Design And Implement A Scheme To Secure Data Storage In Cloud Computing Environment

Mittal J. Patel[#1], Asst Prof. Dhaval Patel[#2]
[#1]P.G Student Department Of Computer Engineering, HasmukhGoswami College Of Engineering, Ahmedabad,India
[#2]Assistant Professor Department Of Computer Engineering, HasmukhGoswami College Of Engineering,Ahmedabad,India

***Abstract* - Cloud Computing is technology for next generation Information and Software enabled work that is capable of changing the software working environment. It is interfacing the large-scale computing resources to effectively communicate to computing resources as a service to users. This technology allows to the users to use applications without installation and access their personal files and application at any computer with internet or intranet access. Cloud computing is a technology that uses the internet or intranet and central remote servers to maintain the data and application. This technology allows for efficient computing by memory, centralizing storage, bandwidth and processing. Here work focuses on RC5 Encryption Algorithm for stored data in cloud. RC5 is sufficient to make both differential and linear cryptanalysis impractical. I give differential attacks better by up to a factor of 512. Also we can show that RC5 has several weak keys with respect to differential attacks.**

***Keywords* - RC5, Differential Attack, N's complement**

I. INTRODUCTION

Cloud computing is emerging field because of its least cost, high availability, performance and many others. In cloud computing, the data will be stored in storage provided by service providers. Cloud computing is a compilation of exiting techniques and technology,packaged within a new infrastructure paradigm that offers elasticity, improved scalability, faster startup time, reduced management costs, business agility and just in time availability of resources. Cloud is kind of centralized database where many organizations and peoples stores their data.

In cloud user is provided services by CSP(Cloud service Provider) based on pay per use.Cloud computing provides a computer user access to Information Technology (IT) services which contains data storage, servers, applications without requiring an understanding of the technology.

Cloud Computing is dynamically delivers everything as a service over the internet basedon user demand, such as network, operating system, storage, hardware, software, and resources.

II. ARCHITECTURE OF CLOUD COMPUTING

Cloud computing is a style is a computing paradigm in which real time scalable resource as files,data,programs,hardware and third party services can be accessible from a web browser.Fig. shows service model for cloud infrastructures.

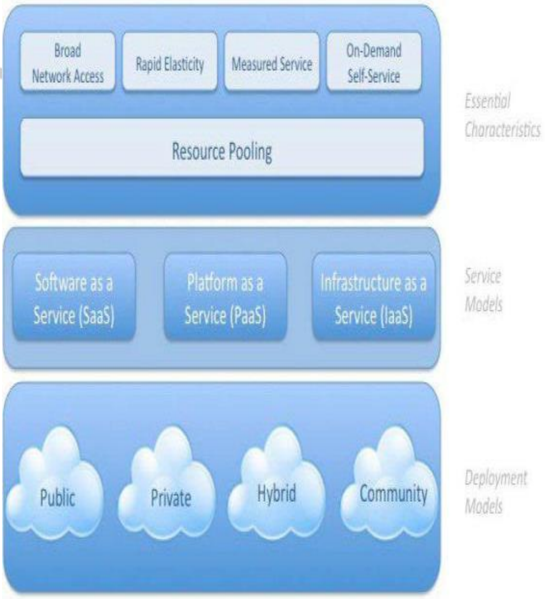

Figure 1 : Cloud computing Architecture

In this Architecture, users and Service Provider of cloud interact between each others. User can sends a request to service provider as per their requirements and service Provider will give response according to QoS requirement. There are mainly three types of Services models in cloud computing.

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

Infrastructure as a Service(IaaS)

Infrastructure as a Service is a cloud computing service model in which Hardware is Virtualized in the cloud. In this particular model, the service vendor owns the equipment: Servers, Storage, Network Infrastructure. Its main purpose is to avoid housing, purchasing and managing the basic hardware and Software infrastructure components. Infrastructure-as-a-Service like Amazon Web Services provides virtual server instances with unique IP addresses and blocks of storage on demand. Infrastructure as a Service is sometimes referred to as Hardware as a Service (HaaS).[3]

Software as a Service(SaaS)

This is where users simply make use of a web-browser to access software that others have developed and offer as a service over the web[2]. At the SaaS level, users do not have control or access to the underlying infrastructure being used to host the software. Google Docs4 are popular examples that use the SaaS model of cloud computing.

Platform as a Service(PaaS)

This is where applications are developed using a set of programming languages and tools that are supported by the PaaS provider. PaaS provides users with a high level of abstraction that allows them to focus on developing their applications and not worry about the underlying infrastructure. Google App Engine5 and Microsoft Azure6 are popular PaaS examples.

Cloud Computing Deployment Models

There are four types of cloud computing deployment models.

1.Public Cloud
2.Private Cloud
3.Community cloud
4.Hybrid Cloud

1. Public Cloud - The cloud computing resource is shared outside, anyone can use it and some payment may be need.The customer has no visibility and control over where the computing infrastructure is hosted.

2.Private Cloud - It is opposite to public cloud, private cloud's resource is limit to a group of people, like a staff of a company etc.

3. Community cloud - This is a special cloud to make use of cloud computing features. More than one community shares a cloud to share and reduce the cost of computing system. Data storage in cloud offers so many benefits to users.

4. Hybrid Cloud - Hybrid clouds combine both public and private cloud models. They can help to provide on-demand, externally provisioned scale. The ability to augment a private cloud with the resources of a public cloud can be used to maintain service levels in the face of rapid workload fluctuations.

III. PROBLEM STATEMENT

The proposed scheme has few important characteristics:

1) It allows the owner to outsource important data to a Cloud service Provider, and perform full block-level operations on the outsourced data, i.e., insertion, deletion, append and block modification.

