INTERNATIONAL JOURNAL OF ADVANCE RESEARCH AND DEVELOPMENT

(Volume3, Issue8)

Available online at: www.ijarnd.com

Build up cloud computing security using ID based cryptographical algorithms

Manogya Pulivendala

Student, Keshav Memorial Institute of Technology, Hyderabad, Telangana

ABSTRACT

So, the user uploads his confidential data over the cloud platform and definitely, he expects it to be transmitted in a secure way with no interruptions and for this to take place, the data should be transmitted through a secure channel. There are solutions to this already, for instance, Diffie Hellman Algorithm but there are problems with this too, even though it uses Discrete Logarithm method which can only decrease the chances of getting attacked. One of the main drawbacks of this algorithm is that it doesn't establish the identity of the other party, making it susceptible to a man-in-the-middle attack (meaning the information shared between two parties is accessible to a third party). On the 9th of June, CERT-EU published an advisory concerning the Logjam attack which is a man-in-the-middle attack, again. Basically, this paper addresses the possible solution that could be provided for a much secure information exchange.

Keywords— *AES, DES*

1. INTRODUCTION

Most of us know that almost all the firms today make use of Cloud Computing and this, we hear so often now that it got many of us wondering what exactly is it and how are we using it on a daily basis. Simply put, Cloud Computing is using a network of servers which is hosted on the internet to store, manage and process data.

2. QUICK DEMONSTRATION

Figure 1 shows sample drawing for better understanding.

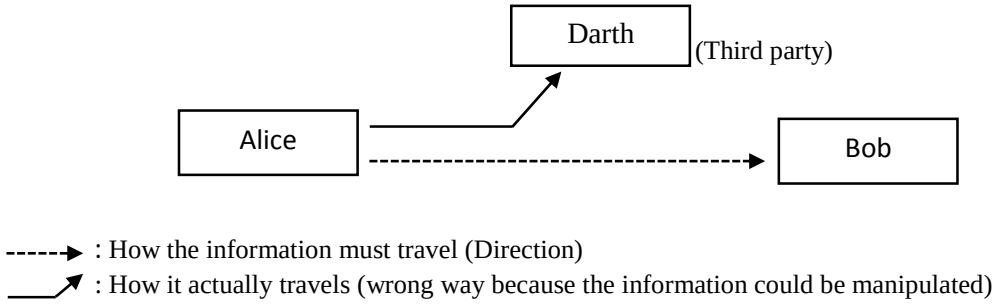


Fig. 1: Demonstration

The summary of this picture is that Darth (The third party) is able to eavesdrop on the conversation (or sensitive data) between Alice and Bob which is incorrect, illegal to be precise.

3. SECURITY IN CLOUD COMPUTING

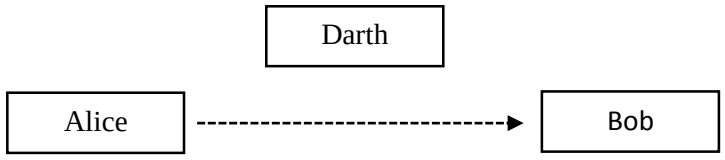
As one of the most promising ways to optimize IT infrastructure, cloud computing is increasingly considered. There are many advantages of Cloud Computing technology, but the question of the reliability of data protection by using the concept of cloud computing is becoming a major deterrent.

The following conditions must be observed to ensure reliable security in cloud services:

1. Cryptographic methods for data safety should be used. All the data that the client is running within the service should be securely encrypted.
2. The very process of transferring information from the client and the server must also be safe, it is necessary to use a secure data transfer protocols to access the server.

Now, Diffie Hellman uses Symmetric Key Encryption type, which means it uses only a single key to encrypt and decrypt the data and this particularly could get harmful as the data can be decrypted easily once the key is found out.

Working of Diffie Hellman Algorithm is explained as:



IMPLEMENTATION OF NORMAL DIFFIE HELLMAN ALGORITHM

- Initially Alice and Bob agree on two random numbers, with one being a prime modulus and other a generator.
- Let the number be *P= 17*, and *g= 3.*
- Now, since these numbers are public, Darth (the third party) knows it too.
- Next Alice selects a random private number, let's say that's 15 and hence we calculate:

  $3^{15} \bmod 17 = 6$

  So now Alice sends this number *(6)* to Bob.
  Note: Darth receives this number too.
- Bob does the same as Alice, let's say he picks a random private number as *13*. Hence we calculate:

  $3^{13} \bmod 17 = 12$
- So, this '*12'* is sent to Alice and again Darth receives it.
- Now comes the tricky part:
  - Alice takes what she has received *'12'* and computes the following:

    $12^{15} \bmod 17 = 10$

    Note: this *'15'* is Alice's private key, so only she knows this number.
  - Bob does the same and he calculates: $6^{13} \bmod 17 = 10$
- The problem is hence solved, Alice and Bob knows the number which is *'10'*
- Here Darth will have no clue about *'10'* and he is stuck with Discrete Logarithmic problem, which if he manages to solve, he can't do it (hard to do but not impossible) in a short span of time.

To settle this problem, this paper addresses the problems of Diffie Hellman (ID-based) also how to securely transfer the data through the communication channel.

The following depicts usage of an Algorithm which might help with the drawback of Diffie Hellman and also by reducing the usage of time. Let's consider the same example where Alice intends to send a message to Bob without the interference of Darth.

- Firstly, Alice chooses a random natural number and double encrypts (for extra security) it by using any of the encryption algorithms like AES (Advanced Encryption Standard), Blowfish, Triple DES or any other strong algorithm. Also, he encrypts his Digital Signature, which is only to prove that she's genuine. This encrypted form of data is sent to Bob.

- TGS Now, Bob finds out the Algorithm used and sends Alice an acknowledgment with his Digital Signature and his random number.

  ***Note*:** Kerberos Authentication can be used here but one main disadvantage is that it mostly works like a Client Server Architecture.

- Next, Alice uses Bob's Random key (which she receives with his Digital Signature after decryption) and sends it to the Cloud with her License (proof to use it, granted by the TGS – Ticket-Granting Service, if Kerberos is used, or likewise showing Authentication) and after verification, she receives the generated Key.

- Bob does the same.

  ***Note*:** Here, the Cloud verifies Mutual Authentication using ID's and Digital Signatures and provides Alice and Bob with their respective Keys, which makes this an Asymmetric Algorithm and less likely to get hacked.

- Alice then encrypts her data with the Cloud generated key and sends it to Bob where on the other hand, Bob decrypts it with his key and hence here, the ID's of both the communicating parties get verified.

This way, even if Darth get through the Discrete Logarithm Attack, he won't be able to decrypt the data as there is absolutely no way he can get the Cloud generated Key. Moreover, there will be a time slot for the ticket and even if the data gets to Darth by any foul means, the time slot expires which makes it next to impossible to retrieve the data.

4. CONCLUSION

Cloud Computing is world emerging, next-generation technology in the field of information technology although Security is one of the biggest challenges it faces. In this paper, I have discussed a way to securely transmit data to the other end and even if the data

doesn't get transmitted, it surely cannot be decrypted by the intruder. Here, I conclude that the data will be secured in either way after encrypted by powerful encrypting algorithms like AES, Blowfish or Triple DES as discussed above. Future work is to implement different techniques in other ways to provide utmost Security protection on Cloud from any type of security attack.

5. REFERENCES

[1] https://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange
[2] https://www.khanacademy.org/computing/computer-science/cryptography/modern-crypt/v/diffie-hellman-key-exchange-part-2
[3] https://en.wikipedia.org/wiki/Cloud_computing

