IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
Vol. 09, Issue 6 (June. 2019), ||S (II) || PP 21-24

Effective Client Server Cryptographic Interaction Technique In Cloud Environment

Tanmoy Mukherjee[1], Sudipta Sahana[1], Debabrata Sarddar[2]
[1](*Department of CSE, JIS College of Engineering, Kalyani, Nadia, India)*
[1](*Department of CSE, JIS College of Engineering, Kalyani, Nadia, India)*
[2](*Department of CSE, University of Kalyani, Kalyani, Nadia, India)*

Abstract: - The modern era of cloud computing has taken a significant turnaround and has become a major talking point among the public. In the midst of all the benefits that can be extracted from cloud computing, there lies some sort of major concern in terms of privacy and security of data that gets exchanged on cloud platform. Various research papers mentioned the use of different cryptographic and encryption and decryption algorithms for the security and privacy of data on cloud platform. In our paper, we have proposed the use of a cloud platform, wherein the request message, supposed to be sent from the client to the server, will be divided into two parts and kept in two separate files. The two parts of the request message will then be sent one by one from the client machine to the server machine using the concepts of asymmetric key cryptographic and symmetric key cryptography one after the other. The same thing happens for the response message as well, which gets transmitted from the server machine to the client machine. Hence, an effective and efficient cryptographic technique related to the client server interaction can be guaranteed on the cloud environment.

Keywords: - Asymmetric Key Cryptography, Client, Client Server Interaction, Public key, Private key, Server, Symmetric Key Cryptography

---

Date of Submission: 02-06-2019 Date of acceptance: 17-06-2019

I. INTRODUCTION

In the modern world, the security of data on the cloud platform has become a matter of primary significance. There are a lot of interactions which happen between a client and a server and the critical issue related to this aspect is the privacy and security of a large volume information or data which gets communicated between the client and the server. Hence, it is imperative that we suggest the use of an effective and efficient cryptographic technique which will go a long way in ensuring that all the interaction happening between the client and the server on the cloud platform will be absolutely risk free and any threat to the information being exchanged between the client and the server will be nullified.

In our paper, we have proposed the use of a cloud platform, wherein the request message, supposed to be sent from the client to the server, will be divided into two parts and kept in two separate files. The two parts of the request message will then be sent one by one from the client machine to the server machine using the concepts of asymmetric key cryptographic and symmetric key cryptography one after the other. The same thing happens for the response message as well, which gets transmitted from the server machine to the client machine. Hence, an effective and efficient cryptographic technique related to the client server interaction can be guaranteed on the cloud environment.

The subsequent sections of this paper talk about the related work (Section II), methodology along with a well defined block diagram (Section III), result analysis along with suitable graphical representations (Section IV) and the conclusion with the mention of further scope of research in this field (Section V).

II. RELATED WORK

Akansha Deshmukh et al. [1] talks about a core secured cloud storage services i.e. cryptography whose main objective is to offer cryptographic techniques for securing data and computation in a cloud environment.

In paper [2] the authors talk about the various aspects of cloud cryptography. The paper further makes the mention of homomorphic encryption and searchable encryption, data integrity, data sharing, skyline computation, trust evaluation, mobile cloud etc.

Rishav Chatterjee et al. [3] review the cloud security issues by suggesting the use of crypto algorithms and effective measures so as to gurarantee the data security in cloud. The paper further tals about some privacy issues of current cloud computing surroundings.

In paper [4], the authors have designed a scheme which is required for uploading the data on cloud platform in a secured and risk free manner. The paper further talks about various methods about saving the data at remote servers without any risk and hindrance.

