2020 International Conference on Electrical and Electronics Engineering (ICE3-2020)

Hybrid Technique of Genetic Algorithm and Extended Diffie-Hellman Algorithm used for Intrusion Detection in Cloud

Himanshi Chaudhary, Awadesh Kumar Sharma
Himanshichaudhary1805@gmail.com
akscse@rediffmail.com
Department of Computer Science and Engineering,
Madan Mohan Malaviya University of Technology,
Gorakhpur

Abstract— It is a well-known fact that the use of Cloud Computing is becoming very common all over the world for data storage and analysis. But the proliferation of the threats in cloud is also their; threats like Information breaches, Data thrashing, Cloud account or Service traffic hijacking, Insecure APIs, Denial of Service, Malicious Insiders, Abuse of Cloud services, Insufficient due Diligence and Shared Technology Vulnerable. This paper tries to come up with the solution for the threat (Denial of Service) in cloud. We attempt to give our newly proposed model by the hybridization of Genetic algorithm and extension of Diffie Hellman algorithm and tries to make cloud transmission secure from upcoming intruders.

Keywords— Cloud Computing, Genetic Algorithm, Extension in Diffie-Hellman algorithm, Denial of Services (DOS)

I. INTRODUCTION

Cloud Computing as a term, refers to hosting and delivery method of data, information or resources. It has become a useful computing technology for large amount of data analysis and data storage. But, it is noticed that there is a risk in data transmission and number of threats has identified. Hackers encompass variety of techniques to gain access in unauthorized manner. In this paper, it tries to identify the denial of services (DOS) threat in Cloud Computing. Denial of Service (DOS) makes the server too busy and attempt to prevent the users from access in network for data information. It send excessive messages to the server and did not allow server to close the connection by sending messages, this make users to unable to access the server. This paper make attempt to gives solution to identify this threat by the hybrid techniques of Genetic algorithm and extension of Diffie Hellman algorithm.

Genetic algorithm is a heuristic search method to come across optimal solution of the problem by selecting fittest individuals and changes are made to produce new one. J.H. Holland has done some work for the expansion of Genetic algorithm. They provide a new aspect and try to attract the attention of many scholars, engineers and scientists. Both exploration and exploitation are used at equivalent time is showed by Holland and David Goldberg in Genetic algorithm by use of K-armed bandit analogy [1].

Diffie Hellman algorithm is a key exchange algorithm; it is not an encryption algorithm. It uses asymmetric key exchange type between sender and receiver. It is being proposed by Whitfield Diffie and Martin Hellman in 1976. As the inventor of this algorithm, Ralph Merkle was remarked due to his public key cryptography contribution.

Extended Diffie Hellman algorithm has been proposed for multi participants. Number of participants can exchange their secret keys in insecure network without knowing the knowledge of each other. It uses one private key on sender's side for encrypting data and on receiver's side for decrypting data. When the key swapping is approved in such a way that in last round the result is been generated, every participant require to add their private key to generate the secret key. And in this extended form of Diffie Hellman algorithm, number of exponentiation is reduce from *N* to *log2(N)+1* whereas steps of this method is also reduce from *N^2* to *3N-2* in comparison with traditional method. There is a table representation of above description is below [2].

Table 1: Comparative analysis of key exchange

Method	**Exponentiations**	**Number of Steps**
Diffie Hellman	N	N^2
Extension of Diffie Hellman	Log2(N)+1	3N-2

We will discuss, in this paper about the hybridization of Genetic algorithm and extension of Diffie Hellman algorithm try to get an idea to obtain a secure path for data transmission in insecure network without having prior knowledge of each other. It may help to identify the intruders which are inevitable and may affect the whole transmission or ma affect the data in between the transmission.

II. RELATED WORK

Diffie Hellman key exchange algorithm is proposed by Whitfield Diffie and Martin Hellman [3] explains a secure key exchange for exchanging data or messages. It was the

978-1-7281-5846-4/20/$31.00 ©2020 IEEE

first to appear the cryptography key exchange. Steiner M et al in [4] extended this algorithm for multiple users twenty year later, where they describe the class of natural extension of Diffie-Hellman algorithm for N number of users. The concept of extension of Diffie-Hellman is described by G.P. Biswas [5]. It generates multiple key with moderately few key generations overhead. Protection is provided additional to the key with increase in applicability. And on another side for large static group, multi-part key generated. Extension of DH algorithm for multiple participants is explained by Shivani Atish Goankar [2]. In this they use the Divide and Conquer method that allow total number of participants involves through raising the value of its exponent to obtain the key.

Tanya Singh discussed about the intrusion Detection System Using Genetic Algorithm for Cloud [6]. They discuss for data transmission with optimized path in insecure network. Intrusion detection and prevention in Cloud Computing using Genetic Algorithm has been discussed by Umar Hameed [7].

III. Some Traditional Cloud Cloud Threats

‘Notorious Nine Cloud Computing Threats’ were identify by cloud security Alliance as the most vital threats to cloud security and their relevance in present era. Cloud Security Alliance calculate from poll of industry experts, are displayed in Table 2 [8].

1. **Information Breaches:**
   A data breaches is an unauthorized action as security incident that hurt businesses and consumers in a variety of ways. It lies hidden within the system of the code.

2. **Data Thrashing:**
   Data loss is a serious problem, in this number of data or information is lost during storage, transmission and in processing. It also happen when system get damage physically by natural disasters.

3. **Cloud Account or Service Traffic Hijacking:**
   In this threat if a hacker get credentials of the user. Then they can access the account or services that are provided the cloud. Eavesdropping of the activity of user may be done by them without having any idea to the user.

