IJARCCE

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

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 6, June 2017

Security Framework for Sharing Data in Fog Computing

V.K. Sowjanya[1]

PG Scholar, Department of CSE, MVGRCE, Vizianagaram, India[1]

Abstract: Cloud computing is an attractive criterion for accessing virtually unlimited storage and computational resources. Cloud computing has many advantage, but providing the data confidentiality in the cloud is major concern. The major disadvantages in the cloud computing is high latency, limited mobility, slow response time because data is transferred through Multiple hops. And it is centralized Geo-distribution. In Our System, we propose the Fog computing which address the above problems faced by cloud computing. Fog computing is a criterion which extends the cloud computing and its services to the network edge. It can’t replace cloud. It extends the cloud computing by providing the security in the cloud atmosphere. Fog has many advantages when compared to the cloud i.e., less data traffic, low cost and latency. It also eliminates the overhead to the centralized computing system, and security is high because data moves across the edge of the network so response is quick. Still there are many advantageous in fog computing, but some of the security issues also taken into consideration while transferring the data. In our system we focus on providing the security to the data while transferred via cloud. Here Outsourcer sends the encrypted data along generated key (cipher key/encrypted key) to the data user via Fog Server. Using that encryption key the user decryption is performed and then viewed the original data. This Cipher key is generated by the Modified ELGAMAL algorithm which provides the better security than the existing algorithm.

Keywords: Fog Computing, Cryptography, ElGamal, Cipher key.

I. INTRODUCTION

Fog computing is mainly used for Internet of Things. From network centre, Fog computing obtain data and services to the network edge. Similar to Cloud, Fog also data, compute, storage, application services are given to the end-users. The services and applications of fog are distributed that means fog fetches the data storage, processing and application. Fog computing is a distributed computing model that from the centralization to the network edge device such as set top box, access point. Fog computing is hosted locally so the user uses the service. Instead of sending to cloud Fog computing provides IOT data processing, storage, it is locally processed in smart devices. The purpose of both Cloud and fog are for compute, storage and networking resources. In fog computing, instead sending the collected data by sensors to the cloud server it is sent to devices such as network edge or set top box, routers, access point for processing. By doing this, the traffic is reduced due to low bandwidth. Fog computing enhance the Quality of service and also latency is reduced. Small computing works are processed locally and end users get the responses back without the use of cloud. For smaller computing works, Fog computing is better option compared to the cloud computing. Fog computing reduces the data traffic to the cloud. Since fog system provides better response time without delaying. Good example for Fog Computing is jet engine. Suppose jet engine is connected to the internet, 10 TB of data is created by jet engine within half an hour running time. For this huge data more bandwidth is needed. Fogging is complemented to cloud. Some features in fog computing differentiate from the cloud, the purpose of Fog Computing is real time interactions but it can’t replace cloud computing as it preferred for high end batch processing. As the name suggests cloud system is placed at a distant where as the fog system is placed locally near to the end user.

Advantages:

1. The environment of core computing is eliminated so reduce a major block and a point of failure.
2. Security is high, as data are concealed as it is moved towards the network edge.
3. Edge Computing provides the faster response to the end users because of it has only one hop.
4. It also provides high levels of scalability, reliability and fault tolerance.
5. Bandwidth consumption is less.
6. It supports mobility.
7. Low latency.
8. Good Location awareness.

Disadvantages:

1. The problem with Fog computing is nobody can identify the attacker when data is interrupted.

DOI10.17148/IJARCCE.2017.6676

2. And identification of the attacker is highly complex.
3. Can't detect which file is hacked.

II. LITERATURE SURVEY

KalyaniKadam, Rahul Paikrao, AmbikaPawar [1] discuss the security issues in cloud computing and also solutions to handle the some security issues. Some of the security aspects for providing the security are Confidentiality, Authentication, Non repudiation, Availability, Integrity, Authorization, Privacy, etc. Some of the security issues and challenges in the Cloud Computing are security problem inherited from Network and Virtualization, Security problem concerning the location of cloud systems, Threats to cloud computing by discovered by CSA.

