sharing of services. Cloud computing allows users to use applications without installation any application and access their personal files and application at any computer with internet or intranet access. Many users place their data in the cloud, so correctness of data and security is a prime concern.Cloud Computing is technology for next generation Information and Software enabled work that is capable of changing the software working environment. It is interconnecting the large-scalecomputing resources to effectively integrate, and to computing resources as a service to users. To ensure the correctness of data, we consider the task of allowing a third party auditor (TPA), on behalf of the cloud client, to verify the integrity of the data stored in the cloud., the auditing process should bring in no new vulnerabilities towards user data privacy, and introduce no additional online burden to user. In this paper, we propose a secure cloud storage system supporting privacy-preserving public auditing. We further extend our result to enable the TPA to perform audits for multiple users simultaneously and efficiently with RC5 Encryption Algorithm. This shows the proposed scheme is highly efficient and data modification attack, and even server colluding attacks. Here Work is focuses on RC5 Encryption Algorithm for stored data in cloud. Resulted encrypted method is secure and easy to use.

Keywords-- Cloud computing, Encryption, Data integrity, Third Party Auditor (TPA), RC5 Algorithm, privacy-preserving, public auditability.

I. INTRODUCTION

A. Cloud Computing: Cloud computing is innovation that uses advanced computational power and improved storage capabilities. Cloud computing is a long dreamed vision of computing utility, which enable the sharing of services over the internet. Cloud is a large group of interconnected computers, which is a major change in how we store information and run application. Cloud computing is a shared pool of configurable computing resources, on-demand network access and provisioned by the service provider [1]. The advantage of cloud is cost savings. The prime disadvantage is security. Cloud computing is used by many software industries. Since the security is not provided in cloud, many companies adopt their unique security structure. The data placed in the cloud is accessible to everyone, security is not guaranteed. To ensure security, cryptographic techniques cannot be directly adopted. Sometimes the cloud service provider may hide the data corruptions to maintain the reputation. To avoid this problem, we introduce an effective third party auditor to audit the user's outsourced data when needed. The security is achieved by RC5 Encryption Algorithm. We utilized public key based homomorphic authenticator with random masking to achieve privacy preserving auditing protocol.TPA performs the auditing task for each user.[2]

B. Third party Auditor (TPA): Third Party Auditor is kind of inspector. There are two categories: private auditability and public auditability. Although private auditability can achieve higher scheme efficiency, public auditability allows anyone, not just the client (data owner), to challenge the cloud server for the correctness of data storage while keeping no private information. To let off the burden of management of data of the data owner, TPA will audit the data of client. It eliminates the involvement of the client by auditing that whether his data stored in the cloud are indeed intact, which can be important in achieving economies of scale for Cloud Computing. The released audit report would help owners to evaluate the risk of their subscribed cloud data services, and it will also be beneficial to the cloud service provider to improve their cloud based service platform [3]. Hence TPA will help data owner to make sure that his data are safe in the cloud and management of data will be easy and less burdening to data owner.

Cloud consumers save data in cloud server so that security as well as data storage correctness is primary concern. A novel and homogeneous structure is introduced [4] to provide security to different cloud types. To achieve data storage security, RC5 algorithm is used. RC5 algorithm is efficient and safer than the former algorithms. It allows TPA to perform multiple auditing tasks for different users at the same.

II. OBJECTIVE

Our contribution in this paper is summarized as follows:

1) We motivate the public auditing system of data storage security in Cloud Computing and provide a privacy-preserving auditing protocol, i.e., our scheme supports an external auditor to audit user's outsourced data in the cloud without learning knowledge on the data content.

2) To the best of our knowledge, our scheme is the first to support scalable and efficient public auditing in the Cloud Computing. In particular, the TPA will be fully automated and will be able to properly monitor confidentiality and integrity of the data with RC5 Algorithm.
3) We prove the security and justify the performance of our proposed schemes through concrete experiments and comparisons with the state-of-the-art.

