ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 8, August 2015

Secure Data Communication in Cloud Computing using Proposed DSA

Swati Chaudhaary[1], Arvind Negi[2], Prashant Chaudhary[3]

M.Tech, CSE, Uttaranchal College, Dehradun, India[1,2]

CSE Dept., Uttaranchal College, Dehradun, India [3]

Abstract: Cloud computing allows for on-demand entry to shared property. It enables to utilize records and purposes over the web. Since they share the information through the net, security is regarded as a major issue so that Cloud computing services need to address the security in the coursework of the transmission of sensitive information and critical applications to shared and public cloud environments. The cloud computing supports distributed services multi-domain Infrastructure, and multi-users. This paper has presented the concept of secure authenticated information and secure cloud storage to deal with security issues that occurs in cloud as a result of malicious activities of attacker.

Keywords: Encryption, Decryption, Digital Signature, DSA, Data Security.

I. INTRODUCTION

Cloud computing is that the next generation within the Internet's technology that provides the user everything in terms of services like computing power to computing infrastructure, applications, business processes as per the necessity of user over the web. Cloud computing accommodates shared computing resources that are opposition native servers or devices. Users can pay on the idea of resource usage as timely basis. Normally we will say that this technology primarily providing hosting services over the web or the delivery of applications or IT services, that are provided by a 3rd party over the web. In straightforward words, Cloud Computing is that the combination of a technology, platform that gives hosting and storage service on the web.

As cloud computing is gaining quality, issues are being voiced concerning the safety problems introduced through the adoption of this new technology. The effectiveness and potency of traditional protection mechanisms are being reconsidered, because the characteristics of this innovative preparation technology, dissent wide from them of traditional architectures.

II. RELATED WORK

An In this paper researcher using proposed DSA algorithm to encrypt the data to provide security so that only the concerned user can access it. User data is encrypted first then it is stared in the cloud. When required user place a request for the data from the cloud provider, cloud provider authenticates the user & deliver the data. DSA consists of public & private key. In our cloud environment, public key is known to all. And private key is only known to the user who originally owns the data. Thus encryption is done by the cloud service provider and decryption is done by the cloud user or consumer.

DSA algorithm consists of two parts.

A. Generation of pair of public key & private key.

B. Generation of Digital signature & verification of digital signature.

A. Generation of pair of public and private key.

I. Key Generation

- Chose a prime number q, which is called the prime divisor.
- Chose the another prime no. p, such that g^p mod p=1 & g=h((p-1)/q)mod p
- Chose an integer, such that 0<x<q.
- Compute y= g^x mod p

So, public key (p, q, g, y) & private key (p, q, g, x)

B. Generation of Digital Signature & verification of Digital Signature.

In case of digital signature generation sender uses a one way hash function to calculate a message digest and then he signs it using private key and receiver verifies the integrity of message using the public key of the sender.

I. Signature Generation

1. Generate the message digest h, using a hash algorithm SHA1.
2. Generate a random no. k, such that 0<k<q.
3. Compute r,

r = (g^kmod p) mod q, if r= 0, select different k.

4. Compute s,

s = k^{-1}(h+ r*x) mod q, if s= 0, select different k.

Digital signature as {r, s}

II. Signature verification

- Generate the message digest h, using a same hash algorithm.
- Compute w, w mod q=1(w is called the modular multiplicative inverse of s modulo q.)
- Compute u_a= h^wmod q.
- Compute u_b= r^wmod q.
- Compute v= ((g^{ua}) (y^{ub}) mod p) mod q.
- If v = = r, the signature is valid.

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 8, August 2015

III. PROPOSED WORK

Original DSA algorithm has its own security disadvantages, that is, only one key is used. So in order to improve its security, more than one key is used due to which the difficulty of deciphering key increases.
For each user, data is encrypted initially so it's started within the cloud for transmission between the user and therefore the cloud. When required, user places a request for the data from the cloud provider. Cloud provider initial authenticates the user & then delivers the data. For this proposed idea we are using DSA algorithm to provide security to the users of cloud. But sometimes generally DSA have its own security disadvantages. For improving security of cloud we are using multiple Keys and random no's for encryption and decryption instead of single key that is using by the users for encryption & decryption. So to enhance the security between the user and cloud we are using multiple keys that is used by the multiple users at a single time & and these keys are generated randomly.