T.RajeshKanna, M. Nagaraju, Ch. Vijay Bhaskar [5] discuss about how to secure the personal and business data in the Cloud. Any malicious insider illegal access to someone's document in cloud, profiling user behaviour continuously determines the number of times user entered. If any deviation observed from user the attack is identified. The user profile management ensures that the legitimate users' behaviour and navigational patterns are recorded. The decoy technology allows the application to keep decoy information or bogus information in the file system to deceive insider data theft attackers.

Nisha Peter [6] discussed application areas of Fog Computing and how it is useful in those fields are described. Some of the application areas of Fog Computing are Smart Grids, Smart Traffic lights, Self Maintaining Train, Wireless Sensor and Actuator Networks (WSAN), Decentralized Smart Building Control, IoT and Cyber-Physical Systems (CPSs), Software Defined Networks (SDN), Health Care, Mobile computing system.

Shakeeba S. Kha1, Prof. R.R. Tuteja [2] discuss about to enhance the security on cloud different cryptographic algorithms are considered. Cryptography is an art of keeping the messages securely by transforming the data into unreadable format. Existing algorithms RSA and DES are single level encryption algorithms. Cyber criminals easily hack the data which is encrypted by single level. So, in this paper discuss the multi-level encryption and decryption for providing more security. So the multilevel encryption only authorized uses gets access the data. Any intruder tried to access the data the intruder must perform the decryption at each level without having a valid key.

Dr. S. S. Manikandasaran [3] discussed about the rapid growth and features of cloud faces many security problems. The different types of attacks are described in this paper. Some of the attacks are Man-in-the-middle attack, Brute Force attack, Network Sniffing, Side channel attacks, Port scanning, Cross Site Scripting. By using the authentication mechanism protect the authentication mechanism. But it is difficult to protect the data from insider's attacks. A new technique or mechanism is necessary for ensuring the confidentiality to data which is stored in cloud. If these issues are resolved then users get more benefits from cloud.

III. DATA SECURITY IN FOG USING CRYPTOGRAPHY

There are many advantages in Fog computing, some security issues consider while transferring the data such as Man-In-Middle-Attack. So In our system we protect the transferred data by sending the encryption or cipher key along with data using modified ElGamal algorithm. Here data is some message and image. Here message converted into cipher text before sending via cloud and also image is over lay by some clumsy image. And also generated encryption or cipher key is sent along with encrypted message and image to the receiver for decryption process. By using the cipher key first perform the decryption and view the both message and image.

Work Flow

User:
1) Register an account
2) During the registration primary key is generated.
3) Login into the account using primary key at the same time one private key is randomly selected.
4) Select a member to data to be shared.
- Select member
- Encrypt the data
- Generate one Cipher Key/Encryption key using Modified ElGamal Algorithm. The Generated Encryption Key is sent along with encrypted data to the receiver.

5) Receiver receives that Cipher/Encryption key.
6) Using that Encryption key Receiver performs the decryption, the receiver view the original data.

DOI10.17148/IJARCCE.2017.6676

Algorithm

Existing ElGamal:

ElGamal cryptosystem is an Asymmetric key cryptography means different keys are used for encrypting and decrypting the messages. This algorithm provides alternative to the RSA for public key encryption.

ElGamal algorithm consists of 3 components

a) Key generation
b) Encryption
c) Decryption

Process

Step1: First Prime number **P** and a number **g** are generated by Bob. **'g'** must be between the 1 and (p-1).