III. METHODOLOGY

There are some of the prerequisites that are necessary to carry out the algorithm. They are given below:

(i) A cloud environment
(ii) A client machine
(iii) A server machine
(iv) Two number of files
(v) Server machine's public key and private key
(vi) Client machine's public and private key
(vii) A shared private key

The algorithm (Fig. 1) for our procedure can be given in the following steps: -

a) At first, there is a client machine which has been set up on the cloud environment.
b) Next, we install a server machine on the other side of the cloud platform.
c) Next, there is a request in the form of a message which is to be sent from the client machine to the server machine.
d) We divide the entire request of the client into two equal parts and keep them in two separate files.
e) Next, we want to take the file containing the 1^{st} part of request and we want to send the same from the client machine to the server machine using the technique of asymmetric key cryptography. In this technique, the 1^{st} part of request made by the client, gets encrypted using the server's public key and that part takes the form of cipher text. When the same reaches the server in the form of cipher text, the cipher text gets decrypted using the server's private key and the server receives the 1^{st} part of request in the form of plain text. Hence, the full protection of the 1^{st} part of request made by the client can be guaranteed through this technique.
f) Next, we want to take the file containing the 2^{nd} part of request and we want to send the same from the client machine to the server machine using the technique of symmetric key cryptography. In this technique, the 2^{nd} part of request gets encrypted by using a shared private key and takes the form of cipher text. When that part of request is received by the server machine in the form of cipher text, the same gets decrypted by the shared private key and hence the server receives the 2^{nd} part of request in the form of plain text. Hence, the full protection of the 2^{nd} part of request made by the client can be guaranteed through this technique.
g) Next, we can divide the response given by the server to the client into two equal parts and keep them in two separate files.
h) Again, we want to take the file containing the 1^{st} part of response and we want to send the same from the server machine to the client machine using the technique of asymmetric key cryptography. In this technique, the 1^{st} part of response made by the server, gets encrypted using the client's public key and that part takes the form of cipher text. When the same reaches the client in the form of cipher text, the cipher text gets decrypted using the client's private key and the client receives the 1^{st} part of response in the form of plain text. Hence, the full protection of the 1^{st} part of response made by the server can be guaranteed through this technique.
i) Next, we want to take the file containing the 2^{nd} part of response and we want to send the same from the server machine to the client machine using the technique of symmetric key cryptography. In this technique, the 2^{nd} part of response gets encrypted by using a shared private key and takes the form of cipher text. When that part of response is received by the client machine in the form of cipher text, the same gets decrypted by the shared private key and hence the client receives the 2^{nd} part of response in the form of plain text. Hence, the full protection of the 2^{nd} part of response made by the server can be guaranteed through this technique.
j) Hence, the full protection of the client server interaction on the cloud environment can be guaranteed by following the above steps.

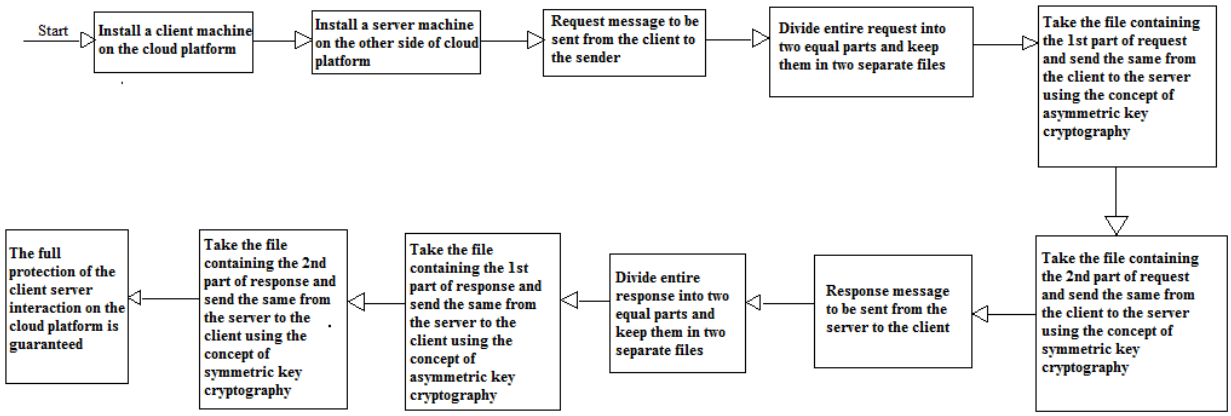

Fig. 1: Flowchart for our algorithm

IV. RESULT ANALYSIS

In our paper, we have used the concepts of asymmetric key cryptography and symmetric key cryptography. Also, we have divided the request message from the client to the server and the response message from the server to the client into two equal parts each and kept the two sections of both the messages in two separate files. Also, we have made use of the cloud environment to suggest the entire procedure.

