J. Basic. Appl. Sci. Res., 2(7)7091-7094, 2012

ISSN 2090-4304
Journal of Basic and Applied Scientific Research
www.textroad.com

Applying Provable Data Possession with Elgamal in Cloud Computing

Memoona Javeria Anwar, M. Younus Javed, Saad Rehman, Nazish Asad

Department of Computer Engineering, College of Electrical and Mechanical Engineering, National University of Sciences and Technology (NUST), Islamabad, Pakistan.

ABSTRACT

Amid the most prominent e-technologies of the modern day, Cloud Computing has changed the manner in which IT architectural solutions are put forward, by shifting towards the theme of Virtualization: be it in terms of data storage, infrastructure or software. While on one hand, the 'Cloud' offers immense benefits for the users, yet on the other hand, information breach / in-security is the foremost challenge that outweighs its colossal success factors. Provable Data possession (PDP) is a technique for validating data integrity over remote servers. In this paper we check that whether changing the encryption scheme affects the performance of PDP or not.
KEYWORDS: Cloud computing, Security, Provable Data possession, Encryption**.**

1. INTRODUCTION

Cloud computing is a service than being a product, where mutual information, software, and resources are provided to computer systems and other devices as a service on a network. Cloud computing has a lot to offer such as computation, data storage and access, software applications and mostly some high ranked computing infrastructure. Anyone can get advantage of cloud services. Users get in contact with cloud based services through a browser or a light weight desktop application. A mobile app can also be used to gain access to the cloud applications. The location where the data and business software are stored is not known to the end users. Its somewhere on server at a remote location. Cloud service providers do their utmost to give same, rather better service and efficiency as if the end user has installed the software program locally on his own computer.

There is no doubt about cloud having unlimited advantages but along with the advantages there come few challenges as well, as described below.

a. Restricted User Access. There is an inherent level of risk associated with processing of data outside the premises of the enterprise due to the reason that subcontracted services bypass the "physical, logical and personnel controls".

b. Supervisory Compliance. The responsibility of data security and integrity lies with the client due to business dictates. Cloud service providers are subjected to external audits and security certifications.

c. Data Locality. The client does not know about the location of the data storage. it may even be in a country with which the interest of the company or government clash

d. Data Isolation. Since the data is lying in a shared environment along with data of otherclients, therefore only encryption might not be a comprehensive solution.

e. Recovery. In the event of a data loss or disaster, the CSP should be bound to tell the whereabouts of the data storage location.

f. Exploratory Support. At times, investigation of unlawful activity with the stored data may not be possible due to the architecture and spread of the Cloud,

g. Long-Term Sustainability. In an ideal environment, the CSP that has been engaged will conti9nue to exist in the swarm of globalization and expansion of giants in the field of CSP.

h. Types of Attacks. Examples of potential attacks to data stored over the cloud are:

(1) XML Signature Attack
(2) Cloud Malware Injection Attack.
(3) Metadata Spoofing Attack.
(4) Flooding Attacks

Amid the most prominent e-technologies of the modern day, Cloud Computing has changed the manner in which IT architectural solutions are put forward, by shifting towards the theme of Virtualization:

***Corresponding Author:**Memoona Javeria Anwar, Department of Computer Engineering, College of Electrical and Mechanical Engineering, National University of Sciences and Technology (NUST), Islamabad, Pakistan. Email: memoonasheikh@gmail.com

be it in terms of data storage, infrastructure or software. While on one hand, the 'Cloud' offers immense benefits for the users, yet on the other hand, information breach / in-security is the foremost challenge that outweighs its colossal success factors.

2. Existing Scheme

Provable Data possession (PDP) is a technique for validating data integrity over remote servers. Ateniese et al *[1]*. have formalized a PDP model. In that model, the data owner pre-processes the data file to generate some metadata that will be used later for verification purposes through a challenge response protocol with the remote/cloud server the file then goes to an untrusted server where it's stored, and the possessor may delete the file from his local system. At a later stage server is questioned about data file, where it is supposed to demonstrate that the file has not been deleted or modified by the answering to the challenges sent from the verifier who can be the original possessor of the data file or any other trusted body. Researchers have proposed different variations of PDP schemes under different cryptographic assumptions.

