IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-5, Issue-12 E-ISSN: 2347-2693

An Algorithm for Encrypted Cloud Communication

Sanketh S. Iyer[1], Hiren Dand[2*], Rajendra Patil[3]

[1]Department of Information Technology, PTVA's Mulund College of Commerce (University of Mumbai), Mumbai, India
[2*]Department of Information Technology, PTVA's Mulund College of Commerce (University of Mumbai), Mumbai, India
[3]Department of Information Technology, S. K. Somaiya College (University of Mumbai), Mumbai, India

**Corresponding Author: dandhiren@yahoo.co.in, Tel.: +91-9821140717*

Available online at: www.ijcseonline.org

Received: 12/Nov/2017, Revised: 19/Nov/2017, Accepted: 02/Dec/2017, Published: 31/Dec/2017

***Abstract*—** Internet has assumed control over everything a rapid pace. With the growth of Internet, we tried to discover way through which we can exploit the internet to the fullest and reap its benefits. Cloud Technology was a result of such brainstorming. With Cloud, we could achieve great deal of benefits. This included access to our resources anytime, anywhere and at a very fast pace. This made the task of various organizations very easy as they could store data over these cloud servers and access them from anywhere at any time. Furthermore, this also brought down the costs for the organization, as they need not invest in creating data centers and servers. In spite of all benefits we are still today unsure about how secure is actually our data on cloud servers and whether our communication with this server is actually secure. The algorithm proposed in this paper when implemented provides a secure way to communicate and store data in cloud servers.

***Keywords*—**Cloud Computing, Encryption,Decryption,Algorithm, Key-Pair

I. INTRODUCTION

Cloud computing is gradually overwhelming the web. This is because of many organizations adapting to Cloud Technologies for storage and recovery of data.

A wordbook calls cloud computing as follows: - "the *act of using an arrangement of remote servers on the web to store regulate and process information, instead of local servers."*

We have not realized that cloud has rooted in so much into our lives that we are using it even without realizing that we are using cloud services.

A cloud is a set of virtual resources either software or hardware which may be accessed by users on pay-per utilization basis.

In the upcoming sections, we would be going through the working of cloud, its features, Types of cloud, Security concerns in cloud, Encryption, The AES and RSA Algorithms and finally would be proposing our algorithm and concluding highlighting the benefits of this algorithm.

II. WORKING OF CLOUD[2]

Its working varies from provider to provider. However, we can give a common framework based on the definition given above.

A client and a remote cloud server exists where the client can store, retrieve and work on his data.

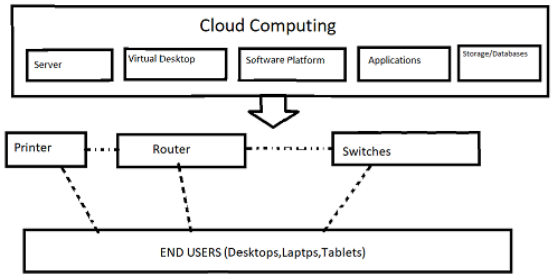

Figure 1: Block diagram of cloud Architecture

As shown above and said earlier, end user using internet accesses the resources, which are on a cloud server.

III. WHY THE NAME CLOUD?

We are aware that clouds keep on moving in the sky, but we are unaware of its exact origin. It is the same with cloud servers, the client need not be aware of its origin. What the client is concerned is about his/her data being accessible from anywhere anytime.

A cloud is an IT service where this cloud provides a virtual space to store large data, which is available anytime and anywhere for the end users.

IV. FEATURES OF CLOUD[1]

A. Provision for Self-Service

The resources can be utilized for any kind of work irrespective of any limitations in the end systems

B. Flexibility

The property of handling any number of users and multiple type of information varying user to user.

C. Pay-per-Utilization

Clouds are available free until some extent however for organizational deployment it is available as a paid service, and this charge is nominal and can't impact an organization considering the innumerable benefits it offers.

D. Maintenance of Cloud Servers

End users need not be concerned about maintenance of cloud servers and are the responsibility of the service provider. Much of the servers are offsite and are able to handle themselves without any manual interventions.

E. Location Independence

Anyone can use and access cloud services from anywhere anytime with no impediments.

F. Backup

Cloud backups save time and very reliable. End users can save on their system space and organizations need not invest in third party backup software of data centers.

G. Cloud-based workload and file sharing.

This enables users to share their data and access them from anywhere, which streamlines teamwork and cooperation.

V. CLOUD SERVICES – TYPES [6][7]

They can be classified into 3 types viz. IaaS, PaaS and SaaS.

A. IaaS

This is the basic form of all cloud services. With this we can take on rent all IT infrastructure elements like VM's, Storages, Networking, Operating Systems etc.