A. Key Generation

- Choose q (prime no.)
- Choose p, such that p-1 mod q=1
- Choose an integer g, g^q mod p=1

$g = h^{(p-1)/q}$ mod p.
g, 1<g<p

- Choose integer x, 0<x<q

For improve security x= (x_1, x_2, x_3…….x_n)
Therefore 0<(x_1, x_2, x_3……. x_n)<q

- Compute y,

For (x_1, x_2, x_3…….x_n)

$y_1=g^{x1}$ mod p
y2=g^{x2}mod p
.
$y_n= g^{xn}$ mod p {p, q, g, y}

Public key as {p, q, g, (y_1, y_2, y_3……..y_n)}
Also we use public key as—

{ p, q, g, y_1}
{ p, q, g, y2}
.
{p, q, g, yn}

Private key---- { p, q, g, x}

{ p, q, g, (x_1, x_2, x_3 ……x_n)}
Also private key used as----
{ p, q, g, x_1}
{p, q, g, x_2}
{ p, q, g, x_3}
.
{p, q, g, x_n}

B. Signature Generation----

- Generate message digest h, using hash algo like SHA1.
- Generate random no. k, such that, 0<k<q. We are selecting multiple random no. for security purposes-

  k ={ k_1, k_2, k_3……k_n }
- So, compute r = (g^k mod p)mod q, if r = 0, select different k.

  For (k_1, k_2, k_3……k_n)
  r_1 = ($g^k{}_1$ mod p) mod q
  r_2 = ($g^k{}_1$ mod p) mod q
  r_3 = ($g^k{}_3$ mod p) mod q
  .
  r_n= ($g^k{}_n$ mod p) mod q
- Calculate S,

$S = k^{-1}(h+ rx)$ mod q, if S=0, select different k.

Compute S, for (r_1, r_2, r_3…….r_n)
$S_1 = k^{-1}(h+ r_1x_1)$ mod q
$S_2 = k^{-1}(h+ r_2x_2)$ mod q
.
$S_n = k^{-1}(h+ r_nx_n)$ mod q

Digital Signature - {r, s }
Or {(r_1, r_2, r_3……. r_n)(S_1, S_2,S_3……. S_n)
Or multiple DS-
(r_1, S_1), (r_2, S_2)…….. (r_n, S_n)
Propose DSA also helpful to generate multiple signature for a single user if user having multiple secret keys.

C. Verification:-

- Generate message digest h, using same hash algorithm.
- So, compute w, S*w(mod q) = 1

For (S_1, S_2, S_3……S_n) the different value of w is(w_1, w_2, w_3…….w_n)

So,
S_1* w_1 (mod q) = 1
S_2* w_2 (mod q) = 1
.
S_n* w_n(mod q) = 1 a_1

- Compute, u_a= h*w(mod q)

  u_{a1}= h*w_1 (mod q)
  u_{a2} = h*w_2 (mod q)
  .
  u_{an}= h*w_n mod q
- Compute,

  V = ($g^u{}_a$ * $g^u{}_b$mod p) mod q
  V_1 = ($g^u{}_a$* $g^u{}_b$mod p) mod q
  V_2 = ($g^u{}_a$* $g^u{}_b$mod p) mod q
  .
  V_n = ($g^u{}_a$* $g^u{}_b$mod p) mod q
- If , V == r

Or (V_1, V_2, V_3……. V_n) == (r_1, r_2, r_3……. r_n)
Signature verified.

Mathematical Proof of Proposed DSA:

1) Let q=3, p=7, (p-1)mod q=0
g=4 (1<g<p)
g^qmod p=1
4^3mod 7=1
64mod 7=1
Select x, 0<x<q
if x= 1
Therefore y=g^xmod p
y= 4^1mod 7
y= 4mod 7
y= 4
Public key (p, q, g, y)= (7, 3, 4, 4)
Private key (p, q, g, x)= (7, 3, 4, 1)
Message hash value h=2
Therefore select k, 0<k<q, k=2
Compute r,

