International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 4 Issue: 1 109 - 112

An Approach to Provide Safety over cloud using Efficient Encryption

Miss. Deepa Tandale
Computer Science Department
Deogiri Institute of Engineering and Management Studies
Aurangabad, India.
Emai-id: tandaledeeps33@gmail.com

Abstract: Cloud computing is a technology, which enables you to store the data remotely instead of local machines and access the stored data over the internet. This technology is getting overwhelming response from various fields, such as IOT where security is one of major concerned area. So, when our data is exposed to the outside world via internet then security should be provided to protect from an unauthorized access to the data stored on cloud. To protect the data when it is in- transit or at-rest the best mechanism is to encrypt the data. So, I had considered two mechanisms to secure the data stored on cloud. I had used two methods, first is AES and the second is Elgamal Encryption. At the end of this paper we compare these two methods by performance graphs using different parameters.

Keywords*: Elgamal algorithm, PFS (Perfect Forward Secrecy), AES (Advanced Encryption Standard), Cloud Data Storage, Security, IOT (Internet of Things)*

*****

I. INTRODUCTION

In simple terms cloud computing is where the data is stored and been processed at remote location over the internet. There are many techniques who are providing storage space over the internet such as Dropbox, SugarSync, GoogleDrive, SkyDrive, Amazon [2], Azure etc. Other service that can be used as a cloud is CYIPRO, which is a multipurpose application.

Introducing cloud in any enterprise gives us lots of benefits like 1. High quality service at cheaper prize which is self infrastructure and software costs are not cost effective. 2. Flexibility is key for small and emerging business, starting small and cheap, growing as needed. 3. Cloud services offer better solutions that are frequently unavailable or require much effort to use outside of the cloud. 4. Workforce and outsourcing is easier to employ as cloud services are commonly used and large part of work can either outsourced or get people that are already up to speed [1].

Even with all these benefits of cloud storage service many organizations will be concerned with security issues to their data in the cloud computing [3]. There are risks involved in utilizing cloud based solutions as per security and privacy of data. So, I had considered two mechanisms to secure the data stored on cloud. First is authentication of a user for proper access and the second one is encryption of data while the data in-transit and data at-rest. Every business wants to know that their data can only be accessed by authorized individuals. If your data is held on a server at your office, then it seems that this is really safe. However, from discussions in Linkedln, they discuss a case where an individual merely walked into an empty room in someone's office and plugged directly into the company's network. Again another discussion describes how a disgruntled employee access corrosive solution into the office server. The company didn't recover all their data and didn't have a good backup. Finally another discussion describes how a retiring partner deleted their outlook PST file destroying years of business information. So this happens very often in recent years. 99% of the time cloud based solutions are held within very secure data centres where physical access is strictly controlled [4]. At the very least, key-cards and pass codes, bar the doors. Again, redundancy is built-in to cloud based solutions- in other words. If something bad happens, then other computers take over providing the service. In this case, our primary server setup is mirrored every few minutes across the city. If the server cluster dies in our primary data centre, then the mirrors take over with minimal downtime, and next to no data loss. This is done at regular intervals of time. Firewalls protect access to the servers themselves over the network. There are uninterruptable power supplies, diesel generators, fire suppression system, multiple redundant connections to the internet, etc that protect our servers and the service they provide. So, it would seem that security access can oftentimes be better in a cloud based solution rather than a normal office environment. With many cloud-based solutions, the data is held in a number of locations at the same time. If you are using the services of global company like Google, it can be difficult to determine 'where is my data'.

This is an important consideration when you need to get access to the original documents for legal discovery for example. Many systems use a unified system with data segregation enforced by the software. Build once, use many times. If these software segregation system break down (because of a bug for example) then everyone's data may become vulnerable to exposure. Bad things do happen. With this in mind, I had built a hybrid system which physically segregates your data. This way, your files etc are sandboxed from that everyone else. So these are possible threats and

their possible way out to that threat. Now let's see some of the key components of a data security strategy over cloud.

1. Data encryption: If firewalls are now vulnerable, data needs to be encrypted at the rest.

2. Access control: SSO (Single Sign-On) and other access controls need to be in a place as apart of an identity management strategy. In the old model, users inside the firewall were assumed to be trusted. In the new model, users are assumed to be untrusted and strict access control needs to be in a place at the device level.

3. Governance and audit: Data should not be available to all personal and copies of sensitive data should tracked and destroyed when no longer needed. Best practiced like limiting access to passwords, robust password policies and ensuring that passwords are stored in encrypted data stores are must.

4. Monitoring: Threats coming from both inside and outside the company need to be monitored at the device level.

5. Testing: All IT departments should have a rigorous penetration testing strategy for both on premise and cloud environments.

So these are different methods to securely access the data on cloud [5]. The best method is the encryption method. In the next section of the paper, I will focus on how I had implemented the Elagamal encryption with PFS and their compare their result graphs with AES algorithm encryption graphs.

