IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
e-ISSN: 2278-2834,p- ISSN: 2278-8735.Volume 9, Issue 1, Ver. V (Feb. 2014), PP 43-47
www.iosrjournals.org

Security Issues with Implementation of RSA and Proposed Dual Security Algorithm for Cloud Computing

Uma Naik[1], V. C. Kotak[2]
[1]*(Electronics, Shah & Anchor Kutchhi Engineering College, Mumbai, India)*
[2]*(Electronics, Shah & Anchor Kutchhi Engineering College, Mumbai, India)*

Abstract : *The concept of data storage allowed to think us on security algorithms to get the relevant data sent and received without any mis-transit in between. For this related security algorithms are existing for ensuring the security of data been encrypted and decrypted. The basic RSA algorithm is been implemented and based on the same further dual security algorithms are proposed. Further expansion of basic algorithm based on security fruitful levels of security algorithms can be implemented.*

Keywords :*Data storage, Security algorithms, Data Security, Encryption Algorithms, RSA, Dual security.*

I. INTRODUCTION

Data Storage through Internet computing technology is known as Cloud Computing. This approach is emerging due to time, cost, distributed complex sourcing, faster delivery of innovation and increasing complexity. In this technology, service providers provide storage for data along with services. The contents in this paper will focus on the various issues and possible solution to data security related issues.

II. CLOUD SERVICES

A Cloud Client consists of computer hardware and/or computer software that relies on computing for application delivery[1].

Three different broad service models for internet computing:

-Software as a Service (SaaS), are applications over internet[1][3][10].

-Platform as a Service (PaaS), deliver a computing platform where the developers can develop their own applications[1][3][10]

-Infrastructure as a Service (IaaS), where a set of virtualized computing resources, customers deploy and run their own software stacks to obtain services. Current examples are Amazon Elastic Compute Cloud (EC2) and Simple Storage Service (S3)[1][3][10]

It also differentiates computing offerings by scope[1][3][10].

- Private clouds
- Public clouds
- Hybrid clouds

III. SECURITY ISSUES IN CLOUD COMPUTING

Due to many characteristics , has effect on IT budget and also impact on security, privacy and security issues[7][10]. Time, Cost and Innovation are merit points of cloud computing, yet security points are still be taken care for cloud environments. Cloud Providers face certain security issues [8][10] mentioned here-

i) Location Of Data
ii) Access to data
iii) Data Classification
iv) Service Level Agreement (SLA)
v) Security Breach
vi) Legal Issues
vii) Authentication and Authorization

IV. Modeling And Analysis Of Security Issue [6] [7]

i) Security Model

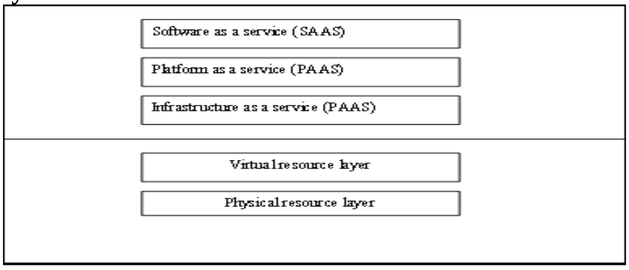

Software as a service (SAAS)
Platform as a service (PAAS)
Infrastructure as a service (PAAS)
Virtual resource layer
Physical resource layer

Figure 1. Security Model

ii] Process Of SACS

The process of SACS is comprised of many steps as given –[7]

-The user creates a local user agent, and set up a temporary safety certificate. The user's authorization and security access is complete.

-When the user's job use the source on the internet service layer, mutual authentication take place between user agent and explicit application.

-According to user's requirements, internet application will make a list of service resource, and then go by it to the user agent.

iii] Simulation Tool

The experimental results are obtained from Hadoop, reduce programming specification.[7] It is the software that is used to write applications that process large amount of statistics. This is a distributed file base system with framework.[8] - Simulating tools like CloudSim, GrimSim and cloud Analyst, docircuits, partsim, Mast Sim.

iv] Experimental Results and Analysis

The proposed tool is the distributed file base system. This tool can be downloaded in Linux base operating system and can be run on the windows operating system[8] After installing this on system the individual user name Hadoop is created that is single node. Log in to this user a cluster working like cloud is designed using Java 1.6 [11]. Linux is secure operating system so attacks like - mandatory access attacks, SQL injection attacks and directory traversal attacks are generated to measure the performance[7]

A] Comparison[7]

