International Journal of Advanced Computer Research (ISSN (print): 2249-7277 ISSN (online): 2277-7970)
Volume-2 Number-4 Issue-6 December-2012

Securing Storage Data in Cloud Using RC5 Algorithm

Jay Singh[1], Brajesh Kumar[2], Asha Khatri[3]
CDSE Indore[1,2], MITM, Indore[3]

Abstract

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-scale computing resources to effectively integrate, and to computing resources as a service to users. 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. Cloud computing effectively the actual separation of physical and virtual services, a variety of business services reduced costs, improved utilization of network resources. Cloud computing is a technology that uses the internet or intranet and central remote servers to maintain the data and applications. This technology allows for efficient computing by centralizing storage, memory, processing and bandwidth. Here Work is focuses on RC5 Encryption Algorithm for stored data in cloud. Resulted encrypted method is secure and easy to use; it is fulfilling the needs of cloud users and providers.

Keywords

Cloud computing, security, Encryption, storage

1. Introduction

Cloud Computing is innovation that uses advanced computational power and improved storage capabilities. Cloud computing is a new processing scheme in which computer processing is performed in the network. This means that users need not concern themselves with the processing details. Although Cloud computing enables flexible and agile computing which is impossible with existing systems.

2. Basic service Models

According to service model, cloud computing can be categorized (as shown in Figure 1) into three main categories:

i. Infrastructure-as-a-Service (IaaS)
ii. Platform-as-a-Service (PaaS)
iii. Software-as-a-Service (SaaS)

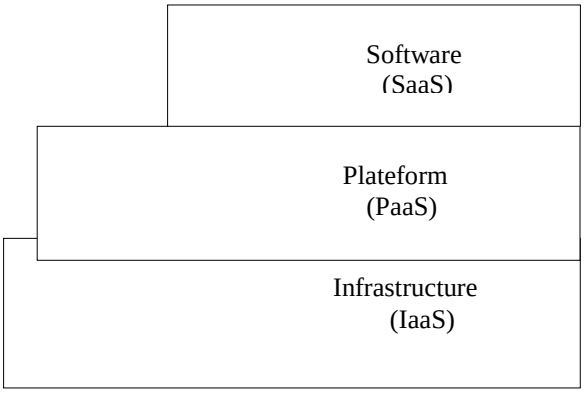


Figure 1: cloud model

3. Layers in Cloud

The Internet functions through a series of network protocols that form a stack of layers, as shown in the figure 2. Once an Internet connection is established among several computers, it is possible to share services within any one of the following layers [Pana11].

CLIENT
APPLICATION
PLATFORM
INFRASTRUCTURE
SERVER

Figure 2: Cloud layer

4. Security as Major Issues

To preventing the system from outside world, so that no one can damage or change the system and system can serve its services continuously. The most damaging aspect is the loss of data and software. There is different types of source are there, they can damage like computer viruses, computer hacking and denial of service attacks have become more common.
There are multiple security issues for cloud computing and it encompasses many technologies including networks, databases, operating systems,

virtualization, resource scheduling, transaction management, load balancing, concurrency control and memory management[Akhi11].

5. Information Security Issue of Cloud Computing

There is a critical need to securely store, manage, share and analyze massive amounts of data and to improve the quality of services. Because of the critical nature of the applications, it is important that clouds to be secure. The major security challenge with clouds is that the owner of the data may not have control of where the data is placed [Chang10]. There are different Security Issues shown in figure 3.

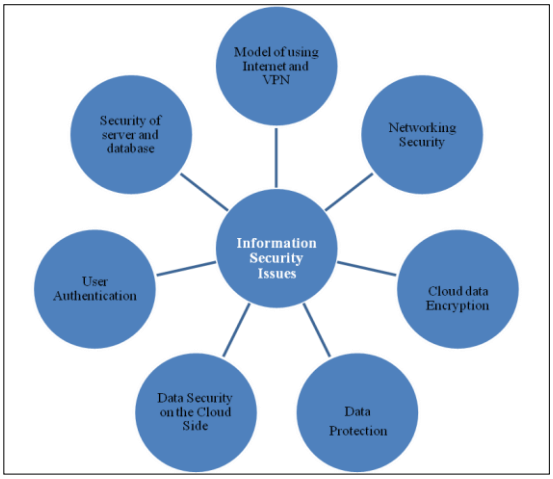


Figure 3: Security Issues

6. 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 [Jian10].

Encryption plays a big role in fulfilment as many policies require specific data elements to be encrypted. This type of requirement is present in GLBA, PCI DSS and HIPAA. 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.

7. Problems Definition

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, such as Hadoop and Sector. In the past, there is no known way to completely handle encrypted data, unless the cloud data is only used for simple storage [Went12]. 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. The user does not have direct access to the software to fix the problems while something goes wrong in any application and its valuable data.

Proposed Solution

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 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.