B. SaaS

This delivers applications using cloud. With this the cloud providers are able to manage and host the software on the internet on subscription basis. They handle all the maintenance and upgradation activity with regards to this. Customers can access this application from any devices like Tablets, Mobile Phones, Laptops or Desktops etc.

C. PaaS.

This is a way to provide an on-demand environment for software development and testing.

VI. CLOUD DEPLOYMENT TYPES[2]

Cloud deployments maybe split into three as below: -

A. Large cloud corporations operate **Public Clouds**. One can take service from them on pay per utilization basis.

B. A **Private Cloud** is deployed by organizations for its own use. They may be located in the company's on site datacenter. Some company's may ask third party service providers to provide them with private cloud services.

C. **Hybrid Cloud** is an amalgamation of above two services bound by technology that enables information and applications to be shared between them. By enabling information and applications to move between above two clouds, hybrid cloud gives organizations adaptability that is more prominent and greater deployment choices.

VII. CONCERNS ABOUT CLOUD SECURITY.[3][4]

Below are some points that explain security concerns of cloud: -

A. Problems with Data

However, the service of cloud maybe provided, there is user data or organizational data associated with it. This leads to our main concern," How secure is our data on cloud servers?" Secondly, we come across the question that "Is our data transmission to these servers in a secure form?"

Most of the attacks in cyber space are targeted at user's organization servers. To avoid this, they are considering moving the data onto cloud servers.

There is a need to secure the communication including the storage of data both of which can be secured with the help off strong encryption algorithms.

B. Infection issues

Any lay user can upload a malicious program in the cloud server and can try to remotely execute it. This will put the data of all the users at risk.

C. Other Security Issues

The other security issues may involve: -

1) *D-DoS Attacks*
2) *Location Transparency*
3) *Network Security*
4) *Data confidentiality issue*

VIII. ENCRYPTION[1]

Encryption is the process by which electronic data is converted into an encoded cipher text that can only be decoded by authorized parties.

There are two types of Encryption: -

A. Symmetric Key Encryption

Here both encryption as well as decryption is performed using a same key.

B. Asymmetric key encryption

Here the encryption uses an open key(public key) and decryption is achieved using a secret(private) key.

Both have specific advantages and are deployed considering various factors.

Here, we would be using RSA and AES algorithm to achieve a strong encryption mechanism for cloud data transmission and storage.

IX. RSA ALGORITHM.[1]

RSA is Rivest-Shamir-Aldeman Algorithm. It is a non-symmetric key algorithm. This means that this uses a key pair (Public-Private).
Simple working of an Asymmetric Key Cryptography is as given below.
A client application sends its public key to the server requesting some data.
The server encodes the response with client's open (public) key and reverts.
Client gets this information and decodes it using Private Key.
This key-pair should be uniquely created for every specific user. These keys are generated combining two very large prime numbers, the concept behind which is that these large prime numbers cannot be factorized.

A. Generation of Public key for RSA Algorithm

1. Let us take two large prime numbers.
   Ex. N=P1 and M=P2.
2. First part of the public-key is obtained as follows =>n=P1*P2= ABCD.
3. Now we select an exponent e satisfying the following conditions: -

a. It must be an integer
b. It must not be a factor of n
c. 1<e<k(n)[k(n) which is explained below]

4. The public-key is made from n and e.

B. Generating the private-key for RSA Algorithm

1. Calculate k(n) = (P1-1)(P2-1)
2. Now our private key(m) will be obtained as m=(I*k(n)+1)/e where I is an integer.

This Key Pair must be unique & generated for each individual users/Organization.

C. Encryption using RSA:

Encryption is achieved by the following formulae: -
$E.T= (P.T.)^e \bmod n$

D. Decryption using RSA

Decryption is achieved by the following formulae: -
$P.T=(E.T)^m \bmod n$

X. AES(RIJNDAEL) ALGORITHM[1]

AES stands for Advanced Encryption Standard. It is a symmetric-key and a block Cipher algorithm. It works using 128/192/256-bit keys. It is very fast, in fact stronger and quicker than triple DES.
We will be using AES to encrypt our client server communication.

For a particular session, we will be using a random generated 128-bit Symmetric AES key to secure all our communication between client and Server.