Results	Attack number	No using SACS		Using SACS	
		Attacked number	Attacked rate	Attack number	Attacked rate
Mandatory Access	10	8	0.8	0	0
	20	17	0.85	1	0.05
	30	26	0.87	3	0.1
SQL Injection	10	9	0.9	3	0.33
	20	18	0.9	5	0.25
	30	22	0.73	4	0.13
Directory Traversal Attacks	10	5	0.5	3	0.3
	20	12	0.6	8	0.4
	30	19	0.63	15	0.5

Table 1. Comparison of SACS usage [7]

B] Comparison result using SACS and no SACS [7]

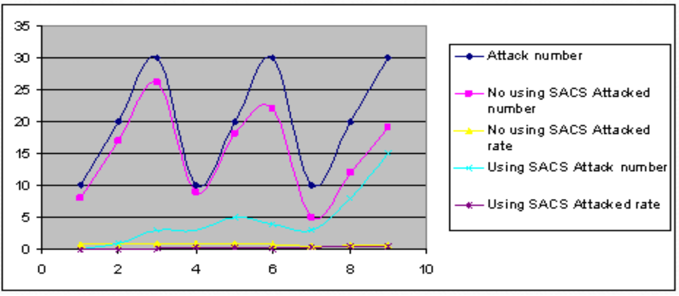


Figure 2. Result using SACS and no SACS [7]

C] <u>Performance Of System</u> [7]

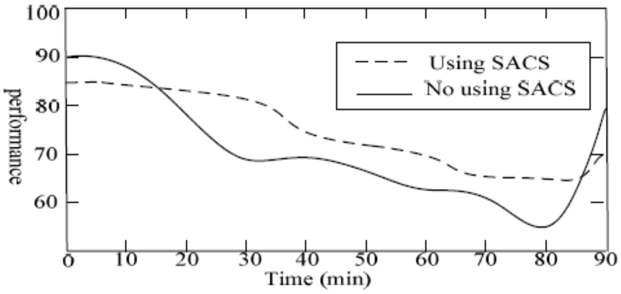


Figure 3. Performance Of System [7]

V. Security Algorithms [3]

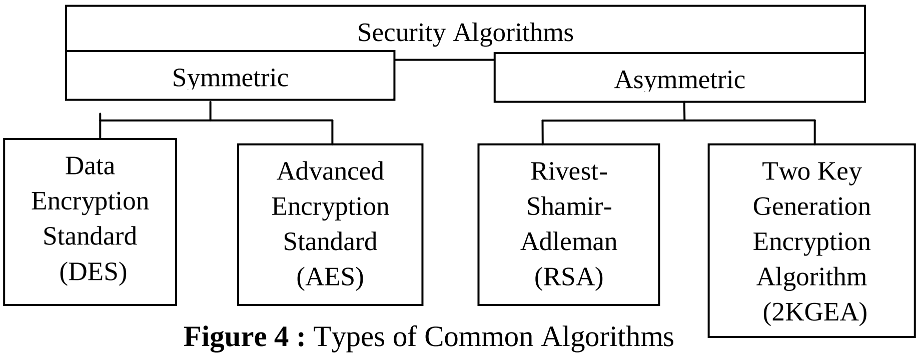

Security Algorithms
Symmetric
Asymmetric
Data Encryption Standard (DES)
Advanced Encryption Standard (AES)
Rivest-Shamir-Adleman (RSA)
Two Key Generation Encryption Algorithm (2KGEA)

Figure 4 : Types of Common Algorithms

VI. ENCRYPTION ALGORITHMS

Blowfish Algorithm - Blowfish is a symmetric block cipher encryption algorithm meaning that it uses the same secret key to both encrypt and decrypt messages and divides a message up into fixed length blocks during encryption and decryption. Blowfish Algorithm is a Feistel Network, iterating a simple encryption function 16 times.

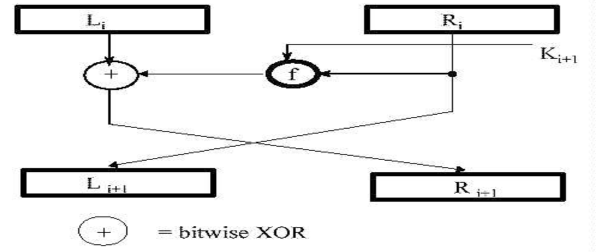


Figure 5. Feistel Network

AES Algorithm - AES uses the same key for both encryption and decryption. The four rounds are called SubBytes, ShiftRows, MixColumns, and AddRoundKey. During SubBytes, a lookup table is used to determine what each byte is replaced with. The ShiftRows step has a certain number of rows where each row of the state is shifted cyclically by a particular offset, while leaving the first row unchanged. Each byte of the second row is shifted to the left, by an offset of one, each byte in the third row by an offset of two, and the fourth row by an offset of three. This shifting is applied to all three key lengths, though there is a variance for the 256-bit block where the first row is unchanged, the second row offset by one, the third by three, and the fourth by four.