2) It ensures that authorized users (i.e., those who have the right to access the owner's file) receive the latest version of the outsourced data,

3) It enables indirect mutual trust between the owner and the Cloud service provider.

4) It allows the owner to grant or revoke access to the outsourced data.

IV. PROPOSED ALGORITHM

This algorithm has a modified Feistel structure and presented symbolically as Proposed RC5 – w / r / b. w indicates 32 bits as the size of word, r denotes the no. of round. If the size of block is 128 bits, then r is 20 and b means 16 byte as the number of a key. The operations used in Proposed RC5 are defined as followings.

- A+B integer addition modulo 2w
- A-B integer subtraction modulo 2w
- A⊕B bitwise ex-or of w-bit words
- A<<B rotation of the w-bit word A to the left by the amount given by the least significant log w bits of B
- A>>B rotation of the w-bit word A to the right by the amount given by the least significant log w bits of B

Encryption algorithm of proposed RC5-w/r/b

The pseudo code of the cryptographic algorithm of RC5 - w/r/b is as followings.

Input: Plain text stored in w-bit input registers A, B

No. of r rounds w-bit round keys k [0,…,2r + 3]

Output: Cipher text stored in [A, B, C, D]
Procedure:

```
Step=1Initialization of Parameter
        W=32 bit
        R=user input [assume12 default]
        B=32/64/128
        u=0
Step=2 Find Key using B where key is in binary form
Step=3 Add u the purity Unicode to the key
For(i=0,i<=(b-1),i++)
        {
                If(k[i]==1)
                u++;
                        }
Step=4   Check the purity checker value
N=M(u/2) = modulo(u/2)
Step=5   Add checker to key
         N's complement with the key
Step=6   Key is ready for cipher text.
Step=7   Load w-bit input registers A, B
Step=8   Perform a mixed(X-or,  left rotation, sum)
A = A + k[0];
B = B + k[1];
for i = 1 to r do
A = ((A⊕ B) <<< B) + k[ 2 * b ];
B = ((B⊕A) <<< A) + k[ 2 * b + 1];
```

Decryption algorithm of proposed RC5-w/r/b

Input: Cipher text stored in two w-bit input registers A, B
No. of r rounds w-bit round keys k [0,…,2r + 3]
Output: Plain text stored in A, B
Procedure:

```
Step=1    Initialization of Parameter
        W=32 bit
        R=user input [assume 12 default]
        B=32/64/128
        u=0
Step =2 Find Key using B where key is in binary form
Step=3   Add "u" the purity Unicode to the key
For(i=0,i<=(b-1),i++)
{
        if(k[i]==1)
        u++; }
Step=4   Check the purity checker value
        N = M(u/2) = modulo(u/2)
Step=5   Add checker to key
N's complement with the key
Step=6   Key is ready for cipher text.
Step=7 Load 2 w-bit input registers A,B
Step=8Perform a mixed(X-or, left rotation, sum)
for i = r down to 1 do
B = (( B – S[2 * b+ 1]) >>> A)⊕ A;
A = (( A – S[2 * b]) >>> B)⊕ B;
B = B – k[1];
A = A – k[0];
```

The encryption & decryption of proposed RC5 makes cipher text and plain text after carrying out twenty rounds repeatedly with cipher text and plain text in the Two storages (A, B) per 32 bit word.

After doing four words round function, it operates left / right rotate per word with parallel operation as shown in the above pseudo code. Before and after executing the round functions, it executes round key and add / subtract operations.

RC5 has differntial Attack so I insert the purity uicode and Purity Checker in proposed algorithm.The major advantage of the Purity Unicode and Purity Checker as follow,

1. Purity Unicode: key Management has 64/32 bit unique key where Purity Unicode will count the number of 1’s in key and calculate 1’s or 0’s.
2. Purity Checker: It will be either 1’s complement or 0’s complement of the key 1’s and 0’s will be decide on basis of Purity Unicode.

V. CONCLUSION

RC5 is sufficient algorithm to make both differential and linear cryptanalysis impractical. We analyze differential attacks better by up to a factor of 512 bits. Also we show that RC5 has several weak keys with respect to differential attacks. This weakness relies on the structure of the cipher and not on the key schedule. Finally We discuss some possible extensions of attacks and possible modifications of RC5 in order to improve the resistance against differential attacks.

VI. REFERENCES

[1] Mohiuddin Ahmed, Abu Sina Md. Rajuchowdhury, Mustaq Ahmed, Md. Ahmudul Hasan Rafee, “An Advanced Survey on Cloud Computing and State-of-the-art Research Issues” www.IJCSI.org

[2] Danwei chen, Yanjun He, “A Study on Secure Data Storage Strategy in cloud computing”

[3] Nirkshetri, Associate Professor, The University of North Carolina-Greensboro, USA, “Privacy and Security issues in cloud computing” PAGES1 to 23

[4] Traian Andrei, “Cloud Computing Challenges and Related Security Issues” http://www.cse.wustl.edu/~jain/cse571-09/ftp/cloud.pdf

[5] Rajesh Pipload, Umesh Kumar Singh, “An overview and Study of Security Issues &
a. Challenges in cloud Computing” www.ijarcsse.com

[6] Pankaj Arora, Rubal Chudhry Wadhawan Er. Satider Pal Ahuja, “Cloud Computing Security Issues in Infrasture as a service”

[7] William Stalling, “Cryptography and Network Security” Principle and Practice, Fifth Edition, Pearson Education.

[8] Atul Kahate, “Cryptography and Network Security”, Second Edition, Published by TATA McGraw Hill Education Private Limited.