Indian J.Sci.Res. 17(2): 158-163, 2018

ISSN: 0976-2876 (Print)
ISSN: 2250-0138(Online)

ENHANCING RSA ALGORITHM FOR CLOUD SECURITY

[1]Lanitha B., [2]Anitha E., [3]Hemalatha R

[1,2] Department of Computer Science and Engineering, KGiSL Institute of Technology, Anna University Coimbatore, Tamilnadu.

[3] Department of Computer Science and Engineering, NIFT-TEA College of Knitwear Fashion, Bharathiar University Tirupur, Tamilnadu.

Abstract:The Primary usage of cloud computing is data storage. Cloud storage enables users to access and store their data anywhere. It is more reliable and flexible to users to store and retrieve their data at anytime and anywhere. Many enterprises have started using cloud storage. Security and privacy are the key issues for cloud storage. Propose a simple data protection model for data is encrypted using Rivest-Shamir-Adleman (RSA) scheme before it is launched in the cloud, thus ensuring data confidentiality and security.

***Keywords* -** Cloud Storage, Rivest-Shamir-Adleman (RSA), Encryption Algorithm, Cryptography.

I. Introduction

Computer owners, finding enough storage area to receive everything they have already acquired can be a real challenge. There are many spend money on larger hardrives. Others prefer external storage devices like thumb drives or discs .Desperate computer owners might delete entire folders importance of old files to make space achievable information. However, many choosing to settle for a developing trend: cloud storage**.**

Cloud storage can be a subcategory of cloud computing**.** Cloud computing systems offer users access not to ever only storage, but probably processing power and computer applications installed on an internet network. While cloud storage may look like there is something to do with weather fronts and storm systems, it really is the word for saving data from an off-site storage system maintained by an alternate party. Rather than storing information in the computer's disk drive or other local storage device, it will save it to an internet database. The Internet offers link between computers in addition to database. On the top, cloud storage has several advantages over traditional data storage. You store your data even over a cloud storage system, you can receive fit it data from any location which include Internet access. Considering the proper storage system, you may choose to even allow other folks to discover the small print, turning an individual project right collaborative effort.

Clouds can supply several types of services like applications (Google Apps, Microsoft online), infrastructures (Amazon's EC2, Eucalyptus, Nimbus), and platforms to help you developers write applications (Amazon's S3, Windows Azure).

II. Most Popular Cloud Services

Compute as a service: Depending on the provider and the options an enterprise chooses, compute as a service also can include automated patch management, management of infrastructure software, storage management, security management, and dedicated customer support. Compute as a service provides compute capacity that includes servers, operating system access, firewalls, routers and load balancing on demand. These systems have management interfaces, and their capacity can be either shared or private.

Web hosting: Loads will always be balanced, and uptime is guaranteed and includes offsite backup and fast connections for eliminating slow page and content downloads. Many organizations rely on their websites for marketing and revenue, and any bug in operations can mean a loss of business. Moving a website to an IaaS based model ensures that the website will not get slowdown during peak traffic times; and that organizations will not have to pay too much for capacity to manage those traffic times.

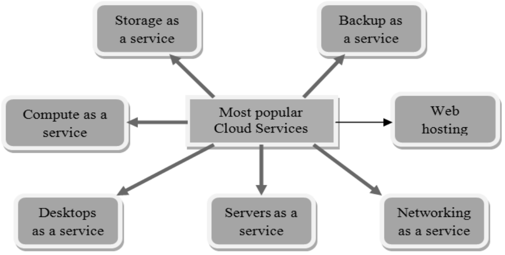

Figure1. Most Popular Cloud Services

Storage as a service: Cloud-based storage has the security controls to ensure that all data is stored securely in data center facilities, with extremely high availability. These solutions have interactive self-service portals that allow administrators to provision storage, transfer data to different tiers of storage, dispatch specific data sets to different media and add or remove storage as needed. Storage-as-a-service providers also have the latest storage technologies and virtually limitless capacity. Generally fast storage for high I/O applications, standard storage for system disk and bulk storage for file serving. And as with other types of IaaS, enterprises pay only for what they use.

