International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 2 Issue 8, August - 2013

Cluster Ciphering for Data Security in Cloud

Ms.A.Baby Mr. D.Srujan Chandra Reddy Mr. A.Hari Prasad

***Abstract- In the present computing environment super computers* are having capability of running PFLOPS of Instructions, to solve complex problems. If this is applied to the security system for breaking public or private keys of an encryption algorithm over the sensible data networks like defense and military it might be a threat to the country. Here we are working with typical algorithm which handles the bunch of Encryption/Decryption methods and process data for security, this process is known as cluster ciphering.**

I. INTRODUCTION

Breaking of security is depending on the algorithm used for encryption and key generation method. In the present method of security there might be a problem of security issue if the intruder or a hacker tries well on the security breaking. Because of limited use of encryption/Decryption algorithms. We can overcome that by using encryption/decryption algorithms widely and systematically. In our system we are having two methods to implement the systematical use of more than one encryption/decryption algorithm.

II. CLUSTER CIPHERING

As we know that converting plain text to cipher/coded text is called ciphering. In this study we are performing this ciphering many times depends on pattern. The encryption/decryption algorithms are classified into two types depends on their key, if an algorithm having same key for both encryption/decryption it is symmetric cryptographic algorithm, if an algorithm uses two different keys for two operations (encryption/decryption) it is asymmetric cryptographic algorithm. Using more than one algorithm for cryptography is called cluster ciphering. In this study we are having two types of cluster ciphering techniques, namely Homo cluster ciphering and Hetero cluster ciphering. Whatever the cluster ciphering method we need to have ten cryptographic algorithms. If licenses available then ok, else use own plain encryption algorithms.

III. HOMO CLUSTER CIPHERING

In this method only one class of ciphering mechanism is used for ciphering, i.e. either symmetric or asymmetric cryptographic algorithms depends on logic. But the preferred one is asymmetric. After collection of algorithms we need to index them with numbers like 0,1,2,3,4,5,6,7,8,9. These numbers are used while calling the algorithm for encryption or decryption.

ALGORITHM:

BEGIN
Step 1: Generate seven/nine digit random prime number.

Step 2: Select 3and 5 position of the random prime number.
Step 3:
If selected positions forms even number

Then use asymmetric cryptographic algorithms for encryption/decryption process in the order of that random prime number.

Else

Use the symmetric cryptographic algorithms in the order of random prime number.
END

Ex:

Name algorithms of two kinds with numbers0,1,2,3,4,5,6,7,8,9
Then generate seven digit random prime number 1705829.
Observe the third and fifth position numbers.

1 2 3 4 5 6 7

1705829

These numbers are forming 08, i.e. even number.
So now it has to take asymmetric algorithms for encryption or decryption process. The order of encryption is like Algorithm with index number 1 and next with 7 like up to the completion of 7digits Refer table1.

INDEX	ALGORITHM	ORDER OF EXECUTION
0	ALG0	3
1	ALG1	1
2	ALG2	6
3	ALG3	--
4	ALG4	--
5	ALG5	4
6	ALG6	--
7	ALG7	2
8	ALG8	5
9	ALG9	7

Table: 1

Now the data which is encrypted by this process is hard to threaten by attacks in various types.

IV. HETIRO CLUSTER CIPHERING

This cluster type is typical compared to homo cluster. Because, here we will use both classes of encryption algorithms. So this is very robust one compare to previous one. Process is same as homo cluster up to numbering the algorithms with index. After generation of random prime number we will use both the algorithms alternatively depends on the number formed by three and five locations of the random prime number. The reason for selecting minimum seven digit prime number is 1) Number is lengthy. 2) If we generate 5 digit prime number then number formed by 3 and 5 position is always odd. But in seven digits there is no such case. 3) Positions three and five are both odd and prime.

ALGORITHM:

BEGIN
Step 1: Generate seven/nine digit random prime number.

Step 2: Select 3and 5 position of the random prime number.
Step 3:

If selected positions forms even number

Then first encryption algorithm is asymmetric and next is symmetric alternatively.

Else

The first encryption algorithm is symmetric and next is asymmetric alternatively.
END

Ex:
Name algorithms of two kinds with numbers0,1,2,3,4,5,6,7,8,9
Then generate seven digit random prime number 4301789
Observe the third and fifth position numbers.

1 2 3 4 5 6 7

4301789

These numbers are forming 07, i.e. odd, so first position numbered symmetric encryption algorithm executes first the next position is with asymmetric encryption algorithm, observe table 2.

INDEX	ALGORITHM	ORDER OF EXECUTION
0	SALG0	3
1	ASALG1	4
2	SALG2/ ASALG2	--
3	ASALG3	2
4	SALG4	1
5	SALG5/ ASALG5	--
6	SALG6/ ASALG6	--
7	SALG7	5
8	ASALG8	6
9	SALG9	7

Table: 2

Here in table 2 SALG means symmetric algorithm and ASALG means asymmetric algorithm.
The decryption process is also reverse of the same processes.

Compare to homo cluster ciphering this hetero cluster ciphering is providing security in a high level. If the secured data is encrypted with this mechanism we can achieve surety on security.

V. APPLYING CLUSTER CIPHERING TO CLOUD

The most sounding computer technology right now is cloud. Whereas cloud has its own Advantages and disadvantages. The disadvantages are majorly because of no standard architecture, security measurements and security diagnostic mechanism. The first and foremost thing to do is, hiding the data from unauthorized access, when it is compromised we have to make the data un-useful to that party by making the data into encrypted format. In all such cases we can implement the cluster ciphering for data security in cloud.

VI. CONCLUSION

Security providing for data using this method needs more computing resources. As the data is securable, there should be no compromising of resources allocation. Even though this method provides security there must be a need of optimization. We will extend this study for the optimization of this method as advanced for this in future.

REFERENCES

[1] A.HariPrasad" Assurance on Data Storage Security in Cloud Computing" (IJERT) Vol. 1 Issue 5, July – 2012, ISSN: 2278-0181

[2] "RSA Algorithm", Pekka Riikonen, 29.9.2002

[3] D.Wagner, B.Schneier, Analysis of the SSl 3.0 protocol, 2nd USENIX workshop on Electronic commerce, 1996.

[2] Kapil Bakshi"Cisco Cloud computing –datacenter strategy, Architecture, and Solutions", point of view white paper, 1st Edition.

[4]"Microsoft Dynamic CRM Online "Guide, version 1.o-JUNE 2011. Gartner1:1, 2011, Jones Lang LaSalle

[5] " Cloud Security Issues", Balachandra Reddy Kandukuri, Ramakrishna Paturi V, Dr.Atanu Rakshit, 2009 IEEE International conference on service computing

[6] "A Break in the Clouds: Towards a Cloud Definition", Luis M.Vaquero, Luis Rodero-Merino, Juan Caceres, Maik Lindner- AC SIGCOMM computer communication Review , volume 39, Number 1, January 2009.