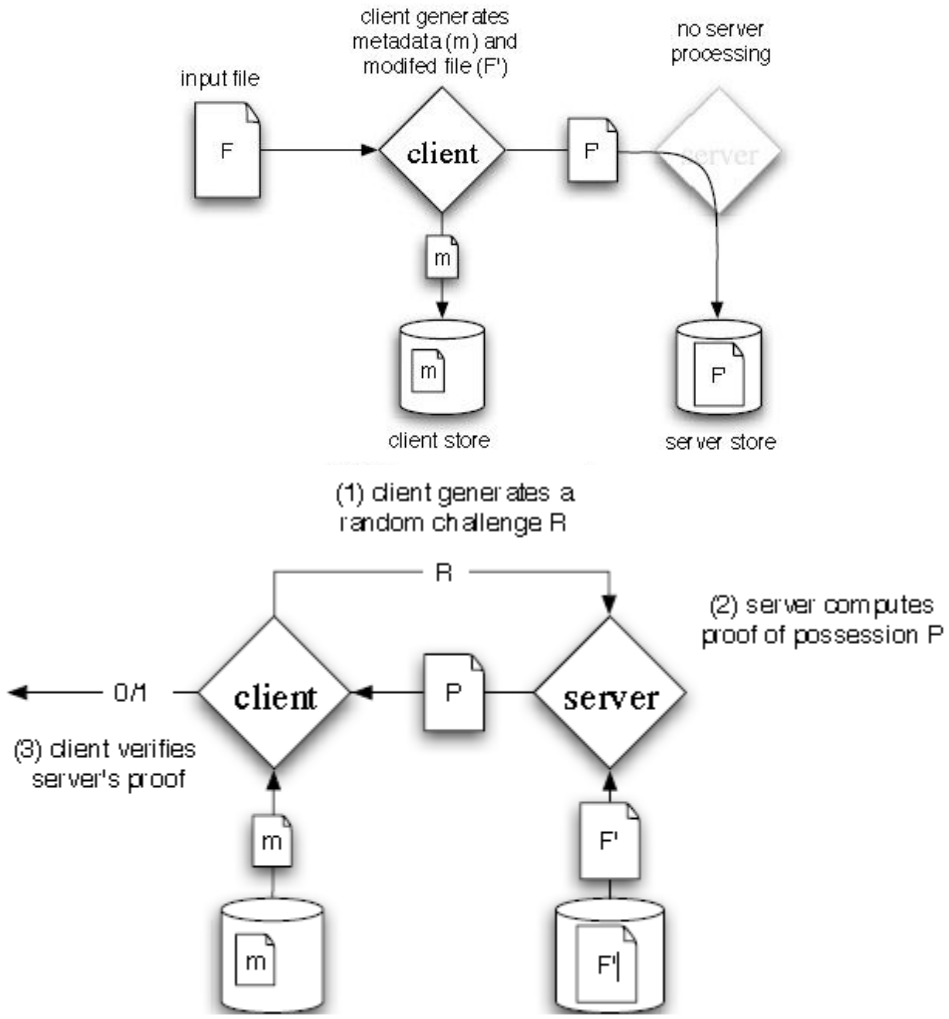

Figure-1 Provable Data Possession *[1]*

(b) Verify server possession

The first variation is RSA Encryption *[4]* refers to *Public-key cryptography* refers to a cryptographic system that requires two separate keys, one to encrypt the plain-text and the other for decrypting the cipher-text. Both the functions are not done by one key; one of these keys is published or made public while the other is kept private. RSA is one of the examples of Public-key cryptography.

The flow chart below describes how RSA decrypts and encrypts a message.