II. ARCHITECTURE

The following Figure(1) shows the architecture of this application. The procedure work as follows:

1. User creates an account and took permission from Admin to activate account.
2. User can upload a file from its terminal PC, where application encrypts the file and send it over to the cloud securely.
3. He gets two keys on his mail id which he can use it for downloading purpose.
4. The keys are created by PFS and encryption is done by using Elgamal encryption algorithm. The next section describes Elgamal and PFS techniques.

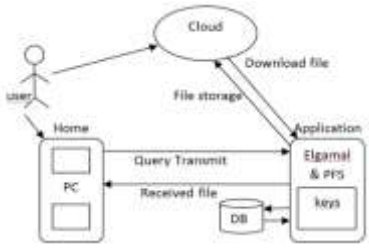


Figure.1 Architecture of secured cloud storage.

III. ENCRYPTION

Here for encryption purpose we use Elgamal and for key security we use the perfect forward secrecy method.

A. Elgamal Encryption Method

The Elgamal system is a public key cryptosystem based on discrete logarithm problem. It consists of both encryption and signature algorithms. The encryption algorithm is similar in nature to the Diffie-Hellman key agreement protocol. In Elgamal encryption algorithm each message is encrypted with different random number [6].

Elgamal is basically invented in 1985. The Elgamal encryption algorithm is very similar to the Diffie-Hellman algorithm, the only difference is that in this Elgamal algorithm we are just re-ordering the steps of Diffie-Hellman encryption algorithm [8]. This algorithm can also be spelled as ELGAMMAL. Elgamal was a famous cryptographer, and he uses his last name for this algorithm.

Now let's see how does this algorithm works step by step with the same example of Alice and Bob. In early days, Alice and Bob know a single key, but now bob having two keys. One is a private key, which he keeps it for himself and other one public key which he can throw out. Suppose Alice wants to send message x to bob and bob has two keys α and p. Now this work as follows:

1. Bob chooses p and primitive element α. Now he has to start to compute the keys. First he started to compute private key and after that public key.
$$k_{pr} = d \in \{2,3,\ldots..p-2\} \quad (1)$$
$$k_{pub} = \beta = \alpha^d mod\ p \quad (2)$$

2. Bob generates β, p, α. So that can told alice what are they actually. Alice chooses i ∈ {2,..,p-2}. So this is her public key.
$$k_e = \alpha^i mod\ p \quad (3)$$
Where k_e is Ephemeral key. This is standard terminology; it is temporal key i.e not for a long period, only for short period.

3. Alice getting the key from bob and she also has her own key, so now she computes the session key. Now, session key is calledk_m, we take β which is bobs public key and alice raised to her own secrete power as i.
$$k_m = \beta^i mod\ p \quad (4)$$
Where k_m is a Masking key

4. Now Alice computes the ciphertext y, which is x times of the masking key.
$$y = xk_m mod\ p \quad (5)$$

5. Alice sends y, $k_e$to bob. This is main difference between Diffie-hellman and Elgamal that here we are re-ordering the communication. Now bob

reassembles and compute the masking key, to do this he has to take k_e (temporary key) raised to secret power α.

$$k_m = k_e \, mod \, p \quad (6)$$

6. Once he has a session key, he ends up with last step

$$x = y{k_m}^{-1} mod \, p \quad (7)$$

The main advantage of elgamal is bob's public key β is fixed and α, p are chosen by him [7].

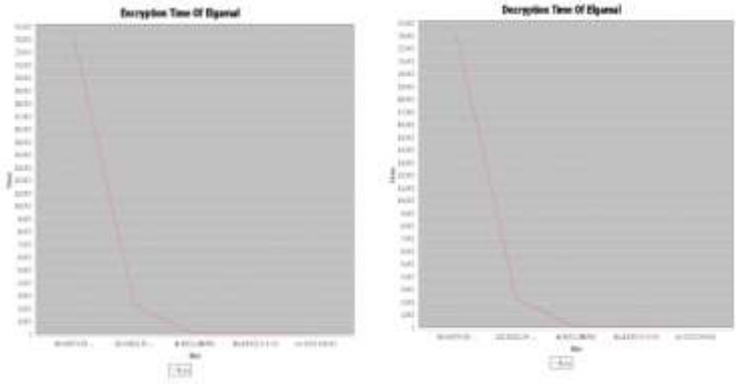
B. Perfect Forward Secrecy:

PFS is a function of the key- exchange protocol. The key- exchange protocol results in generation of shared secrete that may be used as the input to the cipher used to encrypt an SSL session. Key-exchange protocols that provide PFS are called ephemeral because they use a temporary public/private key pair to generate shared secret. Non-ephemeral protocols used a long lived secret, usually the same one for all sessions past and present are tied to the security of the private key.