Step 2: Bob randomly choose his private key **x** then calculates

$$Y= G^{x}modP$$

Step 3: Bob sent these **P, g, Y** to the Alice. Then a message **M** is created by Alice. Select one random value **k** then calculate below values

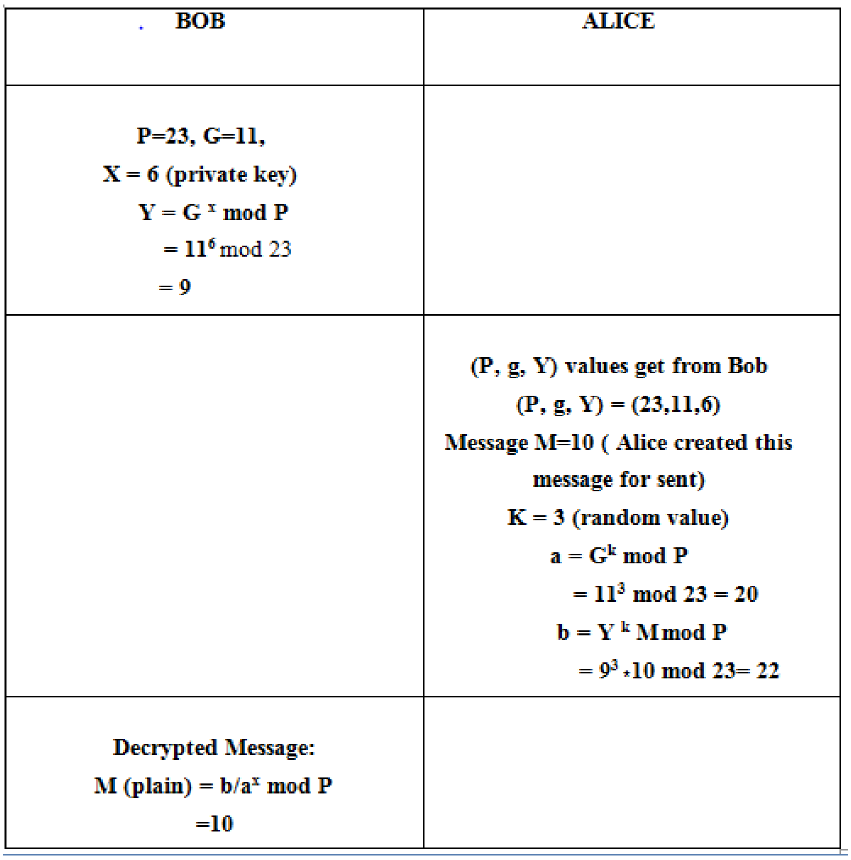
$$a = G^{k}modP$$
$$b = Y^{k}MmodP$$

Step 4: Bob decrypts the message by

$$M = b/a^{x} \bmod P$$

The following table describes the encryption and decryption procedure for ElGamal algorithm

TABLE I ENCRYPTION AND DECRYPTION PROCESS IN ELGAMAL ALGORITHM



BOB	ALICE
P=23, G=11, X = 6 (private key) $Y = G^{x}$ mod P $= 11^{6}$ mod 23 = 9	
	(P, g, Y) values get from Bob (P, g, Y) = (23,11,6) Message M=10 (Alice created this message for sent) K = 3 (random value) $a = G^{k}$ mod P $= 11^{3}$ mod 23 = 20 $b = Y^{k}$ Mmod P $= 9^{3} * 10$ mod 23= 22
Decrypted Message: M (plain) = b/a^{x} mod P =10	

Advantage

The advantage of this algorithm is different cipher text is obtained by same plaintext when it is encrypted each time.

Disadvantage

-Cipher text is double to the plain text.
-Only one user have public key.
-Only one user performed either encryption or decryption.

Modified ElGamal Algorithm:

The Modified ElGamal is used for only key generation instead of taking the plaintext randomly. ElGamal algorithm is modified for improve the security by generating different prime for each user and also each user has own public key. And Users prime and public key is shared with each other when both users want to share the data. In this process the sender can't perform the encryption without receiving the receiver's prime and public key and as well as the receiver can't perform the decryption without receiving the senders prime and public key.