III. EXISTING SYSTEM

Cloud improves due to centralization of data, increased security-focused resources, etc., but concerns can persist about loss of control over certain sensitive data, and the lack of security for stored kernels. Security is often as good as or better than other traditional systems, in part because providers are able to devote resources to solving security issues that many customers cannot afford.

To securely introduce an effective third party auditor (TPA), the following two fundamental requirements have to be met: 1) TPA should be able to efficiently audit the cloud data storage without demanding the local copy of data, and introduce no additional on-line burden to the cloud user; 2) The third party auditing process should bring in no new vulnerabilities towards user data privacy.

A. Drawbacks of existing system

- Cloud Storage system provides the user for safe and consistent place to save valuable data and documents. However, user's files are not encrypted on some open source cloud storage systems. i.e. TPA demands retrieval of user data, here privacy is not preserved.
- The storage service provider can easily access the user's files. This brings a big concern about user's privacy. The user has no supreme control over the software applications including secret data. User has to depend on the provider‘s action, maintenance and admin it.

IV. PROPOSED SYSTEM

In this paper, the TPA will be fully automated and will be able to properly monitor confidentiality and integrity of the data and uniquely integrate it with random mask technique to achieve a privacy-preserving public auditing system for cloud data storage security while keeping all above requirements in mind. Extensive security and performance analysis shows the proposed schemes are provably secure and highly efficient. We also show how to extent our main scheme to support batch auditing for TPA upon delegations from multi-users. The use of RC5 algorithm for encryption, cloud computing can be applied to the data transmission security. Transmission of data will be encrypted, even if the data is stolen, there is no corresponding key that cannot be restored. Only the user knows the key, the clouds do not know the key. Also, because the properties of encryption, the cloud can operate on cipher text, thus avoiding the encrypted data to the traditional efficiency of operation. User's privacy is protected because user's files are encrypted in cloud storage. In this paper, we introduce a dynamic audit service for integrity verification of untrusted and outsourced storages. Our au dit system, based on novel audit system architecture, can support dynamic data operations and timely abnormal detection with the help of several effective techniques, such as fragment structure, random sampling, and index hash table. We propose an efficient approach based on probabilistic query and periodic verification for improving the performance of audit services. A proof of concept prototype is also implemented to evaluate the feasibility and viability of our proposed approaches. Our experimental results not only validate the effectiveness of our approaches, but also sho w our system has a lower computation cost, as well as a shorter extra storage for integrity verification.

A. Advantages:

- A fragment technique is introduced in this paper to improve performance and reduce extra storage.
- The audit activities are efficiently scheduled in an audit period, and a TPA needs merely access file to perform a udit in each activity.
- Each TPA to audit for a batch of files and to save the times for auditing the files.

