ISSN:0975-9646

Implementation of RSA RC5 Algorithm in Cloud

Pallavi Pandey[#1], Priyanka Dhasal[*2], Rakesh Pandit[#3]

[#]*IT – IT Department, RGTU- RGTU University*
PCST, Indore (M.P.), India

[*]*Patel College of Science and Tecnology*
PCST, Indore (M.P.), India

***Abstract*— 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. RC5 RSA Algorithm is implemented in Aneka Cloud Environment. Resulted encrypted method is secure and easy to use; it is fulfilling the needs of cloud users and providers. This model has important security services, including authentication, confidentiality and integrity.**

***Keywords* - Cloud computing, RC algorithm, Remote database, Encryption, Decryption**

I. INTRODUCTION

Cloud Computing is innovation that uses advanced computational power and improved storage. Cloud computing, is a new kind of computing model. It is extend of changing with the need. With the rapid development of the Internet, user's requirement is realized through the Internet, different from shifting with the need. In fact cloud computing is a kind of grid computing, distributed computing, and parallel computing. Its forefront is to provide secure, quick, well-situated data storage and net computing service centered by internet.

The characteristics of cloud computing is the virtualization, distribution and dynamically extendibility. Virtualization is the key quality. Most software and hardware have provided carry on to virtualization.

A. *Basic Service Model*

According to service model, cloud computing can be categorized into three main categories:

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

Computing is a virtual group of computing resources. It provides computing resources in the pool for users through internet. It provides a compulsory application program environment [4]. It can deploy, allocate or reallocate computing resource dynamically and keep an eye on the usage of resources. Cloud computing collects all the computing resources and manages them automatically through software.

B. 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. Sources of damage such as computer
viruses, computer hacking and denial of service attacks have become more common[2].

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.

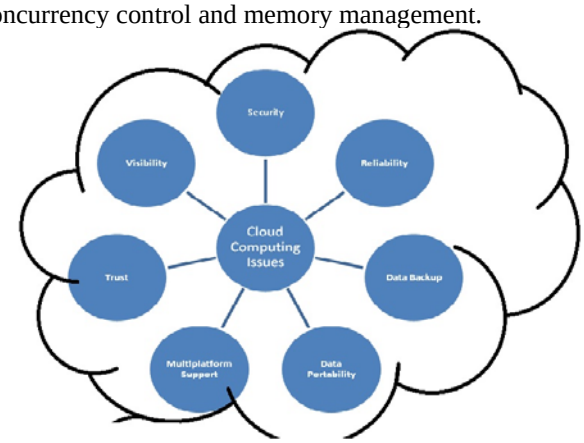

Fig. 1 Issues of cloud computing

II. LITERATURE SURVEY

For understanding different types of issues and resolving such issues, survey on various IEEE published paper are discussed. Related work papers are:

A. Cloud Computing Research and Development Trend.

In this research paper, Cloud computing is trying to build system that can bring lower costs, higher profits and more choice for large scale industry[1]. For engineers and developers are concerned, the advent of cloud computing will shrink to the development of comprehensive web centric development. The clouds will grow in size as soon as available bandwidth and the corresponding service model mature enough. Cloud computing will bring a revolutionary change in the Internet.

B. Cloud Computing Research and Security Issues.

In this paper, discussion is on fresh technology of cloud computing. It is describing definition and some existing issues. There is no doubt that the cloud computing is the development trend in the future. Cloud computing brings us the approximately infinite computing capability, good scalability, service on-demand and so on, also challenges at security, privacy, legal issues and so on.

C. Cloud Hooks: Security and Privacy Issues in Cloud Computing.

In this paper, emphasis is on cost and performance benefits of the cloud. Some fundamental security problems have receded into the background and been left unresolved. Determining the security of complex computer systems is also a long-standing security problem that overshadows large scale computing in general. Attaining the high assurance qualities in implementations has been a hard to pin down goal of computer security. Security of the cloud infrastructure relies on trusted computing and cryptography. Organizational data must be protected in a manner consistent with policies, whether in the organization's computing centre or the cloud[4].

D. Research on Cloud Computing Security Problem and Strategy.

This paper illustrates cloud concepts and demonstrates the cloud capabilities such as scalability, elasticity, low-cost, reliability and platform independent. The security problems in the cloud system are discussed. Cloud computing has a very fast rate of development and shows good prospects and great potential. The cloud computing is related to many areas of information management and services. The data privacy issue becomes more prominent than the traditional network because the data in the cloud computing environment is greatly dependent on the network and server.

E. Research of Cloud Computing Data Security Technology.

In this paper, discussion is on CLOUD COMPUTING DATA SECURITY PROBLEMS. Here designed a way of ensuring the transmission of user data security. There are other discussions related to:

- Security of data transmission
- Security of data migration
- Data reminisce

Data encryption can guarantee the confidentiality of the data, but cannot guarantee data integrity.