The Modified ElGamal algorithm also consists of 3 components i.e.

Key generation, Encryption, Decryption

Process:

Step 1: Alice and Bob calculate their public keys using their prime number, generator and their private keys.

Step 2: After, they share Prime and Calculated their public keys is shared to each other except their private keys. Then Alice chooses one random number that is indicated by **Master key**.

Step 3: Calculate **Cipher key** using that master key and Bob's public key and prime and his own private key. And this Cipher key is sent to the Bob.

Step 4: Then Bob decryption process begins by using Cipher key, Alice public key and his private key. At last Bob find Master key by using Cipher key (which is sent by Alice), Alice public key and his private key. Then decryption process completed.

Advantages

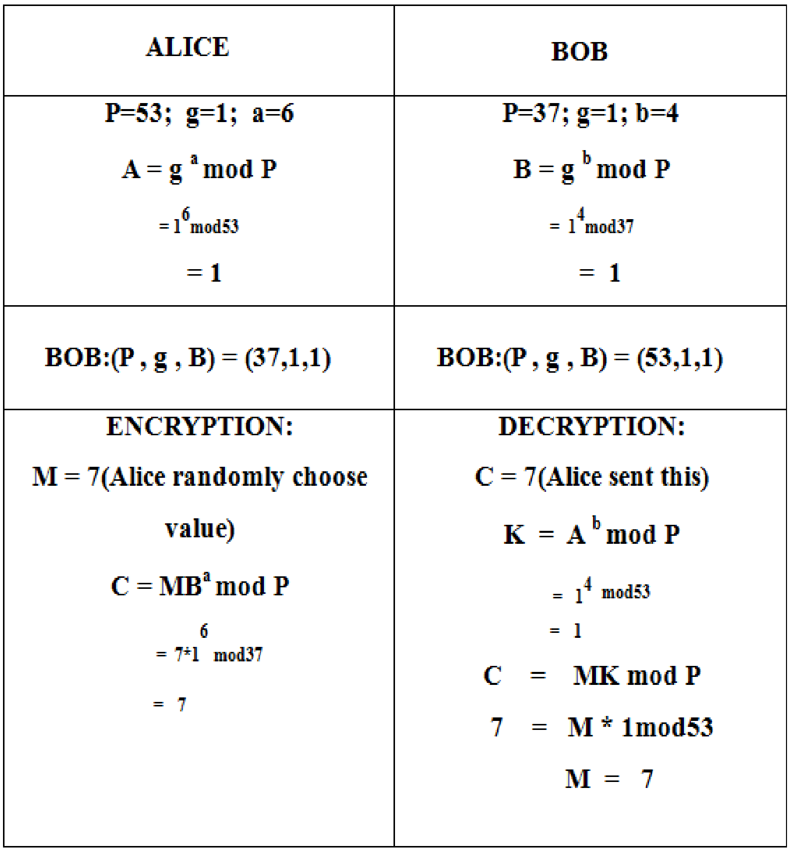
-Each user has different prime numbers.

-Every user has their separate public keys. So advantage of this is each user performs both performs encryption and decryption operation

-Without sharing their public keys and prime the encryption and decryption can't be performed. If any user wants to share any data, sender must take receivers prime and public keys to perform encryption and also receiver perform the decryption by taking senders prime and public key.

The below table describes the encryption and decryption process in Modified Elgamal Algorithm.