V. WORKING METHODOLOGY

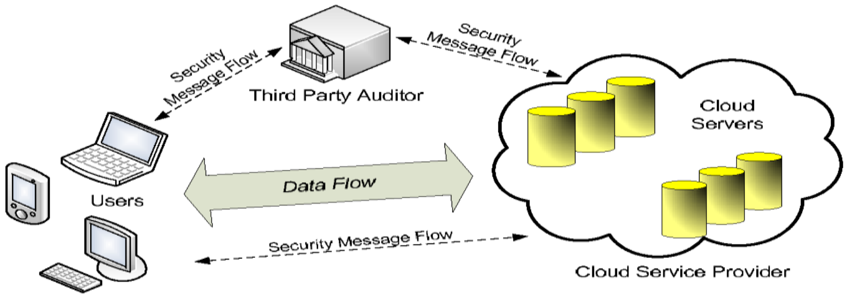


Fig. 1: The architecture of cloud data storage service

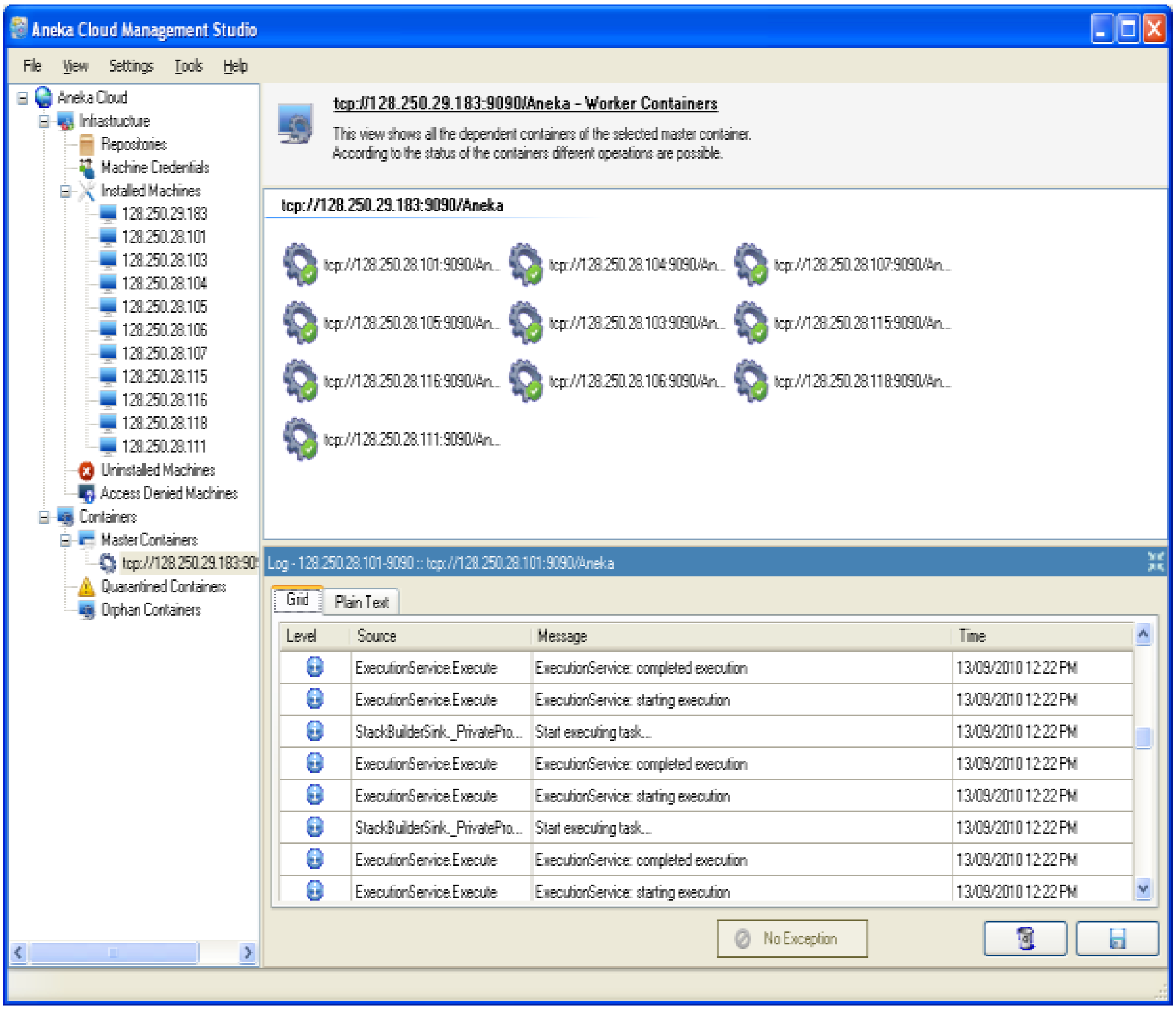
In this paper, we consider data storage and sharing services in the cloud with three entities: *the cloud, the third party auditor (TPA), and users* who participate as a group (as shown in Fig. 1). Users in a group include one original user and a number of group users. The original user is the original owner of data, and shares data in the cloud with other users. Based on access control policies [5], other users in the group are able to access, download and modify shared data. The cloud provides data storage and sharing services for users, and has ample storage space. The third party auditor is able to verify the integrity of shared data based on requests from users, without downloading the entire data. When a user (either the original user or a group user) wishes to check the integrity of shared data, she first sends an auditing request to the TPA. After receiving the auditing request, the TPA generates an auditing message to the cloud, and retrieves an auditing proof of shared data from the cloud. Then the TPA verifies the correctness of the auditing proof. Finally, the TPA sends an auditing report to the user based on the result of the verification.