[1]Corresponding Author

Disaster recovery and backup as a service: Moving disaster recovery to the cloud is to ensure that organizations have continuous access to data and applications, no matter of emergencies, such as power outages, natural disasters or system failures. Backup and restore from the cloud and backup and restore to the cloud. Organizations retain applications and data on their own premise, but back up data to the cloud and restore it to hardware on their own premise when a disaster occurs. Data is restored to virtual machines in the cloud. For mission-critical applications and resources that must be recovered quickly and completely, the best choice is often to replicate data to virtual machines.

Desktops as a service: Desktop environments available to new workers, with enough storage and all the right applications and desktops can be accessed via the Internet; users can log in and access their familiar workspaces from any location. The service provider offers storage for the virtual computers, ensures security and data protection, and controls the network bandwidth to ensure uptime. IaaS cloud created solely for hosting and serving virtual desktops. Essentially, its pay-as-you-go computing that allows enterprises to quickly provision, access, run and deactivate virtual desktop machines as needed. Organizations can choose to connect through a private network service instead of the public Internet.

Servers as a service: The servers are restricted to secure, private areas dedicated to the organization's use, so security is unchangeable. Accessing servers as a service also means organizations can cut their IT administrative, maintenance and service workloads. That is particularly important with servers, which can require complex and expensive system administration.

Networking as a service: Networking service can support quality of service (QoS) and other network-based auditing and monitoring services. NaaS involves no upfront costs and supports full scalability, flexibility and security. The idea is to offer networking resources on demand in order to support virtual networks resources such as firewalls, load balancing and WAN acceleration services. Simply put, NaaS provides unified connectivity across storage, networking and servers that change to meet the demands of virtualized infrastructures.

III. Issues In Cloud Data Storage

Confidentiality: [2] [3] [7] Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. A loss of confidentiality is the unauthorized disclosure of information (security protocols, authentication services and data encryption services).

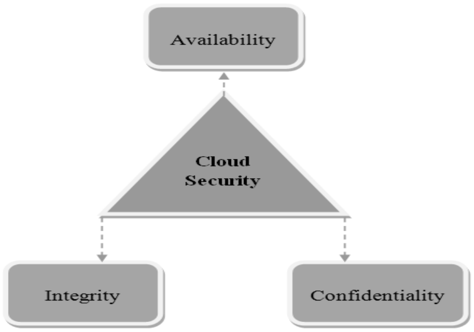

Figure2. Issues in cloud Data Storage

Integrity: [2] [3] [7] Guarding against improper information modification or destruction, including ensuring information non repudiation and authenticity. A loss of integrity is the unauthorized modification or destruction of information (Firewalls and intrusion detection).

Availability: [2] [3] [7] Ensuring timely and reliable access to and use of information. A loss of availability is the disruption of access to or use of information or an information system (fault tolerance, network security and authentication).

IV. Enhanced Rivest-Shamir-Aleman (Rsa) Scheme

Encryption Method: [6] [5] [4]

Message---HI FRIENDS

Step 1. Count the No. of character (N) in the plain text without space.

Step 2. Convert the plain text into equivalent ASCII code. And form a square matrix (S X S >=N).

Step 3. Apply the converted ASCII code value from left to right in the matrix. Divide matrix into three part namely upper, diagonal and lower matrix.

Step 4. Read the value from right to left in each matrix.

Step 5. Each matrix use three different key K=K1, K2, K3 for encryption. Do the encryption.

Step 6. Apply the encrypted value into the matrix in the same order of upper, diagonal and lower.