The use of two separate techniques, i.e. asymmetric key cryptography and symmetric key cryptography, will make it very difficult for any hacker or attacker to decode and tamper the request and response messages and hence, the interaction between the client and the server will be absolutely safe without any hindrance. Also, unlike the traditional approach, our suggested technique goes on to show that with the increase in number of words of the request and response messages, the response time will increase slightly as shown below (Fig. 2).

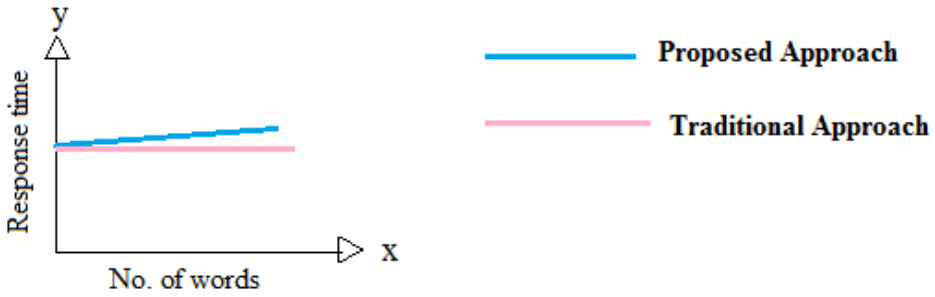

Fig. 2: Comparing the proposed approach and the traditional approach showing that the response time will increase slightly with the increase in number of words

V. CONCLUSION

Our suggested paper makes the use of the concepts of asymmetric key cryptography and symmetric key cryptography for the client server interaction in cloud environment. The performance of a cryptographic technique can be measured on the basis of parameters such as response time. All the proposed methods that we have used in our paper will go a long way in ensuring that the above mentioned parameter can be met with a high degree of precision and accuracy and hence an efficient and effective cryptographic technique for the client server interaction on the cloud environment can be achieved. In our future, we are planning to put our suggested technique into practical purpose and implement the same in cloud environment.

ACKNOWLEDGEMENTS

Authors are grateful towards CSE Department of JIS College of Engineering and University of Kalyani for providing lab and related facilities necessary for doing the research.

REFERENCES

[1]. Akansha Deshmukh, Harneet Kaur Janda, Sayalee Bhusari, "*Security on Cloud Using Cryptography",* International Journal of Advanced Research in Computer Science and Software Engineering, Volume *5*, Issue *3*, March 2015, ISSN: 2277 128X

[2]. Kim-Kwang Raymond Choo, Josep Domingo-Ferrer, Lei Zhang, "*Cloud Cryptograph: Theory, Practice and Furure Research Directions",* Research Gate, Future Generation Computer Systems, ELSEVIER, DOI: 10.1016/j.future.2016.04.017

[3]. Rishav Chatterjee, Sharmistha Roy, "*Cryptography in Cloud Computing: A Basic Approach to Ensure Security in Cloud"*, IJESC, Volume *7*, Issue *5*

[4]. Karun Handa, Uma Singh, "*Data Security in Cloud Computing using Encryption and Steganography",* International Journal of Computer Science and Mobile Computing (IJCSMC), Volume *4*, Issue *5*, May 2015, pg. 786-791, ISSN: 2320-088X

Sudipta Sahana. "Effective Client Server Cryptographic Interaction Technique In Cloud Environment." IOSR Journal of Engineering (IOSRJEN), vol. 09, no. 06, 2019, pp. 21-24.