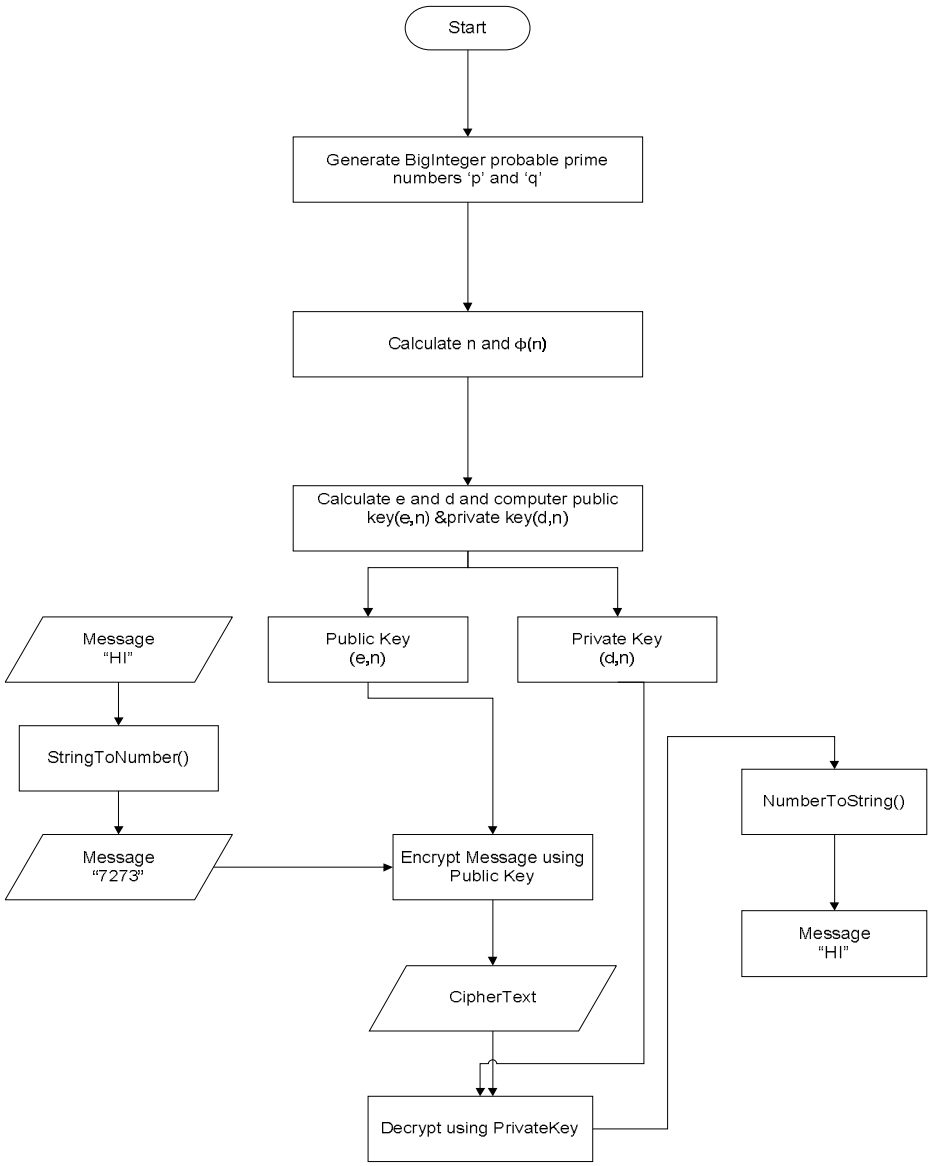

Figure-2 RSA Encryption

While the second variation is ElGamal encryption system *[3]* is a public-key cryptosystem and is defined based upon Diffie–Hellman key exchange. This scheme is firstly used for key generation and later for encryption-decryption. ElGamal encryption system is based on Diffie–Hellman key exchange.

3. IMPLEMENTATION AND RESULTS

The purpose of this research is to check what role encryption scheme plays in the whole PDP mechanism.