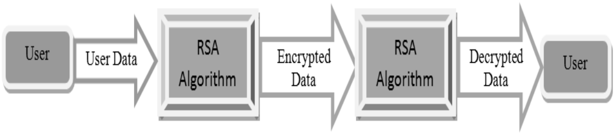

Fig. 3. RSA Scheme

$Select\ p, q$

$p\ and\ q\ both\ prime, p \neq q$

$Calculate\ n = p * q$

$Calculate\ f\ (n) = (p-1)(q-1)$

$Select\ integer\ e$

$gcd\ (f(n),e) = 1;\ 1 < e < f(n)$

$Calculated\ d$

$d \equiv e-1\ (mod\ f(n))$

$Public\ Key\ PU = \{e,n\}$

$Private\ Key\ PR = \{d,n\}$

$Plaintext: M < n$

$Ciphertext: C = M^e\ mod\ n$

$Ciphertext: C$

$Plaintext: M = C^d\ mod\ n$

Plaintext - HI FRIENDS

N= 9

ASCII code value for the plaintext

72 73 70 82 73 69 78 68 83

Plaintext N=9, so S=3.

The order of matrix is 3 X 3>=9, Form a 3 X 3 matrix

$$\begin{bmatrix} 72 & 73 & 70 \\ 82 & 73 & 69 \\ 70 & 68 & 83 \end{bmatrix}$$

$K_1 = 3$

$K_2 = 7$

$K_3 = 2$

Upper Matrix-73 70 69

Diagonal – 72 73 83

Lower matrix-82 78 68

Upper Matrix-76 73 72

Diagonal – 79 80 90

Lower matrix-84 80 70

$$\begin{bmatrix} 79 & 76 & 73 \\ 84 & 80 & 72 \\ 80 & 70 & 70 \end{bmatrix}$$

2 3 1 keys

$$\begin{bmatrix} 79 & 76 & 73 \\ 84 & 80 & 72 \\ 80 & 70 & 70 \end{bmatrix}$$

$$\begin{bmatrix} 73 & 79 & 76 \\ 72 & 84 & 80 \\ 70 & 80 & 70 \end{bmatrix}$$

P=17

Q=11

N=P*Q=17*11=187

$\emptyset(N) = (P-1)(Q-1)$

$\emptyset(N) = (16)(10) = 160$

$e \times d = 1(mod\ N)$

$e = 7$

$e \times d = 1 + 160 = 161$

$d = 161 \div 7$

$d = 23$

$$\begin{bmatrix} 73 & 79 & 76 \\ 72 & 84 & 80 \\ 70 & 80 & 70 \end{bmatrix}$$

Public= (7,187)

Private= (23,187)

$73^7 mod187 = 61$

$79^7 mod187 = 139$

$76^7 mod187 = 32$

$72^7 mod187 = 30$

$84^7 mod187 = 50$

$80^7 mod187 = 75$

$70^7 mod187 = 60$

$80^7 mod187 = 75$

$70^7 mod187 = 60$

$$\begin{matrix} 61 & 139 & 32 \\ 30 & 50 & 75 \\ 60 & 75 & 60 \end{matrix}$$

P=17

Q=5

N=P*Q=17*5=85

$\emptyset(N) = (P-1)(Q-1)$

$$\emptyset(N) = (16)(5) = 64$$

$$e \times d = 1(mod\ N)$$

$$e = 5$$

$$e \times d = 1 + 64 = 65$$

$$d = 65 \div 5$$

$$d = 13$$

$$\begin{bmatrix} 61 & 139 & 32 \\ 30 & 50 & 75 \\ 60 & 75 & 60 \end{bmatrix}$$

Public= (5, 85)

Private= (13, 85)

$$61^5 mod 85 = 6$$

$$139^5 mod 85 = 39$$

$$32^5 mod 85 = 2$$

$$30^5 mod 85 = 30$$

$$50^5 mod 85 = 50$$

$$75^5 mod 85 = 45$$

$$60^5 mod 85 = 25$$

$$75^5 mod 85 = 45$$

$$60^5 mod 85 = 25$$

$$\begin{matrix} 6 & 39 & 2 \\ 30 & 50 & 45 \\ 25 & 45 & 25 \end{matrix}$$

2 3 1 keys

$$\begin{bmatrix} 6 & 39 & 2 \\ 30 & 50 & 45 \\ 25 & 45 & 25 \end{bmatrix}$$

$$\begin{bmatrix} 2 & 6 & 39 \\ 45 & 30 & 50 \\ 25 & 25 & 45 \end{bmatrix}$$

Encryption Value - 2 6 39 45 30 50 25 25 45

Get the plaintext from the user (Ei) E-Encrypted text, i Text length. Get the key value from the range numbers (0 to 256) (Ki) K-Key value, i Key length. Apply the formula Ei (X+K) Mod 256 or Ei (X+K) – 256. Decryption Ei (X-K) Mod 256 or Ei (X-K) – 256.