VI. ENSURING DATA SECURITY WITH ENCRYPTION

One of the best ways to ensure confidential data is protected in the cloud is to utilize encryption for data. Almost all cloud service providers support encryption for data storage, but few offer support for data at rest. The cloud encryption capabilities of the service provider need to match the level of sensitivity of the data being hosted [6]. Encryption plays a big role in fulfillment as many policies require specific data elements to be encrypted. The most important guidance on encryption is publically available from NIST 800-111 and FIPS-140-2. These standards can help you evaluate the encryption capabilities of a cloud provider for compliance with regulations. To protect a user‘s confidential data in the cloud, encryption is a powerful tool that can be used effectively. Only user can confidently utilize cloud providers knowing that their confidential data is protected by encryption.

VII. DEPLOYING RC5 ENCRYPTION ALGORITHM AT MANJRASOFT ANEKA2.0 CLOUD ENVIRONMENT

Aneka is a market oriented Cloud development and management platform with rapid application development and workload distribution capabilities. Aneka is an integrated middleware package which allows you to build and manage an interconnected network in addition to accelerating development, deployment and management of distributed applications using Microsoft .NET frameworks on these networks.



tcp://128.250.29.183:9090/Aneka - Worker Containers

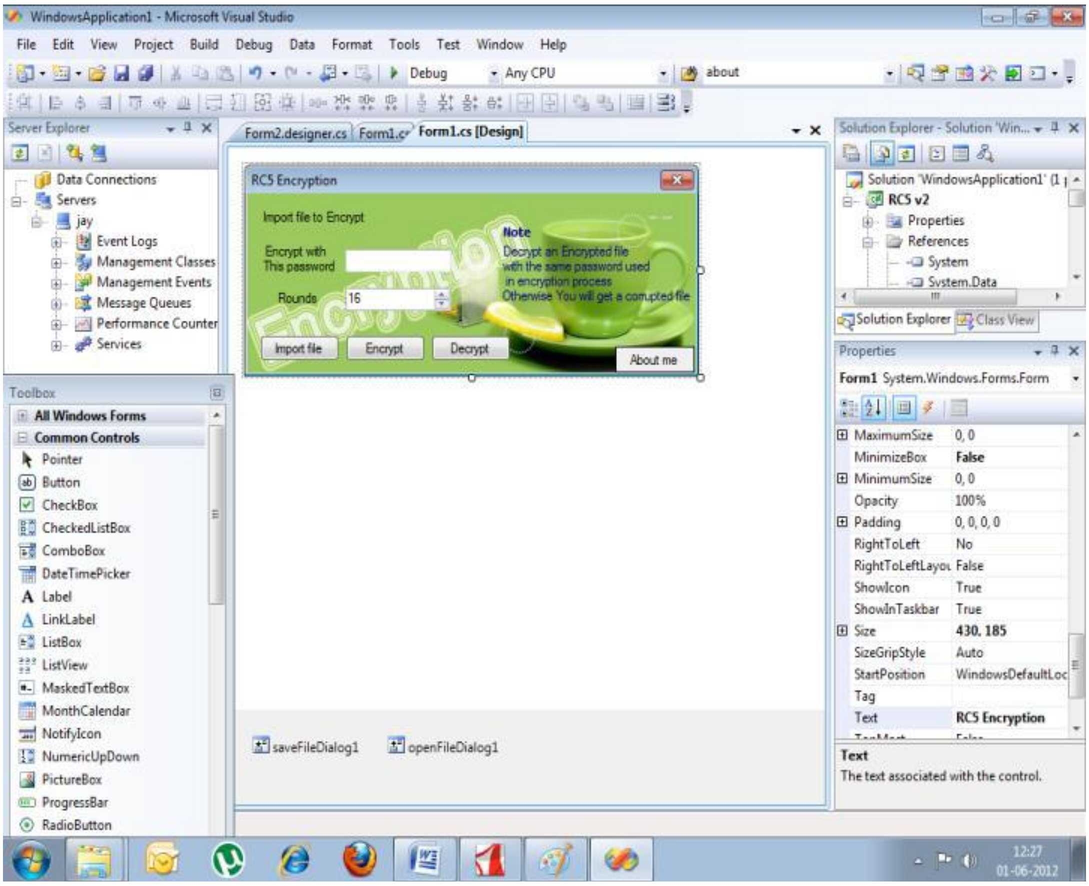
This view shows all the dependent containers of the selected master container.
According to the status of the containers different operations are possible.