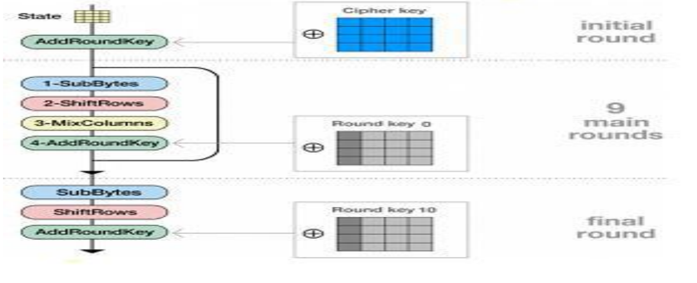
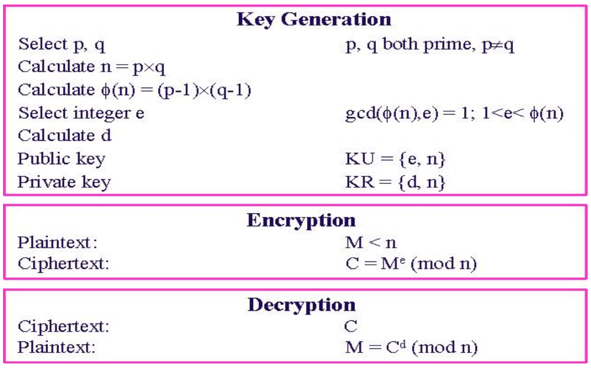


Figure 6. AES Encryption Process

RSA Algorithm - The RSA algorithm is the most commonly used encryption and authentication algorithm and is included as part of the Web browsers from Microsoft and Netscape. RSA is an algorithm for public-key cryptography.[8]



Key Generation	
Select p, q	p, q both prime, $p \neq q$
Calculate $n = p \times q$	
Calculate $\phi(n) = (p-1) \times (q-1)$	
Select integer e	$\gcd(\phi(n), e) = 1;\ 1 < e < \phi(n)$
Calculate d	
Public key	$KU = \{e, n\}$
Private key	$KR = \{d, n\}$

Encryption	
Plaintext:	$M < n$
Ciphertext:	$C = M^e \pmod n$

Decryption	
Ciphertext:	C
Plaintext:	$M = C^d \pmod n$

Figure 6. Steps of RSA Algorithm [8]

VII. RSA SECURITY ALGORITHM IMPLEMENTATION

RSA Algorithm - The RSA algorithm is the most commonly used security algorithm existing for data storage for cloud computing process. The data is been encrypted and decrypted, once the key is generated[8][9][10]

Implementation Of RSA :

A] Key Generation -

Select p=3, q=5 being both prime numbers.
n=pxq = 3x5 =15
Ø(n) = (p-1)(q-1) = (3-1)(5-1) =8
Let e=3, 5, 7 only for 1<3, 5, 7<8
If e=3, then e.d = 1mod Ø(n), d = 3
Encryption Key = {3,15}
Decryption Key = {3,15}

B] Encryption :

If M=3, such that M<n
E=M^e mod n=3

C] Decryption :

M=E^d mod n =3

Figure 7. Example of RSA Algorithm

Similarly based on this basic RSA Algorithm, further development of many more sophisticated algorithms are been implemented for secure and valid data verification. Based on Basic RSA, the small-e and Efficient RSA algorithms are proven. These are asymmetric algorithms whereas few symmetric algorithms like DES, AES, Blowfish, and others are given considerations. The 2 key generation encryption algorithm 2KGEA is proposed for dual encryption security of data.

VIII. PROPOSED DUAL SECURITY ALGORITHM

This proposed dual security algorithm is based on the efficient RSA and RSA small-e merits. In this, the number of exponents will be made 3 and the following steps will be executed.

