IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-7, Special Issue, 4, Feb 2019 E-ISSN: 2347-2693

Key Exchange Technique in Cryptography Using Diffie-Hellman Algorithm

V. Vinothini[1*], C. Muthukumaran [2]

[1]Department of computer science, Idhaya College for women, Kumbakonam, India
[2]Department of computer science, Arasu engineering college, Kumbakonam, India

Corresponding Author: v.vino1290@gmail.com

Available online at: www.ijcseonline.org

Abstract— Internet of Things is a new pattern which provides a set of new services for the next form of technological development. IOT in the sense, it is a "universal global neural network" in the cloud which connects various things. The form of communication that is either human-device, or human-human but the Internet of Things (IoT) promises a great future for the internet where the type of communication is machine-machine (M2M). This paper aims to provide a future vision , IoT Architecture , Applications and its Challenges.

Keywords— Vision, Challenges, Applications, Architecture.

I. INTRODUCTION

Whitfield Diffie and Martin Hellman discovered what is now known as the Diffie-Hellman (DH) algorithm in 1976. It is an amazing and ubiquitous algorithm found in many secure connectivity protocols on the Internet. DH is a method for securely exchanging a shared secret between two parties, in real-time, over an untrusted network. A shared secret is important between two parties who may not have ever communicated previously, so that they can encrypt their communications. As such, it is used by several protocols, including Secure Sockets Layer (SSL), Secure Shell (SSH), and Internet Protocol Security (IPSec).

II. ALGORITHM FOR EXSTING SYSTEM

The algorithm chooses two public known numbers a Prime number n and g that is primitive root of n. Suppose user A and B wish to exchange a key for their communication, then user A select random integer (private key) $X_a < n$ and compute public key $y_a=g^{xa}$ mod n. Then user B select random integer(private key) $X_b< n$ and compute public key $y_b=g^{xb}$ mod n. Secret key compute by A is $K=y_b^{xa}$ mod n. similarly Secret key compute by A is $K=y_a^{xb}$ mod n.

A) *Insecure against attacks*

The algorithm is insecure against man in the middle attack as follows, Suppose there is a user C who is going intercept the secret key shared between user A and user B. C generates two random private keys x_{d1} and x_{d2} and then computes corresponding public keys y_{d1} and y_{d2}. User A transmits public key y_a to user B. in the meanwhile user C intercepts y_a and transmits his public key y_{d1} to user B. user C also calculate $K_2= y_{d2}^{xa}$ mod n. B receives y d1 and calculate secret key $K_1=y^{d1}\ x_b$ mod n. Now, user B transmits his private key x_a to A. Now, C intercepts and transmits his own public key y_{d2} to A. Now, A receives y_{d2} and calculates corresponding K_2. Since the algorithm is easily cracked by discrete logarithm approach as above, we have to strength the algorithm to avail better security key transmission.

III. CONTRIBUTION OF WORK

In order to increase the strength of the algorithm, we are going to generate the private keys using pseudo random number mechanism. In our method , we are defining our own mathematical equations to generate values for both X_a and X_b. Suppose we are generating value by the equation Xa =a*b*c and generating X_b = a+b+c.. For example the values of a, b, c is 1 , 8 , 5 then the value of X_a =40 and the values of a, b, c is 2,1,3 then the value X_b of 6 . The above two equations have more than solutions at any time (i.e.) suppose we give the values of a, b, c as 4,2,5 then the value of X =40. Therefore more than one solution exists for a given equation .we are restricting the factors of the equation by choosing one of the factors that is known to the programmer itself and it cannot be easy for the intruder to break. In our example the programmer factors have the value a ,b, c is 1 , 8 ,5 and the intruder factors are a, b, c is 4,2,5 is NOT the same. Even though the values g, n are public, it is now difficult for the intruder to find the private key values X_a and X_b along with correct factors for that equation. Since it is difficult for the intruder to workout all possible values for a set of equations

© 2019, IJCSE All Rights Reserved

to choose the correct one, it is absolutely difficult task to choose the desired one.
User A Using following algorithm as follows:
Choose Private key $x_a = a * b * c$.
Calculate Public Key $y_a = g^{xa} \bmod n$.
Secret Key $K1 = y_b^{Xa} \bmod n$.
User B Using following algorithm as follows:
Choose Private key $x_b = a+b+c$.
Public Key $y_b = g^{xb} \bmod n$.
Secret Key $K_2 = y_a^{xb} \bmod n$.
Thus using our own private key generation algorithm it is difficult for the intruder to decide correct factor for the equation that we defined.

IV. EXPERIMENTAL RESULT AND ANALYSIS

To test the execution time of our method, we compare the execution time for both normal diffie Hellman algorithm and modified diffie Hellman algorithm

Table 1. GENERAL DIFFIE-HELLMAN ALGORITHM EXECUTION TIME

x_a	x_a	g	n	Time in (ms)
3	7	5	7	2621961879710
3	5	23	53	2621961594354
7	11	11	13	2621961965370
7	11	17	23	2621962111512
9	11	31	41	2621962202524

Table 2. MODIFIED DIFFIE – HELLMAN ALGORITHM EXECUTION TIME

a	b	c	g	n	Times in (ms)
6	7	18	37	529	262212278806
2	17	16	61	449	2622123638752
2	18	16	61	289	2622123756612
2	5	16	61	449	2622123793340
4	6	13	29	377	2622123859782

The execution time for both methods found to be more or less same. Suppose we take a=2, b=5, c=16. At any time intruder recognizes $x_a=160$, he has to find correct factor to generate x_a value. There are more than one factor available for above equation $x_a=a*b*c$. Suppose he give values a=4,b=5,c=8 then value of $x_a=160$ but he is not able to provide correct factors a=2,b=5,c=16 that is already defined by user.

V. CONCLUSIONS AND FUTURE WORK

This paper proposed a novel diffie Hellman approach. The system defines a method to generate private keys using equations that is defined by user. Experimental results show that the proposed diffie Hellman can work effectively by generating correct factors and it is almost impossible to be crack by intruder. In future, we will test the proposed system with complex equations and to provide a better security mechanism.

REFERENCES

[1] Y. Amir, Y.Kim, C. Nita-Rotaru, "Secure communication using contributory key agreement", IEEE Transactions on Parallel and Distributed systems, pp. 468-480,2009.
[2] M. Bellare, D. Pointcheval, P. Rogaway, " Authenticated Key exchange secure against dictionary attacks", IN Proc. Of Eurocrypt, pp. 139-155.2010
[3] S. Blakke Wilson, A. Menezes, " Entity authentication and authenticated transport protocols employing asymmetric techniques", SPRINGER 1997.

© 2019, IJCSE All Rights Reserved