Log - 128.250.28.101-9090 :: tcp://128.250.28.101:9090/Aneka

Level	Source	Message	Time
ⓘ	ExecutionService.Execute	ExecutionService: completed execution	13/09/2010 12:22 PM
ⓘ	ExecutionService.Execute	ExecutionService: starting execution	13/09/2010 12:22 PM
ⓘ	StackBuilderSink._PrivatePro...	Start executing task...	13/09/2010 12:22 PM
ⓘ	ExecutionService.Execute	ExecutionService: completed execution	13/09/2010 12:22 PM
ⓘ	ExecutionService.Execute	ExecutionService: starting execution	13/09/2010 12:22 PM
ⓘ	StackBuilderSink._PrivatePro...	Start executing task...	13/09/2010 12:22 PM
ⓘ	ExecutionService.Execute	ExecutionService: completed execution	13/09/2010 12:22 PM
ⓘ	ExecutionService.Execute	ExecutionService: starting execution	13/09/2010 12:22 PM

Fig 2: Aneka Container Logging (Real time monitoring and log archives)

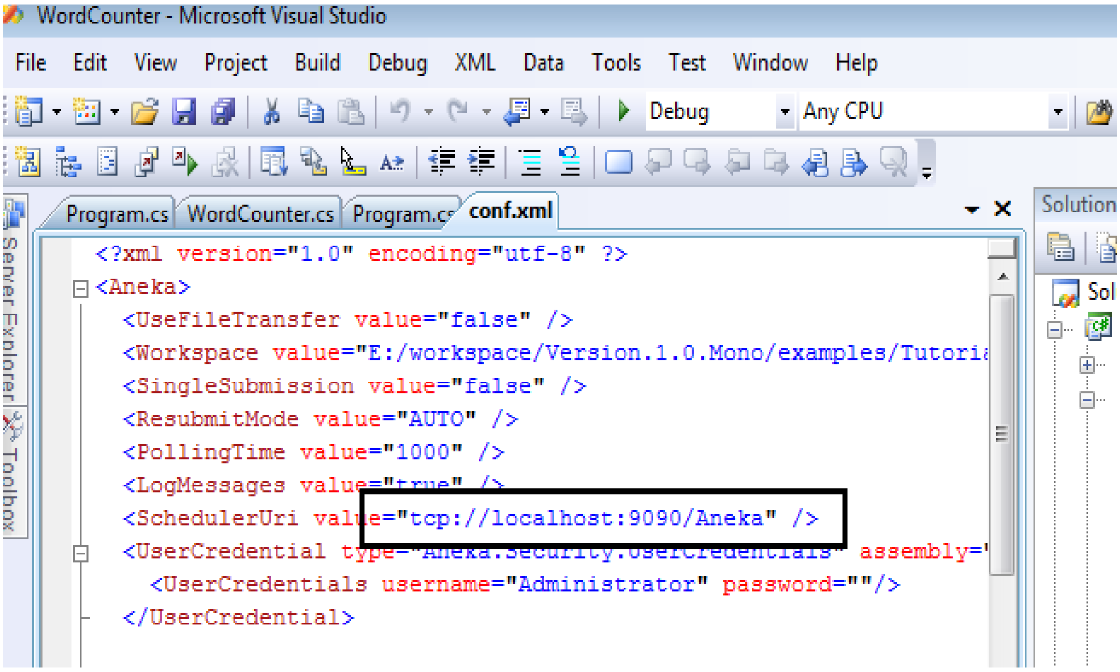
A. RC5 Developing Environment



MaximumSize	0, 0
MinimizeBox	False
MinimumSize	0, 0
Opacity	100%
Padding	0, 0, 0, 0
RightToLeft	No
RightToLeftLayou	False
ShowIcon	True
ShowInTaskbar	True
Size	430, 185
SizeGripStyle	Auto
StartPosition	WindowsDefaultLoc
Tag	
Text	RC5 Encryption

Text
The text associated with the control.