A. Working of AES(Rijndael) Algorithm[9][10]

The following steps are followed in the Encryption Operation of AES: -
When using a 16 byte key, the algorithm runs for 10 rounds, the 10th round being slightly different. Each round uses a unique 16-byte key called round key that is obtained from the initial key value though calculation. Each round has the following steps: -

1. Byte based substitution
2. Shifting Rows
3. Mixing Columns
4. Round Key Addition

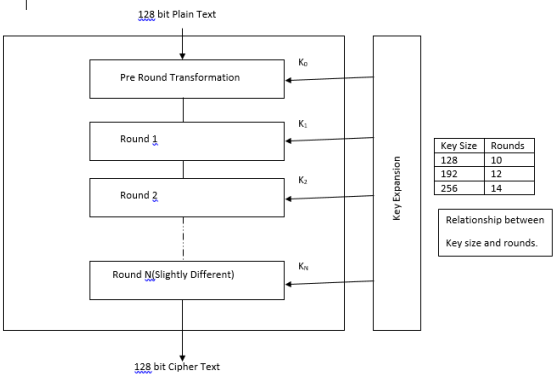

Figure 2: Rounds of AES Algorithm

The above diagram shows how the AES algorithm works overall, we now would see the encryption process: -

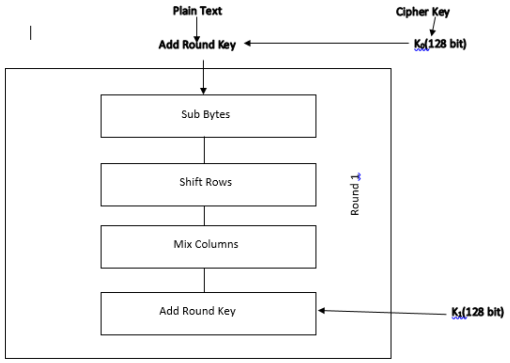

Figure 2: Steps of AES Algorithm

1) Byte based substitution

The 16 input bytes substitution is done with reference to a standard S-Box table.

2) Shifting Rows

Each of the four rows of a matrix is moved one position to the left. The shifting process is as follows: -

i. Do not shift the first row.
ii. Shift the second row one (byte) position to left.
iii. Shift the third row two positions to left.
iv. Shift the 4th Row three positions to the left.
v. The resultant matrix is the same with elements shuffled in the matrix.

3) Mixing Columns

Each section(column) is processed using a unique numerical function. This takes input 4 bytes of a section(column) of that matrix and outputs a completely new byte set of same length. The resultant matrix consists of new 16 bytes***. This is avoided in the final round.***

4) Round Key Addition

XOR is performed with 128 bit key (round key) and the 16 byte matrix split as 128 bits.

In case of the last round, the output is the encrypted text else, this is considered as another 4x4 matrix and the complete process begins again.

B. AES Decryption Process:

The reverse process in AES(decryption) is similar with the only difference being that of the steps are performed differently.

Below are the steps for AES decryption: -

Each round has 4 steps performed in the reverse order:-

1. Round Key Addition
2. Mixing Columns
3. Shifting Rows
4. Byte based substitution
5.

C. Strength of AES:-

It is a very fast and reliable algorithm that does not take much overhead.

Till date no practical attacks using cryptanalysis against AES has been discovered. It is supported by most of the hardware's and software's. Again, as DES, AES's strength lies on correct implementation and good key management practices.

XI. IMPLEMENTING OF RSA AND AES FOR SECURE CLOUD COMMUNICATION.

The following steps how we tend to achieve a secure cloud communication using the above algorithms: -

A. Prerequisites:-

1. Every user is allocated unique Public Private Key-pair.
2. A Random AES Key generated for the session.
3. A Random Public Private Key for one-time key exchange.

B. Algorithm:-

a. Client Establishes connection with server and demands a public key(P_k).
b. The server creates a random Public-private Key Pair (P_k ,P_r).
c. Server sends this key to the client(P_k).
d. A random encryption key(E_k) is generated by the client, encrypts it with Server's public key(P_k) and send it to the Server.
e. Server decrypts this key using the private key(P_r) and obtains the Client Key(E_k).
f. Server Generates the AES Session Key(S_k), encrypts it using the AES Algorithm using the Key provided by the client(E_k) and sends it to the client.
g. The client receives the Encrypted AES Session Key[$E(S_k)$].
h. It decrypts it using the AES algorithm and stores it.
i. Now the Client has Session Key(S_k).
j. The client now demands the unique Public-Private Key Pair from the Server for the respective user ID.
k. The Server Responds by encrypting this key pair (P_1,P_2) using the AES algorithm using the determined Session Key(S_k).
l. The Client Receives the Encrypted Public Private Key-Pair [$E(P_1,P_2)$], Decrypts it and stores it(P_1,P_2).
m. All communication between client-server is now encrypted by Rijndael(AES) algorithm using the unique session key.