A] Key Generation Algorithm :

Select p and q as being both prime numbers.
n= p x q
Ø(n) = (p-1)(q-1)
ϒ n, h = ph-p0 ph-p1…ph-ph-1 + qh-q0 qh- q1 … qh-qh-1
r such as1<r<n and gcd r, Ø=1 and gcd r,ϒ=1 (r should be small integer)
e such as r.e = 1 mod Ø(n) and 1<e< Ø(n)
d such as d.e= 1mod ϒn and 1<d< ϒn
Encryption Key = {e,n}… public key
Decryption Key = {r,d,n}… private key

B] Encryption Process :

If M=3, such that M<n
E=((M^e mod n)e mod n)

C] Decryption Process:

M=((Er mod n)d mod n)

r in 2KGEA has same role of e in RSA small-e and exponent e has same size as Ø(n). d is been computed as per the Efficient RSA algorithm and the values of ϒ n,h. In the proposed algorithm encryption carried with two consecutive steps while decryption is been different. So the security of both algorithms explained herewith differ. Further expansion in this proposed scheme can be modified based on performance and security of data.

IX. SECURITY ATTACKS

The security analysis done based on three attacks –

A] Brute Force Attack - This attack is been reduced in RSA algorithm by selecting exponents larger than 2048 bits while in 2kGEA algorithm attack is with even 1024 bits exponents[3][12]

B] Timing Attack - In RSA prevented by random delay by multiplying random number with cipher text, while in dual 2kGEA algorithm protection is at higher level and no need for multiplication with the cipher text[3][12]

C] Mathematical attack - In RSA, prevented by using 2048 bits exponents, while in 2KGEA algorithm the h value increased for the number of mathematical attacks to get reduced. Decryption with 2 different keys added security to data been encrypted and unreachable[3][12]

Data analysis is done with the help of MATLAB Software. This software is used to train and test the dataset and the efficiency of the result is measured. Eclipse start code system are fruitful for Java application to run smoothly. The simplest and basic conceptual method based on Turbo C or TC is also identified by experts as the preliminary stage of data analyzing[11]

X. CONCLUSION

The dual security algorithm was with respect to cloud computing environments, where the challenge is to use in cloud servers with respect to time and memory limitations during encryption and decryption process in servers due to its sharing performance. So it is better if encrypting stored data by symmetric algorithm such as AES in cloud servers and afterwards encrypting secret key with dual algorithm for sharing actions.[3][9]

XI. FUTURE WORK

So the existence of algorithms for security purpose is still in its way to research much better approaches and is been pointed out by experts. More and more fruitful efforts are in their way to be presented and implemented timely to ensure secure data between users.[3][8][9][10][12]

REFERENCES

Books :

[1] Cloud Security and Privacy, An Enterprise Perspective - Tim Mather, Subra Kumaraswamy

[2] Cloud Computing - Web Based Applications That Change the Way You Work and Collaborate Online - Michael Miller

Journal Papers :

[3] An Improved RSA Encryption Algorithm For Cloud Computing Environments : Two Key Generation Encryption (2KGEA) – Ms Shubhra Saggar (Faculty, Guru Nanak Institute Of management, New Delhi), Dr. R.K.Datta (Director, M.E.R.I.T., New Delhi) (Research Paper on IJSWS).

[4] On Technical Security Issues In Cloud Computing, Meiko Jensen, Jorg Schwenk and Nils Gruschka, Luigi Lo Lacono, 2009 IEEE International Conference on Cloud Computing.

[5] Providing Privacy Preserving in Cloud Computing, Jian Wang, Yan Zhao, Shuo Jiang, Jiajin Le, 2009 International Conference on Test and Measurement.

[6] Chang, L, Ti ; Chin L; Chang, A.Y.; Chun J, C;(2010), " Information security issue of enterprises adopting the application of cloud computing", IEEE 2010 Sixth International Conference on Networked Computing and Advanced Information Management (NCM),pp 645, 16-18 Aug. 2010.

[7] A review on cloud computing security issues & challanges F. A. Alvi1, B.S Choudary ,N. Jaferry , E.Pathan (white paper) - Department of Computer Systems and Electronic Engineering, QUEST Nawabshah, Sindh, Pakistan

[8] Cloud Computing: Security Issues And Description Of Encryption Based Algorithms To Overcome Them. Leena Khanna Prof. Anant Jaiswal *IITM, JanakPuri ASET, Noida (I.P.University) (Amity University)* New Delhi, India U.P, India

[9] Developing An Application Of RSA Algorithm with Java – M.Nusret Sarisakal, Selcuk Sevgen, Dogal Acar, Istanbul University, faculty Of Engineering, Department Of Computer Engineering, 34850, Avcilar, Istanbul, turkey.

[10] Review On Security Issues And Challenges On Data Storage Through Internet- Uma Naik, Prof. V.C.Kotak, Shah and Anchor Kutchhi Engineering College,Mumbai, India·

Search Sites :

[11] Online Technical Support based on Google and other search engines.

[12] Cryptography concepts from Internet.