Fig 3: Development at Visual Studio Environment

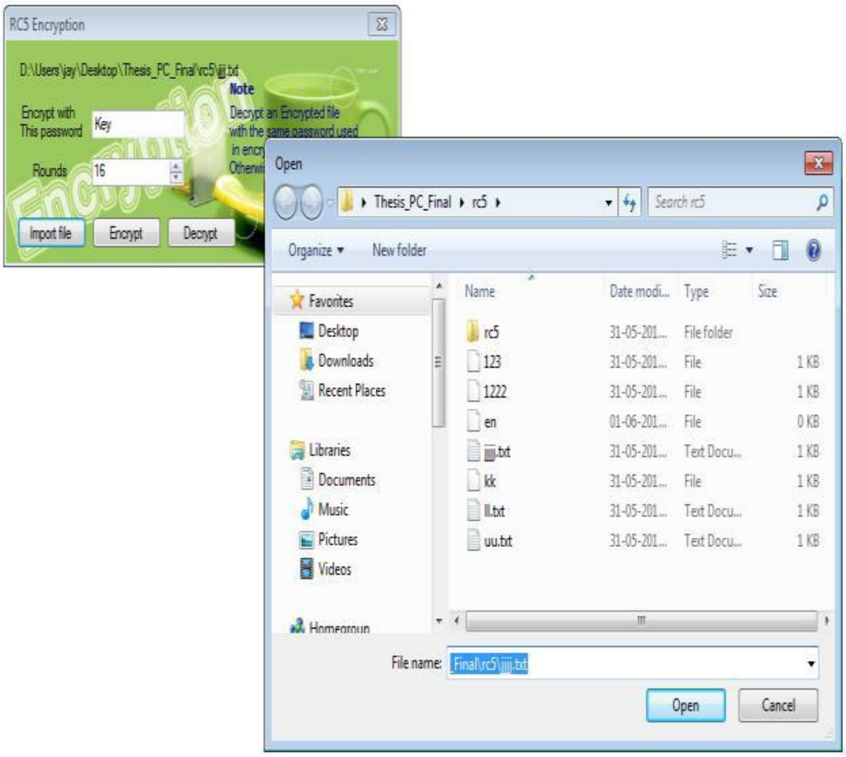

WordCounter - Microsoft Visual Studio
File Edit View Project Build Debug XML Data Tools Test Window Help
Debug
Any CPU
Program.cs
WordCounter.cs
Program.cs
conf.xml
Server Explorer
Toolbox
Solution
Sol

```
<?xml version="1.0" encoding="utf-8" ?>
<Aneka>
  <UseFileTransfer value="false" />
  <Workspace value="E:/workspace/Version.1.0.Mono/examples/Tutoria
  <SingleSubmission value="false" />
  <ResubmitMode value="AUTO" />
  <PollingTime value="1000" />
  <LogMessages value="true" />
  <SchedulerUri value="tcp://localhost:9090/Aneka" />
  <UserCredential type="Aneka.Security.UserCredentials" assembly='
    <UserCredentials username="Administrator" password=""/>
  </UserCredential>
