ISBN 978-93-5156-328-0
International Conference of Advance Research and Innovation (ICARI-2015)

Enhanced Data Security on Cloud Based using Encryption Algorithm, Elliptic Curve Cryptography & Blowfish Algorithm

Neetu Sharma [a], Monika Kansal [b]
[a] Department of Computer Science Engineering, ABES Engineering College, Ghaziabad, Uttar Pradesh, India
[b] Department of Computer Science Engineering, ITS College, Ghaziabad, Uttar Pradesh, India

Article Info
Article history:
Received 9 January 2015
Received in revised form
12 January 2015
Accepted 20 January 2015
Available online 31 January 2015

Keywords
Cloud computing,
Security Algorithm,
For security

Abstract

With the advent internet in the 1990s to the present day facilities of ubiquitous computing, the internet has changed the computing world in a drastic way. It has traveled from the concept of parallel computing to distribute computing to grid computing and recently to cloud computing. Although the idea of cloud computing has been around for quite some time, it is an emerging field of computer science. Some of the major firms like Amazon, Microsoft and Google have implemented the "CLOUD" and have been using it to speed up their business. In this paper we will discuss Distributed scheme and Different algorithm to provide security of the data in cloud to prevent Data access from unauthorized access.

1. Introduction

Cloud computing can be defined as a computing environment where computing needs by one party can be outsourced to another party and when need be arise to use the computing power or resources like database or emails, they can access them via internet. Cloud computing [1, 2] is a recent trend in IT that moves computing and data away from desktop and portable PCs into large data centers. The main advantage of cloud computing is that customers do not have to pay for infrastructure, its installation, required man power to handle such infrastructure and maintenance. The rapid deployment [1] of cloud computing promises network users with elastic, abundant, and on-demand cloud services. The pay-as-you-go model allows users to be charged only for services they use. Sales force, Amazon and Google are currently providing such services, charging clients using an on-demand policy. As the users deal their sensitive data to clouds i.e. public domains, the major hurdles for cloud adoption are lack of security and access control. The main setback is that the insecure information flows as service provider can access multiple virtual machines in clouds. So it is necessary to build up proper security for cloud implementation

2. Service Models in Cloud

Cloud computing [5] is generally broken down into three primary service levels:

1) **Software-as-a-Service"(SaaS):** We are provided with access to application software often referred to as on-demand software. We don't have to worry about the installation, setup and running of the application. Service provider will do that for us. We just have to pay and use it through some client. Examples: Google Apps, Microsoft Office 365.The simplest example to understand is e-mail.
2) **Infrastructure-as-a-Service (IaaS):** It provides us the computing infrastructure, physical or (quite often) virtual machines and other resources like virtual-machine disk image library, block and file-based storage, firewalls, load balancers, IP addresses, virtual local area networks etc.

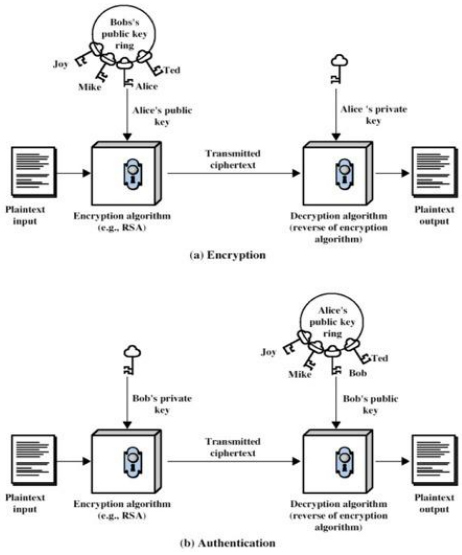
In IaaS we outsource the hardware. In such cases [3], it's not just the computing power that we rent; it also includes power, cooling, and networking. Furthermore, it's more than likely that well need storage as well. Generally IaaS is this combination of compute and cloud storage. **Examples:** Amazon EC2, Windows Azure, Rackspace.

3) **Platform-as-a-Service (PaaS) :** The vendor takes care of the underlying infrastructure for us, giving us only a platform with which to (build and) host our application(s). PaaS provides us computing platforms which typically includes operating system, programming language execution environment, database, web server etc. Examples: AWS Elastic Beanstalk, Heroku, Force.com, Google App Engine.

PaaS user is a SaaS developer. An IaaS user could very well be a PaaS or SaaS developer

3. Encryption Algorithms

RSA Algorithm



Corresponding Author,
E-mail address: neetu.sharma@abes.ac.in

The RSA algorithm [9] 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, involves a public key and a private key. The public key can be known to everyone and is used for encrypting messages.