8. Deploying RC5 Encryption Algorithm at Manjrasoft Aneka2.0 Cloud Enviroment

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.

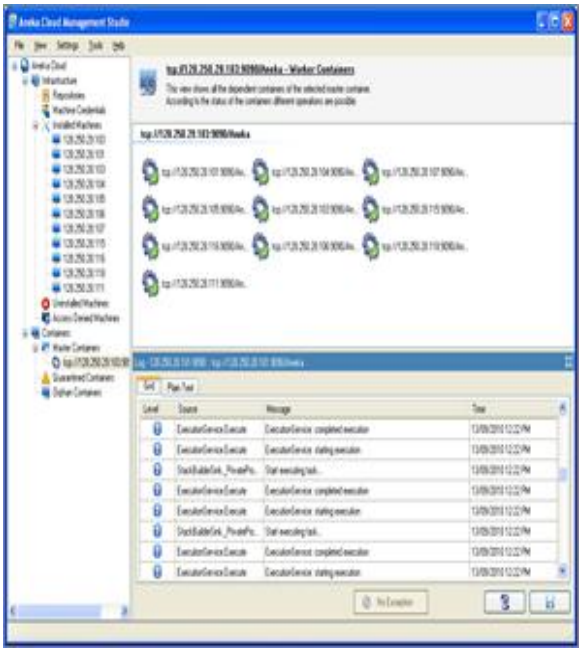


Figure 4: Aneka Container Logging (Real time monitoring and log archives)

RC5 Developing Environment

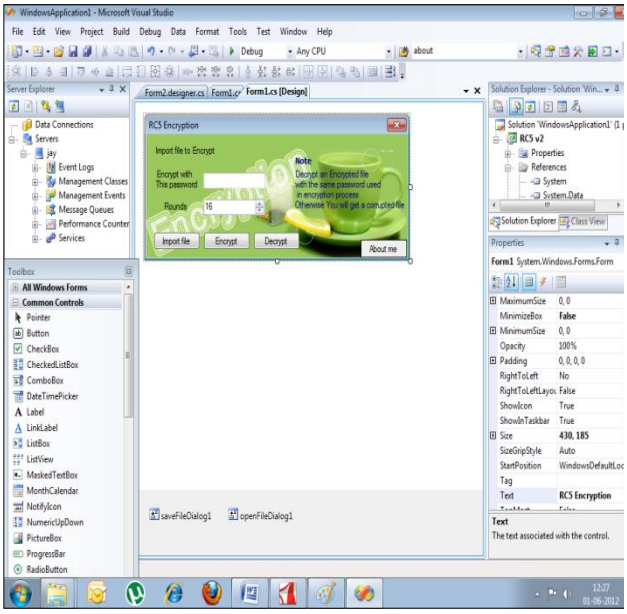


Figure5: Development at Visual Studio Environment

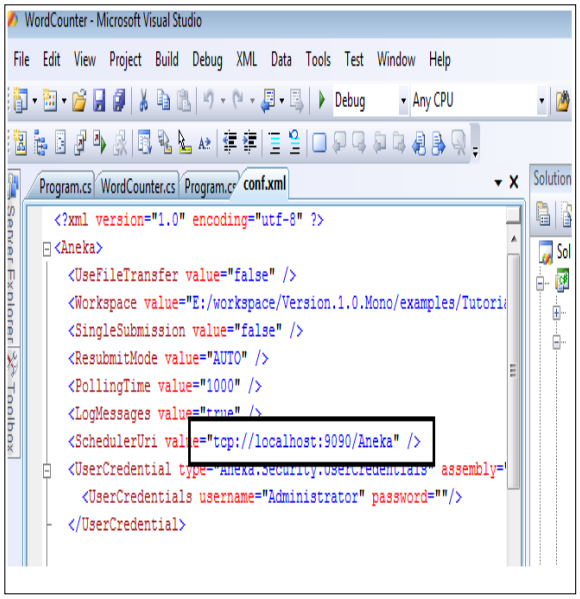


Figure 6: Deployment Environment at IP lavel

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"