```

Fig 4: Deployment Environment at IP lavel

Select the conf.xml file & write as
<SchedulerUri Value =” tcp://10.10.21.110:9090/Aneka” (ip address of master container)
In place of
<SchedulerUri Value =” tcp://localhost:9090/Aneka”

B. Running and Encryption Wizard



D:\Users\jay\Desktop\Thesis_PC_Final\rc5\jjjj.txt

Encrypt with This password: Key

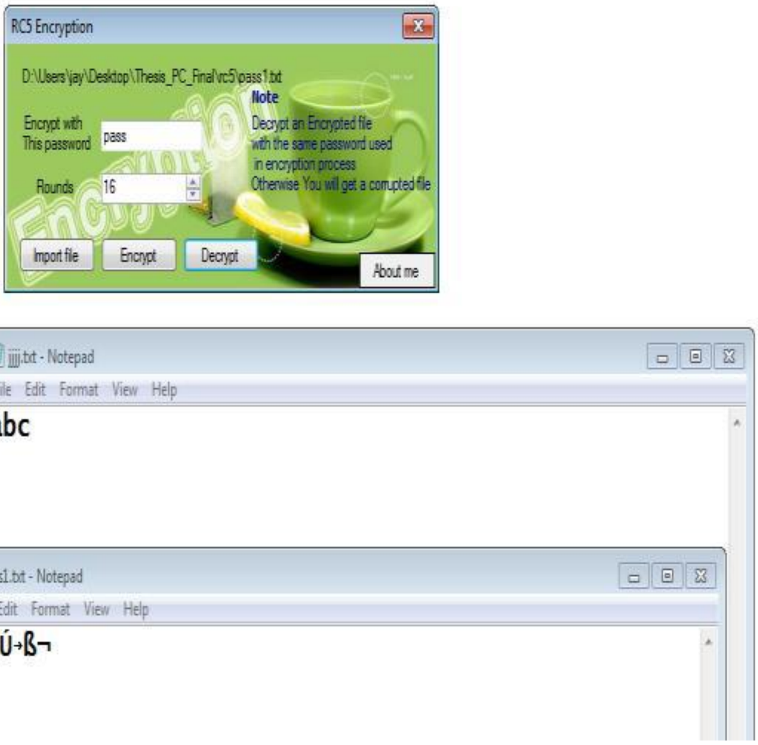
Rounds: 16

Note
Decrypt an Encrypted file with the same password used in encry… Otherwi…

Name	Date modi...	Type	Size
rc5	31-05-201...	File folder	
123	31-05-201...	File	1 KB
1222	31-05-201...	File	1 KB
en	01-06-201...	File	0 KB
jjjj.txt	31-05-201...	Text Docu...	1 KB
kk	31-05-201...	File	1 KB
ll.txt	31-05-201...	Text Docu...	1 KB
uu.txt	31-05-201...	Text Docu...	1 KB