Without PFS, an adversary in position of the private key for a site can decrypt all communications forever and always between that host and all clients. You might say that, make sense, but note that the actual encryption employed over SSL is not encrypted via public cipher. Without PFS, the cipher key is tied to the site's private key. This means an adversary can sniff and store all encrypted traffic from a particular host in hopes of compromising the security in the future. If it ever does, the whole a lot can be decrypted at once. Without PFS, that isn't possible, as a unique secrete is used to generate the shared secret for each session

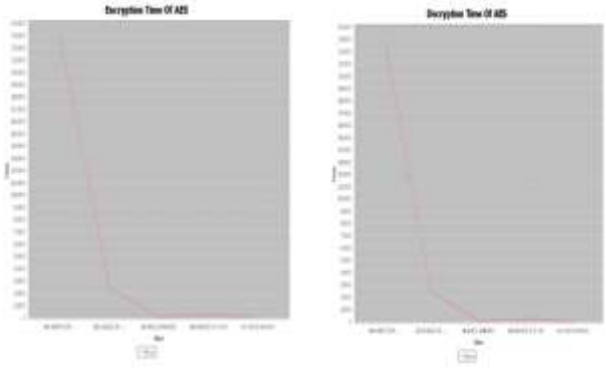
(a) (b)

Figure.2 (a) Encryption time (b) Decryption time of Elgamal and AES algorithm.



(c) (d)

Figure.3 (c) Encryption time (d) Decryption time of Elgamal with Five different file sizes



(e) (f)

Figure.4 (e) Encryption time (f) Decryption time of AES with Five different file size

Now let's see how does it works
1. Client wants to talk to server
2. Server generates a new set of public and private keys, y' and x'
3. Server sends y' to client.
4. Client generates a large, random integer M.
5. Client encrypts M using Y' and send Y(M') to server.
6. Server decrypts Y(M')using X', yielding M.
7. Both server and client now have M and use it as the key whatever cipher they agreed to use for the SSL session.

IV. RESULTS AND COMPARISON

Now, in this section, I compare the result graphs of two algorithms. One is the existing application which is works on Advanced Encryption standard and the second one is the one that implemented in this paper and this application works on Elgamal method with PFS. The comparison of these two methods can be done by showing the results with their performance graphs with the use of different parameters [9] like time, speed, file size etc.

But in this paper, the comparison of these two algorithms is done by time and file size parameters. The following graph shows comparison. In figure(2)a. their is encryption time is given while uploading the file, the algorithm 1 is Elgamal algorithm and algorithm 2 is for AES algorithm. In figure(2)b. the decryption comparison with time is given for these two algorithms. It clearly shows that encryption and decryption time of Elgamal is less than AES. Figure (3) shows line graphs of the encryption and decryption time of five different sizes of different files, using Elgamal algorithm. The AES algorithm encryption and decryption time for five different sizes is given in figure(4).

V. CONCLUSION

I had designed a new algorithm with a new approach to provide security on cloud of uploading and downloading data and secured those data files by encrypting them. The existing system has encrypted algorithm called Advanced Encryption standard but in our paper we developed Elgamal with PFS which provide us better security, scalability and reliability than Advanced Encryption Standard. The result graphs are more improved and show better result than previous method.

REFERANCES

[1] VARIA, J.2009. "Cloud Architectures. Amazon Web Services".
[2] Sun Microsystems, "Introduction to Cloud Computing Architecture", 2009.
[3] M. Jensen, J. Schwenk, N. Gruschka, and L. Lo Iacono, On Technical Security Issues in Cloud Computing. IEEE, 2009.
[4] "Secure group addresses cloud computing risks", http://www.secpoint.com/security-group-addresses-cloudcomputingrisks.html, April 25, 2009.
[5] Hasan Omar Al-Sakran" ACCESSING SECURED DATA IN CLOUD COMPUTING ENVIRONMENT", International Journal of Network Security & Its Applications (IJNSA) Vol.7, No.1, January 2015.
[6] CZESŁAW KOSCIELNY" A NEW APPROACH TO THE ELGAMAL ENCRYPTION SCHEME", Int. J. Appl. Math. Comput. Sci., 2004, Vol. 14, No. 2, 265–267
[7] Preeti*, Bandana Sharma" Review Paper on Security in Diffie-Hellman Algorithm", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 3, March 2014.
[8] Yiannis Tsiounis1 and Moti Yung2" On the Security of ElGamal Based Encryption", H. Imai and Y. Zheng (Eds.): Public Key Cryptography, PKC'98, LNCS 1431, pp. 117–134, 1998. c Springer-Verlag Berlin Heidelberg 1998.
[9] Nidhi Singhal1, J.P.S.Raina2" Comparative Analysis of AES and RC4 Algorithms for Better Utilization", International Journal of Computer Trends and Technology- July to Aug Issue 2011.