Running and Encryption Wizard

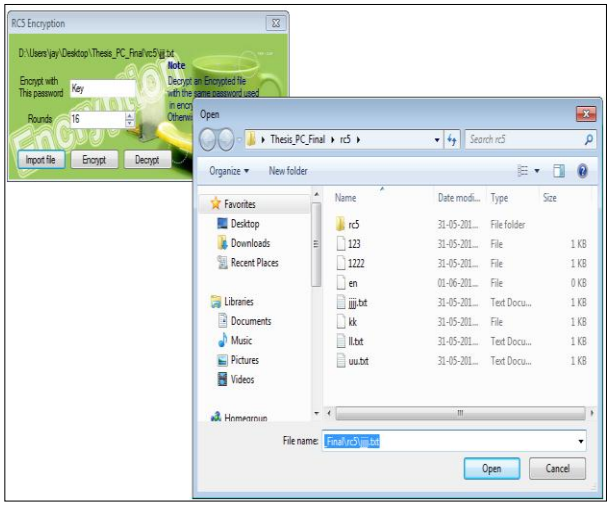


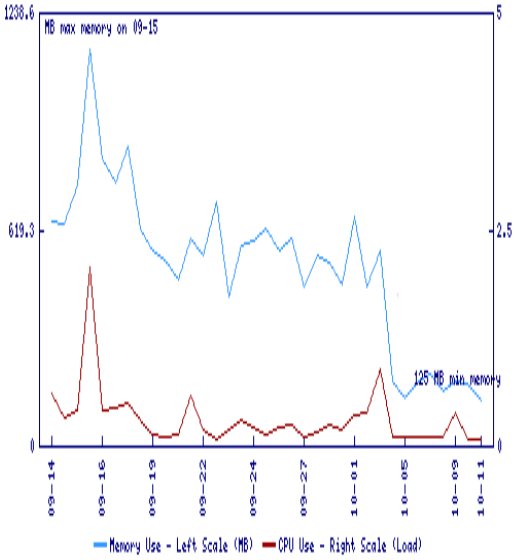
Figure 7: Selection of File for Encryption

Figure 8: Original file Text & Encrypted File Text

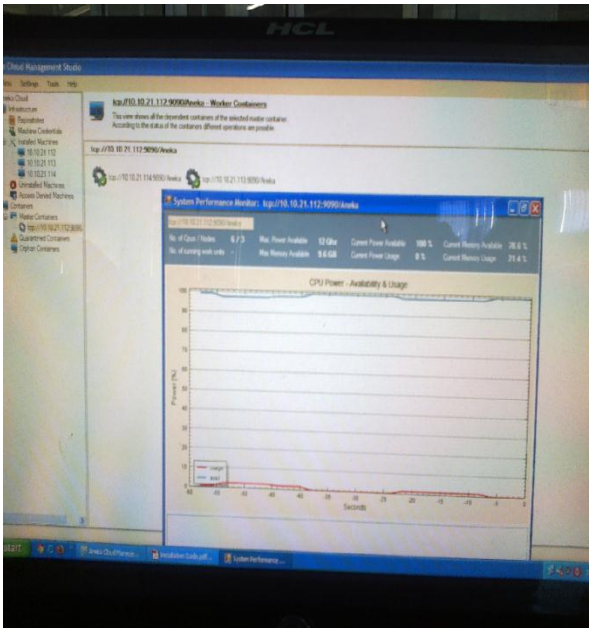
9. Result Analysis

Here we are comparing the actual result with Amazon s3 storage service. Amazon S3 (Simple Storage Service) is an online storage web service which is offered by Amazon Web Services. Amazon S3 provides storage through web services interface REST.

Amazon S3 service graph



Aneka 2.0 Service Graph



Conclusion of result: In Aneka service graph, getting better performance.

10. Conclusion and Future Scope

We believe that data storage security in 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. We envision several possible directions for future research on this area. 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.

References

[1] [Akhi11] Akhil Behl, Emerging Security Challenges in Cloud Computing . Congress on Information and Communication Technologies (WICT), 2011 World.

[2] [Chang10] Chang-Lung Tsai Uei-Chin Lin Allen Y. Chang Chun-Jung Chen. Information Security Issue of Enterprises Adopting the Application of Cloud Computing. National Science Council and Chinese Culture University of Taiwan, R.O.C.

[3] [Jian10] Jianfeng Yang, Zhibin Chen, Cloud Computing Research and Security Issues. 2010 International Conference on Computational Intelligence and Software Engineering (CiSE).

[4] Junfeng Tian, Zhijie Wu. A Trusted Control Model of Cloud Storage.2012 International Conference on Computer Distributed Control and Intelligent Enviromental Monitoring.
[5] [Pana11] Panagiotis Kalagiakos, Panagiotis Karampelas, Cloud Computing Learning, Application of Information and Communication Technologies (AICT), 2011 5th International Conference.
[6] [Thar10] Tharam Dillon, Chen Wu and Elizabeth Chang. Cloud Computing: Issues and Challenges. 2010 24th IEEE International Conference on Advanced Information Networking and Applications.
[7] [Went12] Wentao Liu, Research on Cloud Computing Security Problem and Strategy. 2012 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet).
[8] [Cong12] 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.
[9] [Eman12] Eman M.Mohamed. Cloud and Mobile Computing Track Randomness Testing of Modem Encryption Techniques in Cloud Environment. The 8th International Conference on INFOrmatics and Systems (INFOS2012).
[10] [Eric12] 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.
[11] [Guru12] Gurudatt Kulkarni & Jayant Gambhir, A Security Aspects in Cloud computing. 2012 IEEE 3rd International Conference on Software Engineering and Service Science (ICSESS).