TABLE II ENCRYPTION AND DECRYPTION PROCESS IN MODIFIED ELGAMAL ALGORITHM



ALICE	BOB
P=53; g=1; a=6 $A = g^{a} \bmod P$ $= 1^{6}$ mod53 = 1	P=37; g=1; b=4 $B = g^{b} \bmod P$ $= 1^{4}$ mod37 = 1
BOB:(P , g , B) = (37,1,1)	BOB:(P , g , B) = (53,1,1)
ENCRYPTION: M = 7(Alice randomly choose value) $C = MB^{a} \bmod P$ $= 7*1^{6}$ mod37 = 7	DECRYPTION: C = 7(Alice sent this) $K = A^{b} \bmod P$ $= 1^{4}$ mod53 = 1 C = MK mod P 7 = M * 1mod53 M = 7

DOI10.17148/IJARCCE.2017.6676

IV. RESULTS AND DISCUSSION

The below table and graphs describes the Encryption time and Decryption time for number of times different data (message and image) sent from sender to receiver.

TABLE III ENCRYPTION AND DECRYPTION TIME

Execution Attempts	E-time (ms)	D-time (ms)
1	4	5
2	3	6
3	5	7
4	4	6
5	3	5
6	3	6
7	3	4
8	3	4
9	4	5
10	5	6
11	5	7
12	3	8
13	4	5
14	5	6
15	3	5
16	4	5
17	5	7
18	6	8
19	4	5
20	5	6

The below graph describes the Encryption and Decryption time for different size of data sent from sender to receiver. The result shows that average encryption and decryption times are almost same for multiple numbers of data being encrypted and decrypted.

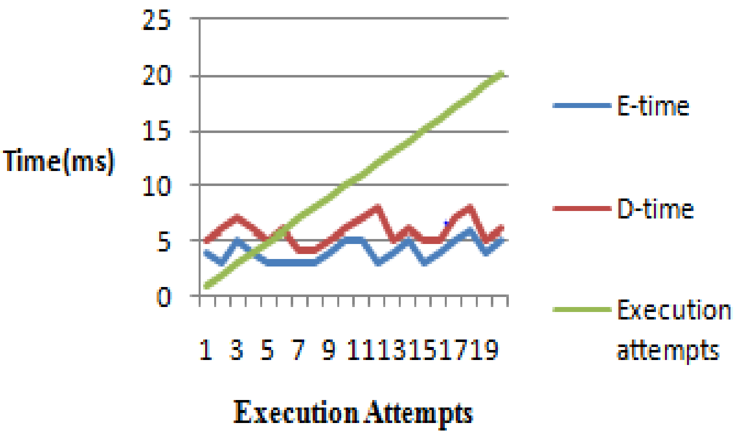


Figure 8: Time taken for executing the Encryption and Decryption

The below graph describes the total time taken to perform encryption and decryption operations.

DOI10.17148/IJARCCE.2017.6676

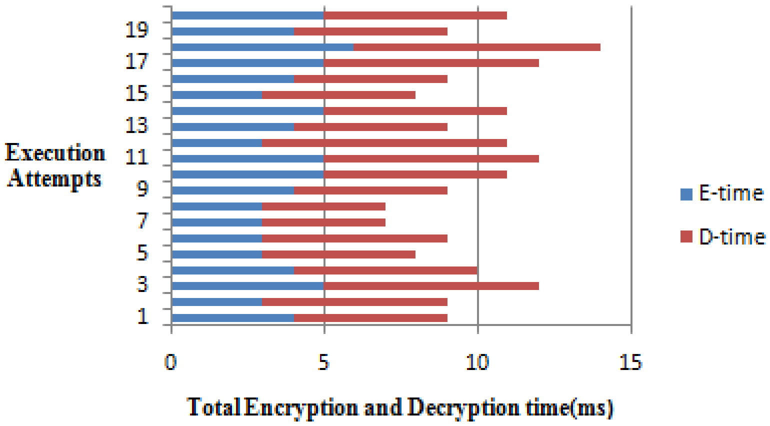


Figure 9: Total Time taken to perform Encryption and Decryption

Discussion

In Fog Computing, data security is major concern while transferring the data. In our system modified ElGamal algorithm is used for key generation. When user is registered in to the cloud then prime is generated to each user. Using that prime user successfully entered into the cloud. Then data is encrypted before sending to the cloud. And Cipher key is sent along with this encrypted data. Using the cipher key the receiver decryption process is performed and then appeared the original data. If enter the wrong cipher key the encrypted data is viewed instead of original data. The advantage of this modified algorithm is the execution time for encryption and decryption process is almost same while sending the different sizes of data.