F. Secure Data Storage and Retrieval in the Cloud.

In this paper, presented a system that is allowing cooperating organizations to securely share large amounts of data. It is ensured that the organizations have a large common storage area by using Hadoop. Further, Hive to present users of system with a structured view of the data and to also enable them to query the data with a SQL like language. Here used a simple salted hash mechanism to authenticate users in the current version of system. There is the implementation of more sophisticated technique for authentication in future versions of cloud system.

G. *Secure Cloud Towards a Comprehensive Security Framework for Cloud Computing Environments.*

In this paper, discussion is on Security Framework for the Cloud. Also described its components, discussed existing solutions and identified possible approaches to deal with different security issues related to the cloud. There is other point of discussion is on:

- Authentication and Identity Management
- Access Control
- Policy Integration
- Service Management
- Trust Management

H. Ensuring Data Storage Security through A Novel Third Party Auditor Scheme In Cloud Computing.

This paper aims for designing a third party auditor scheme in cloud computing. Investigated the problem of data security in cloud data storage, which is essentially a distributed storage system. To ensure each data access in control and reduce the complexity of cloud computing, propose a scheme using RSA and Bilinear Diffie-Hellman techniques. They designed a message header and series of mechanism to accomplish the authentication function with the minimum cost. Confidentiality of users' access privilege and authentication accountability can be achieved. The analysis show that our proposed scheme is secure under standard cryptographic environment and efficient in cloud computing.

III. 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. Encryption is a powerful tool that can be used effectively to protect a user's confidential data in the cloud. Only then the user can confidently utilize cloud providers knowing that their confidential data is protected by encryption.

IV. 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.

V. DEPLOYING RC5 ENCRYPTION ALGORITHM AT MANJRASOFT ANEKA 2.0 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.

A. ANEKA 2.0 Cloud Development

From the diagram 5.1, after implementation of Aneka 2.0 Tool for cloud simulation, on master side, there is master container and other slave are connected.

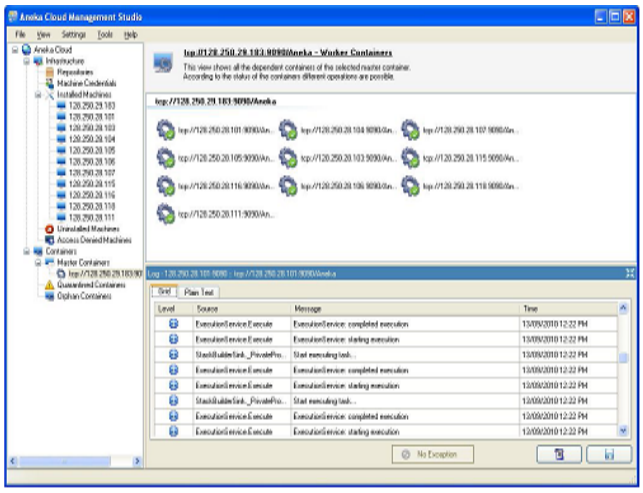

Fig. 2 Aneka cloud

B. RC5 Developing Environment

For developing RSA-RC5 algorithm,Visual Studio(dot net) frame work is used. From Diagram 5.2,it is development environment and RC5 algorithm is coded and form designed for GUI user interface.

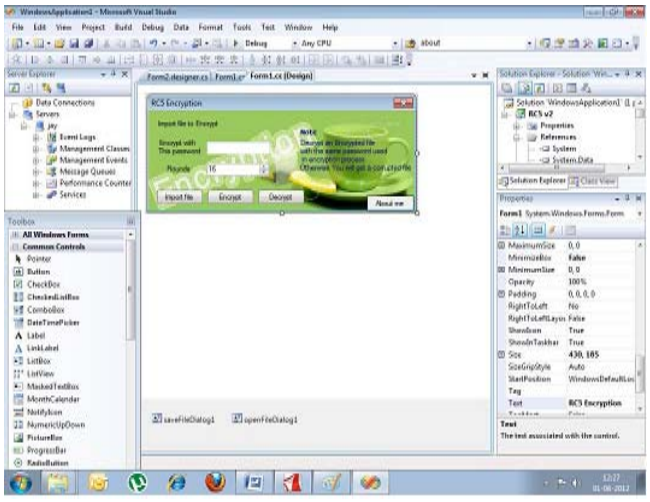

Fig. 3 RC5 development

C. Encryption Of Data With RC5 Algorithm

From the figure 5.3, password and no. of rounds for data encryption is selected and data is encrypted as plain text to cipher text.

Fig. 4 RC5 data encryption

D. *Implementation Of RC5 Algorithm in Cloud*

From the conf.xml file, in place of local host, replaced with server IP address. It is shown in figure 5.4.