File name: Final\rc5\jjjj.txt

Fig 5: Selection of File for Encryption



D:\Users\jay\Desktop\Thesis_PC_Final\rc5\pass1.txt

Encrypt with This password: pass

Rounds: 16

Note
Decrypt an Encrypted file with the same password used in encryption process Otherwise You will get a corrupted file

abc

¦œ╕Ú→ß¬

Fig 6: Original file Text & Encrypted File Text

VIII. CONCLUSION

We believe that data storage security in Cloud Computing is an emerging computing paradigm, allows users to share resources and information from a pool of distributed computing as a service over Internet. Cloud storage is much more beneficial and advantageous than the earlier traditional storage systems especially in scalability, cost reduction, portability and functionality requirements. Cloud Computing is an area full of challenges and of paramount importance, is still in its infancy now, and many research problems are yet to be identified. System uses encryption/decryption keys of user‘s data and stores it on remote server. Each storage server has an encrypted file system which encrypts the client‘s data and store. Cryptographic techniques are used to provide secure communication between the client and the cloud. The system ensures that the client‘s data is stored only on trusted storage servers and it cannot be accessed by administrators or intruders. In particular, we consider the task of allowing a third party auditor (TPA), on behalf of the cloud client, to verify the integrity of the dynamic data stored in the cloud. TPA can perform multiple auditing tasks simultaneously. Here Work is focuses on RC5 Encryption Algorithm for stored data in cloud. Resulted encrypted method is secure and easy to use.

REFERENCES

[1] P. Mell and T. Grance, “Draft NIST working definition of cloud computing”.

[2] A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica,

M. Zaharia, “Above the clouds: A berkeley view of cloud computing,” University of California, Berkeley, Tech. Rep, 2009.

[3] G.Ateniese et al., ―Provable Data Possession at Untrusted Stores,‖ Proc. ACM CCS ‗07, Oct. 2007, pp. 598–609.

[4] Balakrishnan S, Saranya G, et al. (2011). Introducing Effective Third Party Auditing (TPA) for Data Storage Security in Cloud, International Journal of Computer Science and Technology, vol 2(2), 397–400.

[5] Yu, S., Wang, C., Ren, K., Lou, W.: Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing. In: Proc. IEEE INFOCOM. pp. 534–542 (2010)

[6] Mohammed A. AlZain, Ben Soh and Eric Pardede AlZain, M.A.; Soh, B.; Pardede, E. A New Approach Using Redundancy Technique to Improve Security in Cloud Computing. International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), 2012.

[7] Akhil Behl, Emerging Security Challenges in Cloud Computing . Congress on Information and Communication Technologies (WICT), 2011 World.

[8] Jianfeng Yang, Zhibin Chen, Cloud Computing Research and Security Issues. 2010 International Conference on Computational Intelligence and Software Engineering (CiSE).

[9] Panagiotis Kalagiakos, Panagiotis Karampelas, Cloud Computing Learning, Application of Information and Communication Technologies (AICT), 2011 5th International Conference.

[10] Tharam Dillon, Chen Wu and Elizabeth Chang. Cloud Computing: Issues and Challenges. 2010 24th IEEE International Conference on Advanced Information Networking and Applications.

[11] Wentao Liu, Research on Cloud Computing Security Problem and Strategy. 2012 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet).

[12] Cong Wang, Qian Wang. Toward Secure and Dependable Storage Services in Cloud Computing. Ieee transactions on services computing, vol. 5, no. 2, april-june 2012.

[13] Amazon.com, “Amazon s3 availability event: July 20, 2008,” Online at http://status.aws.amazon.com/s3-20080720.html, 2008.

[14] M. A. Shah, R. Swaminathan, and M. Baker, “Privacypreserving audit and extraction of digital contents,” Cryptology ePrint Archive, Report 2008/186, 2008.

[15] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, “Enabling public verifiability and data dynamics for storage security in cloud computing,” in *Proc. of ESORICS’09, volume 5789 of LNCS*. Springer-Verlag, Sep. 2009, pp. 355–370.

[16] R. C.Merkle, “Protocols for public key cryptosystems,” in *Proc.of IEEE Symposium on Security and Privacy*, Los Alamitos, CA, USA, 1980.