(The repeated characters encryption using the character string = plaintext char + 1, so i+1(105+1) =106.consider decryption i - 1(105-1) =104)

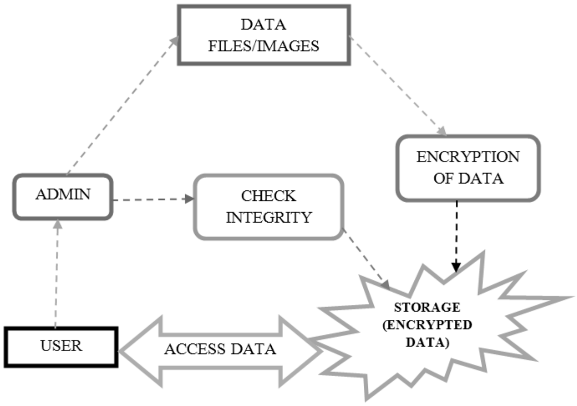

Figure 4. Secure Data Storage and Retrieve

Value	= 2
Key	=10
Sum	=12
ASCII Table	=256 -12=244
Value	= 6
Key	=10
Sum	=16
ASCII Table	=256 -16=240
Value	= 39
Key	=10
Sum	=49
ASCII Table	=256 -49=207
Value	= 45
Key	=10
Sum	=55
ASCII Table	=256 -55=201
Value	= 30
Key	=10
Sum	=40
ASCII Table	=256 -55=216
Value	= 50
Key	=10
Sum	=60
ASCII Table	=256 -60=196
Value	= 25

Key	=10
Sum	=35
ASCII Table	=256 -35=221
Value	= 25+1=26
Key	=10
Sum	=36
ASCII Table	=256 -36=220
Value	= 45+1
Key	=10
Sum	=56
ASCII Table	=256 -56=200

Encryption Value - 224 240 207 201 216 196 221 220 200

224-À

240-Ð

207-Ï

201-É

216-Ø

196-Ä

221-Ý

220-Ü

200-È

PLAIN TEXT -H I F R I E N D S

CIPHER TEXT -À Ð Ï É Ø Ä Ý Ü È

Decryption Method: [6] [5] [4]

CIPHER TEXT -À Ð Ï É Ø Ä Ý Ü È

Encryption Value - 224 240 207 201 216 196 221 220 200

Decryption Ei (X-K) Mod 256 or Ei (X-K) – 256.

(The repeated characters encryption using the character string = plaintext char + 1, so i+1(105+1) =106.consider decryption i - 1(105-1) =104)

Encryption Value - 2 6 39 45 30 50 25 25 45

$$\begin{bmatrix} 2 & 6 & 39 \\ 45 & 30 & 50 \\ 25 & 25 & 45 \end{bmatrix}$$

$$Keys\ (1\ 2\ 3) = D(Keys\ (1\ 2\ 3)) =$$

$$Keys\ (3\ 2\ 1)$$

2 3 1 keys 2 1 3

$$\begin{bmatrix} 2 & 6 & 39 \\ 45 & 30 & 50 \\ 25 & 25 & 45 \end{bmatrix} \qquad \begin{bmatrix} 2 & 6 & 39 \\ 45 & 30 & 50 \\ 25 & 25 & 45 \end{bmatrix}$$