V. CONCLUSION

In Our Thesis, Advantages and Disadvantages of Fog computing is discussed and later focus on security of data while transferred in Fog. Here data is some message. Message is converted into cipher text before sending to the cloud. At the same time Encryption key is generated by using modified ElGamal Algorithm. The receiver view the original data by decryption process done with his private key and finally view original image and message. The Modified ElGamal algorithm provides better security when compared with existing ElGamal algorithm. And also draw the graphs for the total time taken to perform encryption and decryption. In this way, our thesis secured the data by only accessing the authorized users.

REFERENCES

[1] KalyaniKadam, Rahul Paikrao, AmbikaPawar, “Survey on Cloud Computing Security,” IJETAE, ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 3, Issue 12, pp.239-249, December 2013.
[2] Shakeeba S. Kha1, Prof. R.R. Tuteja, “Security in Cloud Computing using Cryptographic Algorithms,” IJIRCCE, Vol. 3, Issue 1, pp.148-154, January 2015.
[3] Dr. S. S. Manikandasaran, “Security Attacks and Cryptography Solutions for Data Stored in Public Cloud Storage,” IJCSITS, ISSN: 2249-955, Vol.6, No1, pp.498-503, Jan-Feb 2016.
[4] Mrs. R. Waheetha, Mrs.Sowmya Fernandez, “Fog Computing and its applications,” IJARBEST, Volume 2, Special Issue 19, pp.56-62, October 2016.
[5] T.RajeshKanna, M. Nagaraju, Ch. Vijay Bhaskar, “Secure Fog Computing: Providing Data Security,” IJRCCT, Vol.4, Issue 1, pp.53-55, January 2015.
[6] Nisha Peter, “FOG Computing and Its Real Time Applications,” IJETAE, ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 5, Issue 6, pp.266-269, June 2015.
[7] AnnapoornaShetty, ShravyaShetty K, Krithika K, “A Review on Asymmetric Cryptography –RSA and ElGamal Algorithm,” IJIRCCE, Vol.2, Special Issue 5, pp.98-105, October 2014.
[8] Mitali, Vijay Kumar, Arvind Sharma, “A Survey on Various Cryptography Techniques,” IJETTCS, Volume 3, Issue 4, pp.307-312, July-August 2014.
[9] ApekshaWaghmare, AbhishekBhagat, AbhishekSurve, SanujKalgutkar, “Chaos Based Image Encryption and Decryption,” IJARCCE, Vol. 5, Issue 4, pp.64-68, April 2016.
[10] Monica G. Charate1, Dr. Savita R. Bhosale, “Cloud Computing Security using Shamir’s Secret Sharing Algorithm from Single Cloud to Multi Cloud,” IJATES, Volume No 03, Special Issue No. 01, pp.349-357, April 2015.
[11] Sulochana Devi, RituMakani, “Generation of N-party Man-In-Middle Attack for Diffie–Hellman Key Exchange Protocol: A Review,” IJCSIT, Vol. 6 (5) , pp. 4281-4285, 2015.
[12] S.Anandakumar, “Image Cryptography Using RSA Algorithm in Network Security,” IJCSET, Vol. 5, Issue 9, pp.326-330, September 2015.
[13] ShwethaKamath, “Survey on CHAOS Based Image Encryption Techniques,” IJETAE, Volume 7, Issue 4, pp.76-82, April 2016.
[14] Pooja Rani, Apoorva Arora, “Image Security System using Encryption and Steganography,” IJIRSET, Vol. 4, Issue 6, pp.3860-3869, June 2015.

DOI10.17148/IJARCCE.2017.6676