C. Encrypted Communication.

1. Whenever the client wants to upload data, the client first encrypts all data with RSA Algorithm with the public key(P_1).
2. This data is now encrypted using the unique session key(S_k) and transmitted to the server.
3. Decryption of the received data is done first using the Session Key(S_k)(AES), then using the Private Key(P_2)(RSA) at the server and then it is stored.
4. Whenever the client requests for data, the reverse is done.
5. Data encryption is done by the server first using public Key(P_1)(RSA) then it encrypts it again using Session Key(S_k) before transmitting it over the network to the client.
6. The client first decrypts the data using Session Key(S_k)(AES) and then again using private Key(P_2) before finally possessing the required information.

7. In this way, multiple encryptions secure the whole cloud communication process.

XII. FEATURES OF THIS ALGORITHM.

1. MITM Attack is impossible since the beginning all the communication is encrypted using unique keys. Sniffing would yield only encrypted information.
2. Strength of AES is such that cryptanalysis is only a failure.
3. Even if the attacker is successful in breaking into the packets by decrypting the AES encrypted data, he would only land on to encrypted data again.
4. Since the session keys are unique and regularly discarded and changed session to session, the attacker cannot perform a pattern analysis.
5. RSA and AES are known to work very fast and does not pose a serious risk in performance.

XIII. CONCLUSION

Cloud technology has risen and is dominating the IT industry very fast. Most of the things are now on cloud including lay users and large corporate organizations implementing cloud for their use. The algorithm proposed in this paper can aid in making cloud communication even more secure.

REFERENCES

[1] A. Kahate, "*Cryptography & Network Security*", McGraw Hill Publications, India

[2] M.R.Shinde,R.D.Taur,"*Encryption Algorithm for Data Security and Privacy in Cloud Storage*", American Journal of Computer Science and Engineering Survey, Volume 3,Issue 1,pp 1-6,2015

[3] V.Alangar, "*Cloud Computing Security and Encryption*",International Journal of Advance Research in Computer Science and Management Studies,Volume 1,Issue 5,pp 1-3,2013

[4] Rashmi P., Bharathi R.K., Shruthi Prabhakar, Reshma Banu, Rachana C.R., "*Performance Analysis of Self Adaptive Image Encryption Technique*", International Journal of Scientific Research in Network Security and Communication, Vol.5, Issue.3, pp.44-58, 2017.

[5] S.S.Khan, R.R.Tuteja, "*Security in Cloud Computing using Cryptographic Algorithms*", International Journal of Innovative Research in Computer and Communication Engineering,Volume 3,Issue 1,pp 1-2,2015

[6] S.Kumar, R.H.Goudar, "*Cloud Computing – Research Issues, Challenges,Architecture, Platforms and Applications: A Survey*",International Journal of Future Computer and Communication,Volume 1, Issue 4,pp 1-3,2012

[7] Shaheen Ayyub, Devshree Roy, "*Cloud Computing Characteristics and Security Issues*", International Journal of Computer Sciences and Engineering, Volume 1, Issue 4, pp1-5, 2013

Authors Profile

Mr. Sanketh Iyer completed Bachelors Degree in Information Technology from University of Mumbai. Presently, he is pursuing his Master's Degree in Information Technology from University of Mumbai. He is working as an Associate Consultant with cyber security firm Sequretek. He has completed various certifications including EC Council's Ethical Hacking, Security Analysis, Penetration Testing and Forensic Analysis and is presently working on to research more to make the digital space safer.

Dr. Hiren Dand completed his B.E. in Electronics from University of Mumbai, M.Tech in Information Technology from AAIDU and Ph.D. in Computer Engineering on "Increasing Energy Efficiency of Mobile Phones by Offloading tasks to Cloud" from Shri JJT University. He has published research papers on various topics in national and international journals. He has authored several books like PL/SQL, R, Web Programming, OOPs, Internet Technologies and more. He has been awarded Lifetime Education Achievement award for his outstanding achievements and remarkable role in the field of Education by National and International Compendium, New Delhi. His research areas include security, cloud computing, virtualisation, mobile cloud computing, data analytics, networking and the likes.

Dr. Rajendra Patil completed his B.Sc in Computer Science, M.Sc. in Computer Science and Ph.D. from North Maharashtra University, Jalgaon. He is the Head of Department of Information Technology at S. K. Somaiya College. qualified a State Eligibility Test for Lecturer ship (SET), in the subject of Computer Science and Applications. His topic of research was "Design and Development of a tool for automatic donor matching in sperm banks and IVF Centres using data mining techniques". His work focuses on designing an expert system using machine learning techniques for donor matching. He has published research papers on various topics in national and international journals. He is Life member of Indian Science Congress, India. He has received Best HOD award from Computer Society of India, in National conference organized by IIT Powai, Mumbai in TechNext 2017.