$$\begin{bmatrix} 6 & 39 & 2 \\ 30 & 50 & 45 \\ 25 & 45 & 25 \end{bmatrix}$$

$$6^{13} mod 85 = 61$$

$$39^{13} mod 85 = 139$$

$$2^{13} mod 85 = 32$$

$$30^{13} mod 85 = 30$$

$$50^{13} mod 85 = 50$$

$$45^{13} mod 85 = 75$$

$$25^{13} mod 85 = 60$$

$$45^{13} mod 85 = 75$$

$$25^{13} mod 85 = 60$$

$$\begin{bmatrix} 61 & 139 & 32 \\ 30 & 50 & 75 \\ 60 & 75 & 60 \end{bmatrix}$$

$$61^{23} mod 187 = 73$$

$$139^{23} mod 187 = 79$$

$$32^{23} mod 187 = 76$$

$$30^{23} mod 107 = 72$$

$$50^{23} mod 187 = 84$$

$$75^{23} mod 187 = 80$$

$$60^{23} mod 187 = 70$$

$$75^{23} mod 187 = 80$$

$$60^{23} mod 187 = 70$$

$$\begin{bmatrix} 73 & 79 & 76 \\ 72 & 84 & 80 \\ 70 & 80 & 70 \end{bmatrix}$$

Step 1. The encrypted text is converted into ASCII code values.

Step 2. Count the No.of character (N) in the decrypted text and form a square matrix S X S.

Step 3. Apply the ASCII code in the SXS matrix as column by column based on key K4.

Step 4. Divide the matrix into upper, diagonal and lower.

Step 5. Apply reverse encryption using the keys K1, K2 and K3 on the upper, diagonal and lower matrix respectively.

Step 6. Apply the message into table by upper, diagonal and lower matrix.

Step 7. Read the message as row by row from left to right.

$Keys\ (1\ 2\ 3) = D(Keys\ (1\ 2\ 3))$ = $Keys\ (3\ 2\ 1)$

$$\begin{array}{ccc} 2 & 3 & 1 \\ \hline 73 & 79 & 76 \\ 72 & 84 & 80 \\ 70 & 80 & 70 \end{array} \quad \text{keys} \quad \begin{array}{ccc} 2 & 1 & 3 \\ \hline 79 & 76 & 73 \\ 84 & 80 & 72 \\ 80 & 70 & 70 \end{array}$$

Upper Matrix-76 73 72

Diagonal – 79 80 90

Lower matrix-84 80 70

$K_1 = 3$

$K_2 = 7$

$K_3 = 2$

Upper Matrix-73 70 69

Diagonal – 72 73 83

Lower matrix-82 78 68

$$\begin{bmatrix} 72 & 73 & 70 \\ 82 & 73 & 69 \\ 78 & 68 & 83 \end{bmatrix}$$

72 73 70 82 73 69 78 68 83

Message---HI FRIENDS

V. Conclusion

Cryptographic techniques are widely-used to provide secure communication between the consumer as well as the cloud. All of the cloud providers has their very own list of rules, pricing, flexibility, support along with important parameters. The main element consideration dealt in this proposal may be the encryption schema to secure data by making it unintelligible for all. Implementing RSA for security over data provides advantages of less memory consumption and less computation time. Inside the algorithm that has been proposed here the time and effort has become in the direction of faster public key encryption without compromising the safety with the system.

Reference

[1] The most famous of the fallen contenders is the trapdoor knapsack proposed by Ralph Merkle.We describes this in Appendix J.

[2] Apparently, the first workable public-key system for encryption/decryption was put forward by Clifford Cocks of Britain’s CESG in 1973 [COCK73]; Cocks’ method is virtually identical to RSA.

[3] Dr. L. Arockiam, S. Monikandan “Data Security and Privacy in Cloud Storage using Hybrid Symmetric Encryption Algorithm” International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 8, August 2013

[4] Joshi, J.B.D., Gail-Joon Ahn. Security and Privacy Challenges in Cloud Computing Environments. IEEE Security Privacy Magazine, Vol 8, IEEE Computer Society, 2010, p.24-31.

[5] Sonal Guleria, Dr. Sonia Vatta “TO ENHANCE MULTIMEDIA SECURITY IN CLOUD COMPUTING ENVIRONMENT USING CROSSBREED ALGORITHM “international journal of application or innovation in engineering & management Volume 2, Issue 6, June 2013

[6] Andrea Pellegrini, Valeria Bertacco, “Fault-Based attack of RSA Authentication”.

[7] These examples are taken from a security policy document published by the Information Technology Security and Privacy Office at Purdue University.