r= (g^kmod p) mod q

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 8, August 2015

r= (4^2mod 7) mod 3
r= 2
Compute s,
s = k^{-1}(h +r*r)mod q
s = 2^{-1}(2 +2*1)mod 3
s = 2^{-1}(4mod 3)mod 3
s = 2^{-1}(1)mod 3
s= 2
Signature (2, 2)
Verification
h = 2
Compute w,
S*w mod q=1
2*w mod 3=1
2*5 mod 3=1
Therefore w=5
Compute u1, u1=h*w mod q
u1 =2*5 mod 3
u1= 1
u2=r*w mod q
u2=2*5 mod 3
u2= 1
Compute v, v= (g^{u1} y^{u2} mod p) mod q
v = (4^1 *4^1 mod 7) mod 3
v = (16 mod7) mod 3
v = 2
Therefore v = = r
2= =2 (Verified)

2) Let q=3, p=7, (p-1) mod q=0
g=2 (1<g<p)
g^qmod p=1
2^3mod 7=1
8mod 7=1

Select x, 0<x<q
if x= 2
Therefore y=g^xmod p
y= 2^2mod 7
y= 4mod 7
y= 4
Public key (p, q, g, y)= (7, 3, 4, 4)
Private key (p, q, g, y)= (7, 3, 4, 2)
Message hash value h=2
Therefore select k, 0<k<q, k=1
Compute r,
r= (g^kmod p) mod q
r= (2^1mod 7) mod 3
r= 2mod 3
r= 2
Compute s,
s = k^{-1}(h +r*r)mod q
s = 1^{-1}(3 +1*2)mod 3
s = 1^{-1}mod 3 (5mod 3)
s = 1^{-1}mod 3*1
s= 1*2
s= 2
Signature (2, 2)
Verification
h = 2
Compute w,
S*w mod q=1
2*w mod 3=1
2*5 mod 3=1
Therefore w=5
Compute u1, u1=h*w mod q
u1 =2*5 mod 3
u1= 1
u2=r*w mod q
u2=2*5 mod 3
u2= 1
Compute v, v= (g^{u1} y^{u2} mod p) mod q
v = (4^1 *4^1 mod 7) mod 3
v = (16 mod7) mod 3
v = 2mod 3
v= 2
Therefore v = = r
2= =2 (Verified)

IV. CONCLUSION

Even though the utilization of cloud computing has improved in market, however it has quite a lot of protection problems like information correctness, integrity, availability and etc. Owner of the data do not want to be stolen his information or data loss in cloud. For that reason, high security and data availability need be maintained with in cloud.Security in a cloud environment requires a systemic point of view, from which security will be constructed on trust, mitigating protection to a trusted third party. The main purpose of this work is to survey the recent research done on single cloud as well as on multi cloud to solve the security issues faced by the data owners and to provide the high level security.

REFERENCES

[1] http://blog.cloudflare.com/ecdsa-the-digital signature - algorithm-of-a-better-internet
[2] Rahul Bhatnagar, SuyashRaizada, PramodSaxena, SECURITY IN CLOUD COMPUTING, International Journal For Technological Research In Engineering, ISSN (Online) : 2347 4718, December – 2013.
[3] Mohammed A. AlZain, Ben Soh and Eric Pardede, MCDB: Using Multi-Cloudsto Ensure Security in Cloud Computing, 978-0-7695-4612-4/11, IEEE, 2011
[4] Kuyoro S. O, Ibikunle F, Awodele O, "Cloud Computing Security Issues and Challenges" International Journal of Computer Networks (IJCN), Volume (3) : Issue (5) : 2011
[5] Kuyoro S. O, Ibikunle F, Awodele O, "Cloud Computing Security Issues and Challenges" International Journal of Computer Networks (IJCN), Volume (3) : Issue (5) : 2011.
[6] Mohammed A. AlZain, Ben Soh and Eric Pardede, A New Approach Using Redundancy Technique to Improve Security in Cloud Computing, Department of Computer Science and Computer Engineering, La Trobe University, Bundoora 3086, Australia.
[7] Rahul Bhatnagar, SuyashRaizada, Pramod Saxena, SECURITY INCLOUD COMPUTING, International Journal For Technological ResearchIn Engineering, ISSN (Online) : 23474718, December - 2013.
[8] Takabi H, Joshi J. (2010) 'Security and Privacy challenges in Cloud Computing Environment', Security & Privacy, IEEE, vol. 8, no. 6, December, pp. 24-31.