The basic steps of RSA algorithm are:

- Key Generation
- Encryption and
- Decryption

Key Generation

1. Select p, q (p, q both prime, p! = q)
2. Calculate n=p*q
3. Calculate ϕ(n)=(p-1)*(q-1)
4. Select integer e gcd(ϕ(n),e)=1; 1<e< ϕ(n)
5. Calculate d
6. Public key KU= {e, n}
7. Private key KR= {d, n}

Encryption

Plaintext: M<n

Cipher text: C=Me (mod n)

Decryption

Cipher text: C

Plaintext: M=Cd (mod n)

The algorithm involves multiplying two large prime numbers and through additional operations deriving a set of two numbers that constitutes the public key and another set that is the private key. Both the public and the private keys are needed for encryption /decryption but only the owner of a private key ever needs to know it. Using the RSA system, the private key never needs to be sent across the Internet. The private key is used to decrypt text that has been encrypted with the public key.

RSA Algorithm Example

- Choose p = 3 and q = 11
- Compute n = p * q = 3 * 11 = 33
- Compute φ(n) = (p - 1) * (q - 1) = 2 * 10 = 20
- Choose e such that 1 < e < φ(n) and e and n are co prime. Let e = 7
- Compute a value for d such that (d * e) % φ(n) = 1. One solution is d = 3 [(3 * 7) % 20 = 1]
- Public key is (e, n) => (7, 33)
- Private key is (d, n) => (3, 33)
- The encryption of m = 2 is c = 27 % 33 = 29
- The decryption of c = 29 is m = 293 % 33 = 2

4. Algorithm for Data Security using Elliptic Curve Cryptography

Elliptical curve cryptography (ECC) is a public key encryption technique based on elliptic curve theory that can be used to create faster, smaller, and more efficient cryptographic keys. ECC [5] generates keys through the properties of the elliptic curve equation instead of the traditional method of generation as the product of very large prime numbers. ECC can yield a level of security with a 164-bit key that other systems require a 1,024-bit key to achieve.

An elliptic curve is a type of cubic curve whose solutions are confined to a region of space that is topologically equivalent to a torus. An elliptic curve over a field K is a nonsingular cubic curve in two variables, f(x, y) =0 with a rational point (which may be a point at infinity). The field K is usually taken to be the complex numbers, reals, rationals, and algebraic extensions of rationals, p-adic numbers, or a finite field. Elliptic curves groups for cryptography are examined with the underlying fields of Fp $y2=x3+ax+b$

(Where p>3 is a prime) and F2m (a binary representation with 2m elements). An elliptic curve is a plane curve defined by an equation of the form Consider elliptic curve

E: $y2 = x3 - x + 1$

If P1 and P2 are on E, we can define addition

P3 = P1 + P2

Both clouds agree to some publicly-known data item.

a. The elliptic curve equation
   ii. values of a and b
   iii. prime, p

b. The elliptic group computed from the elliptic curve equation

c. A base point, B, taken from the elliptic group

Key Generation:

1. A selects an integer dA. this is A's private key.
2. A then generates a public key PA=dA*B
3. B similarly selects a private key dB and computes a public key
   PB= dB *B
4. A generates the security key K= dA *PB. B generates the Secrete key K= dB *PA.

Signature Generation: For signing a message m by sender of cloud A, using A's private key dA 1. Calculate e=HASH (m), where HASH is a cryptographic hash function, such as SHA-1 2. Select a random integer k from [1, n − 1] 3. Calculate r = x1 (mod n), where (x1, y1) = k * B. If r = 0, go to step 2 4. Calculate s = k − 1(e + dAr) (mod n). If s = 0, go to step 2 5. The signature is the pair (r, s) 6. Send signature (r, s) to B cloud.

Encryption algorithm: Suppose [9] A wants to send to B an encrypted message.

i. A takes plaintext message M, and encodes it onto a point, PM, from the elliptic group.
ii. A chooses another random integer, k from the interval [1, p-1]
iii. The cipher text is a pair of points
   PC = [(kB), (PM + kPB)]
iv. Send cipher text PC to cloud B.

Decryption algorithm: Cloud B will take the following steps to decrypt cipher text PC.

a. B computes the product of the first point from PC and his private key, dB

dB * (kB)

b. B then takes this product and subtracts it from the second point from PC

(PM + kPB) – [dB (kB)] = PM + k(dBB) – dB(kB) = PM

5. Blowfish Algorithm

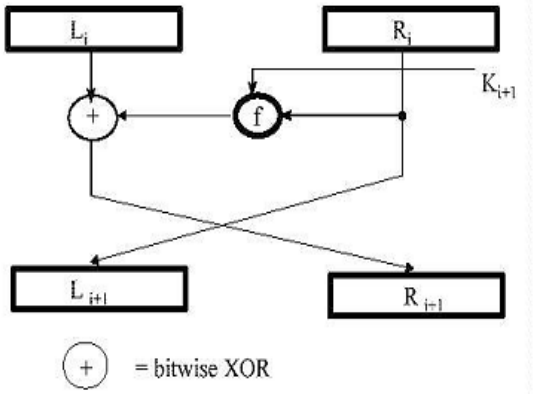
Blowfish is a symmetric block cipher encryption algorithm meaning that it uses the same secret key to both encrypt and decrypt messages and divides a message up into fixed length blocks during encryption and decryption. The block length for Blowfish is 64 bits; messages that aren't a multiple of eight bytes in size must be padded. It takes a variable-length key, from 32 bits to 448 bits, making it ideal for securing data. It [8, 10] is suitable for applications where

ISBN 978-93-5156-328-0

the key does not change often, like a communications link or an automatic file encrypt or. It is significantly faster than most encryption algorithms when implemented on 32-bit microprocessors with large data caches. Blowfish Algorithm is a Feistel Network, iterating a simple encryption function 16 times. The block size is 64 bits, and the key can be any length up to 448 bits.