Client and Server performance has been compared upon different norms. Whether RSA gives best results or ElGamal is a good choice for PDP, our results show this all. We have made a comparison between computation complexities of both cryptosystems and formulated a result shown in the graphs.

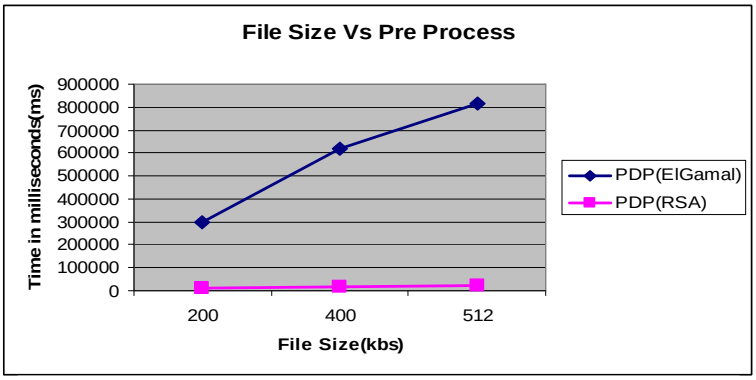

Figure-3 File size versus Preprocess time in PDP (RSA) & PDP (ElGamal)

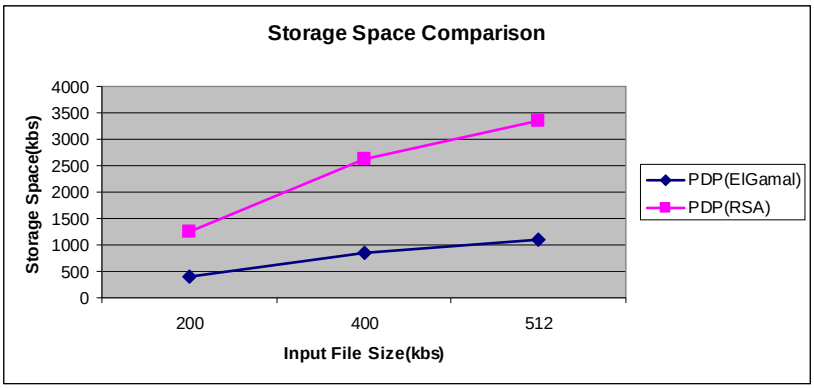

Figure-4 File size versus time to compute proof in PDP (RSA) & PDP (ElGamal)

4. Conclusions

ElGamal encryption takes longer time compared to RSA which leads to a delayed preprocess stage. Preprocess time for both the algorithms have been shown in figure 3. ElGamal shows exceptionally high readings compared to RSA. Preprocess includes key generation, metadata creation and file transfer. The key generation time for both the algorithms is almost same. Major contribution in this huge graph reading is of encryption by ElGamal. This known fact about ElGamal encryption's slow speed has been seen in our implementation too.

ElGamal is slower at encryption end but faster while decrypting. So the cryptosystem generates proof quickly compared to RSA as seen in Figure 3 and Figure 4.

5. REFERENCES

[1] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song. *"Provable data possession at untrusted stores"*, In CCS, pp. 598–609, 2007.

[2] Li Xiao-fei, Shen Xuan-jing, Chen Hai-peng. *"An Improved ElGamal Digital Signature Algorithm Based on Adding a Random Number"*. In 978-0-7695-4011-5/10 $26.00 © 2010 IEEE

[3] T. ElGamal. *"A public key cryptosystem and a signature scheme based on discrete logarithms"*, In: Proceedings of CRYPTO 84 on Advances in Cryptology, New York, NY, USA, Springer-Verlag New York, Inc. pp. 10-18 1985.

[4] A. Selby , C. Mitchell. *"Algorithms for software implementations of RSA"*, In 6612E (C l , C 2) , first received 23rd December 1987 and in revised form 17th January 1989

[5] A. Fiat. Batch RSA. In G. Brassard, editor, Proc. CRYPTO 89, pages 175–185. Springer-Verlag, 1990.