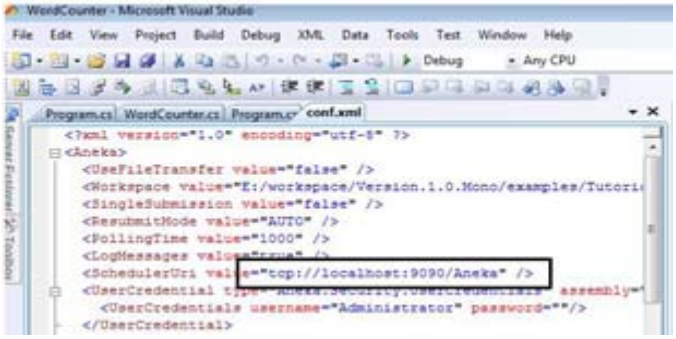

Fig. 5 .xml file

VI. 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 offered by Amazon Web Services. Amazon S3 provides storage through web services interface rest. Amazon S3 service graph.

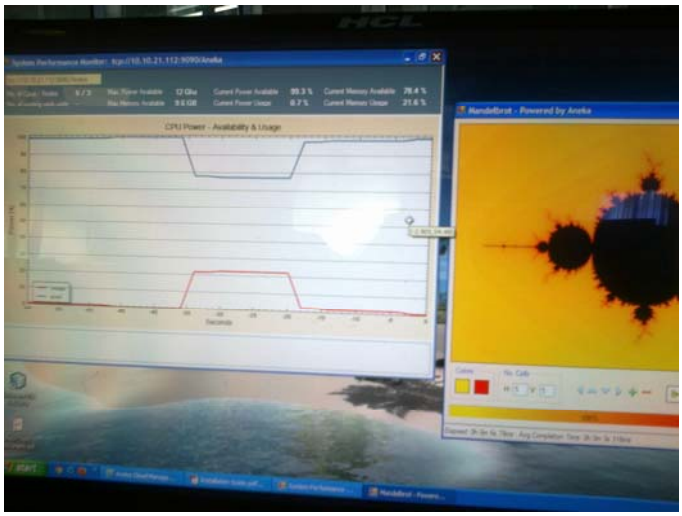

Fig. 6 Aneka Cloud Graph

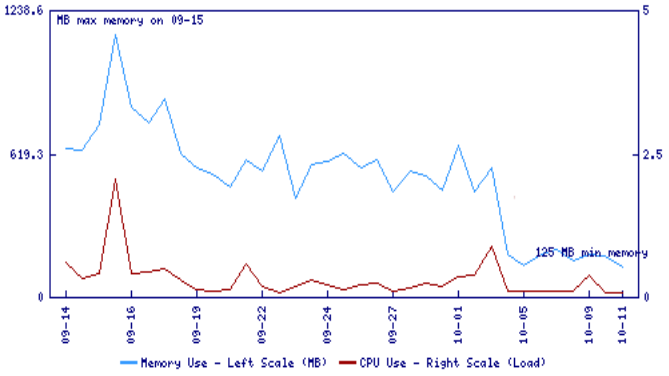

Fig. 7 Amazon S3 graph

TABLE I

COMPARISION OF ANEKA RC5 SERVICES WITH AMAZON S3

TOOL	CPU POWER		MEMORY	
	Available	Usage	Available	Usage
Aneka 2.0	100%	99.3%	78.6%	78.4%
Amazon S3	100%	92%	82%	51.2%
Saving		7.3%		27.2%

VII. CONCLUSION AND FUTURE WORK

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

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

[3] Cong Wang, Qian Wang. Toward Secure and Dependable Storage Services in Cloud Computing. *Proceedings of ieee transactions on services computing*, vol. 5, no. 2, April-June 2012.

[4] Eman M.Mohamed. Cloud and Mobile Computing Track Randomness Testing of Modem Encryption Techniques in Cloud Environment. *Proceedings of The 8th International Conference on INFOrmatics and Systems (INFOS2012)*

[5] 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. *Proceedings of International Conference on Cyber Security, Cyber Warfare and Digital Forensic. (CyberSec),* 2012.

[6] Gurudatt Kulkarni & Jayant Gambhir, A Security Aspects in Cloud computing. *Proceedings of 2012 IEEE 3rd International Conference on Software Engineering and Service Science (ICSESS).*

[7] Hassan Takabi, James B. D. Joshi, Gail-Joon Ahn. SecureCloud: Towards a Comprehensive Security Framework for Cloud Computing Environments. *Proceedings of 2010 34th Annual IEEE Computer Software and Applications Conference Workshops.*

[8] Jayant Baliga, Robert W. A. Ayre, Kerry Hinton, and Rodney S. Tucker. Green Cloud Computing: Balancing Energy in Processing, Storage, and Transport. *Proceedings of the IEEE , 2011*

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

[10] Li, Jing-min. Research of distributed database system based on Hadoop. *Proceedings of 2010 2nd International Conference on Information Science and Engineering (ICISE).*

[11] Junfeng Tian, Zhijie Wu. A Trusted Control Model of Cloud Storage. *Proceedings of 2012 International Conference on Computer Distributed Control and Intelligent Enviromental Monitoring.*

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

[13] J.C.R. Licklider, Intergalactic Computer Network. http://en.wikipedia.org/wiki/Intergalactic_Computer_Network.

[14] Lixin Fu, Cloud computing hosting. *Proceedings of 2010 3rd IEEE International Conference Computer Science and Information Technology (ICCSIT).*