The basic working of a Feistal Network is:

- Split each block into halves
- Right half becomes new left half
- New right half is the final result when the left half is XOR'd with the result of applying f to the right half and the key.



6. AES Algorithm

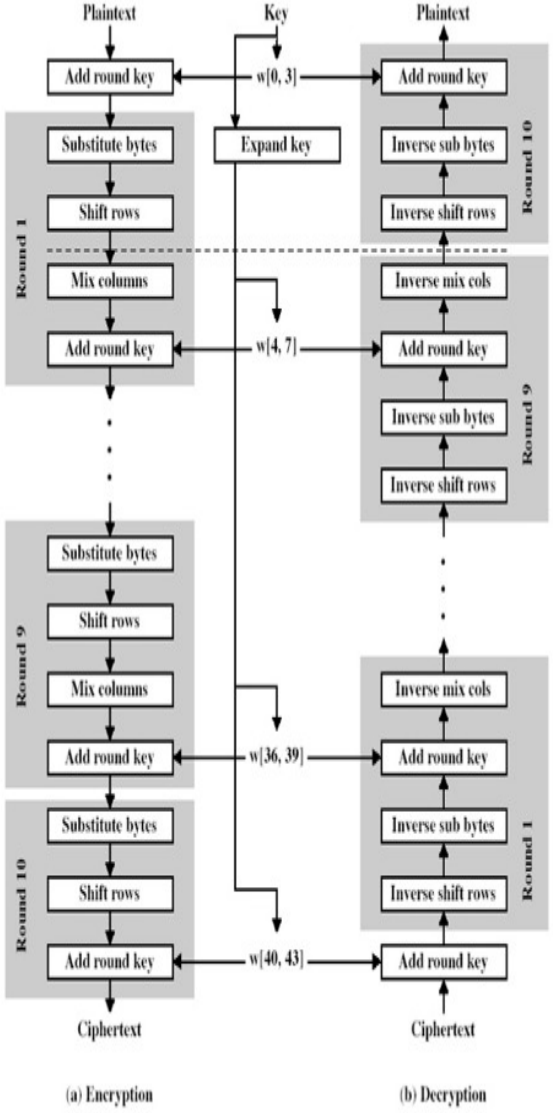
AES is a symmetric block cipher. This means that [4] it uses the same key for both encryption and decryption. AES standard states that the algorithm can only accept a block size of 128 bits and a choice of three keys - 128, 192, 256 bits.

Depending on which version is used, the name of the standard is modified to AES-128, AES-192 or AES- 256 respectively. Encryption consists of 10 rounds of processing for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys. Except for the last round in each case, all other rounds are identical.

The four rounds [6] are called Sub Bytes, Shift Rows, Mix Columns, and Add Round Key. During Sub Bytes, a lookup table is used to determine what each byte is replaced with. The Shift Rows 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.

The Mix Columns step is a mixing operation using an invertible linear transformation in order to combine the four bytes in each column. The four bytes are taken as input and generated as output. In the fourth round, the Add Round Key derives round keys from Rijndael's key schedule, and adds the round key to each byte of the state. Each round key gets added by combining each byte of the state with the corresponding byte from the round key.

Lastly, these steps are repeated again for a fifth round, but do not include the Mix Columns step.



7. Conclusion

As the users deal their sensitive data to clouds i.e. public domains, the major hurdles for cloud adoption are lack of security and access control. The main setback is that the insecure information flows as service provider can access multiple virtual machines in clouds. So it is necessary to build up proper security for cloud implementation, data security are the main problem of the cloud computing security. We concern here data security with different cryptography algorithm to provide confidentiality and authentication of data between clouds. In future we will concern more security issues of cloud computing and try to find better solutions using cryptography.

References:

[1] Q. Wang, C. Wang, K. Ren, W. Lou, J. Li, ‖ Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing in IEEE Transactions on Parallel and Distributed Systems, 22(5), 2011
[2] http://www.certicom.com/index.php/ecc
[3] http://mathworld.wolfram.com/EllipticCurve.html
[4] http://searchsecurity.techtarget.com/definition/elliptical-curve-cryptography
[5] J. Yang, Z. Chen, Cloud Computing Research and Security Issues
[6] http://www.cloudsecurityalliance.org/topthreats
[7] http://www.aws.amazon.com/
[8] Nurmi, Woloski, Obertelli, The Eucalyptus Opensource Cloud computing, 2009
[9] U. Somani, K. Lakhani, M. Mundra, Implementing digital signature with RSA Encryption Algorithm to enhance the data security of cloud in Cloud Computing, 2010
[10] G. Boss, Cloud Computing IBM 2007.10