4. **Insecure Interface and APIs:**
   Cloud server provide numbers of software interface and APIs to the user to have interactive communication but hackers built value added services upon the interface to the customers.

5. **Denial of Services:**
   In Denial of Services, intruders get access in data transmission. It makes the server busy so that no other user can access to the user by sending data continuously. Even server can not able to close the connection because of the continuous transmission of data.

6. **Malicious Insiders:**
   To influence the confidentiality, integrity and availability of the organization’s data or information it misuses the access of the organization or intentionally exceed.

7. **Abuse of Cloud Services:**
   It is a part of service provider issue rather than a Cloud consumer problem. When the,
   Nefarious cloud instances are causing congestion on the cloud platform.

8. **Insufficient due Diligence:**
   It is a type of investigation or audit for the company and businesses that are expected to take before entering into an agreement or contract with other party.

9. **Shared Technology Vulnerable:**
   In cloud there are number of resources are available as there is a huge amount of it. Number of users get access to these resources this make the resources inaccessible.

Table 2: Security Threats and their Relevance

Security Threats	Relevance
Abuse of Cloud Services	84%
Account or Services Traffic Hijacking	87%
Data Thrashing	91%
Information Breaches	91%
Insufficient due Diligence	81%
Insecure interface and APIs	90%
Denial of Services	81%
Malicious Insiders	88%
Shared Technology Vulnerabilities	82%

These types of threats or attacks may be solving by various algorithms. But in this paper, we will discuss on hybrid algorithms of Genetic algorithm and extended form of Diffie Hellman algorithm as the solution for the attack denial of services. It may give an optimized path for data transmission.

IV. Algorithm Used

1. Genetic Algorithm:

This algorithm reflects on changes immediately for the natural selection of the nodes where fitness of the individuals is determined. It is mostly used for searching. It provides a solution to the problem which related to the search.

It works in following steps:

i. **Selection:** In this process, a population of individuals is created. And from that selection of best group is been made for the further.

ii. **Crossover:** In crossover process, from number of groups only two chromosomes are selected for crossover to generate a new individual.

iii. **Mutation**: After the crossover process, mutation is performed to the new individual by changing any value of it so that it seems to be different from other individuals.

iv. **Fitness Function:** Fitness function is check to see whether the obtained individual is up to our desired goal or not.

Initially using the program logic N numbers of cities is generated, and fitness of each individual is calculated. Selection of the nodes/ cities is done, then crossover is process between the individuals and mutation is selected [6].

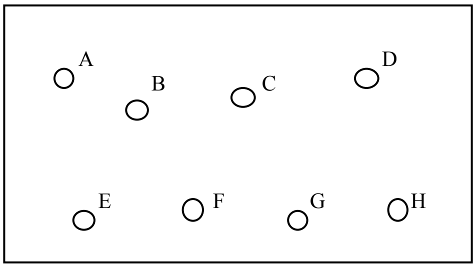

Fig. 1: There are 8 nodes/cities in the network.

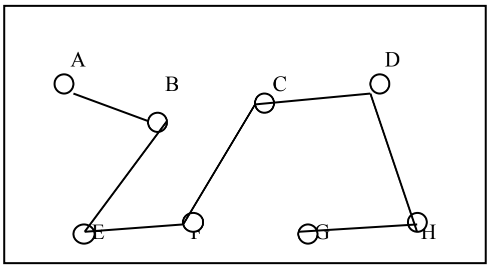

Fig. 2: Assume network path applying genetic algorithm.

2. Extension of Diffie Hellman Algorithm:

This algorithm uses key exchange technique in multiple participants/users. Users do not have the prior knowledge of each other and by using this algorithm they get a secure path for transmission. [2] In this divide and conquer method is used in multiple participant as it uses simple steps as exponentiation. Each participant has their own private key which they exchange in each round to get a secret key. Three participants encompass three slots with three key using this following arrangement.

i. The participants agree on two parameter p and m. And assumes'd', 'e' and 'f' as the private keys.

ii. In the first slot, David compute m^d , send it to Eliza. Eliza then compute $(m^d)^e = m^{de}$ and send to Fanny. Next Fanny computes $(m^{de})^f = m^{def}$ as her secret.

iii. In the second slot, Eliza compute m^e and send it to Fanny. Fanny compute $(m^e)^f = m^{ef}$ and send to David. David computes $(m^{ef})^d = m^{efd} = m^{def}$ as her secret.

V. Proposed Method

In this proposed method, the hybridization of the Genetic Algorithm and extension of the Diffie Hellman Algorithm is used to come across the optimized path for data transmission in insecure network. Without getting interrupted by any intruders it may gives an optimized path without data damaged or without getting server busy transmission may continuous and secure. In following steps:

i. First, initial populations are determined and selection process is done to get an optimized node of network to get an optimized path.

ii. Then crossover method is done by that selected group to get more optimized one.

iii. After the crossover process, mutation is been perform to make each path unique by changing one value of all individuals.

iv. Then using fitness function, it will check the fitness of the entire individual to find out whether they are according to our desire.

v. If intrusion is not detected during fitness check then process will remain start again until any intruders get detected. And if they get detected then divide the participants/nodes in two equal half and each participant/node get its own 'user key' also known as 'private key' will exchange to each other.

vi. During exchange of user key they will perform exponentiation and secret key will generate. Those nodes of network will have that secret key; the server will send the data or resources only to that node. By this no other node or intruder will get to enter in data transmission and transmission become secure in insecure network.

978-1-7281-5846-4/20/$31.00 ©2020 IEEE

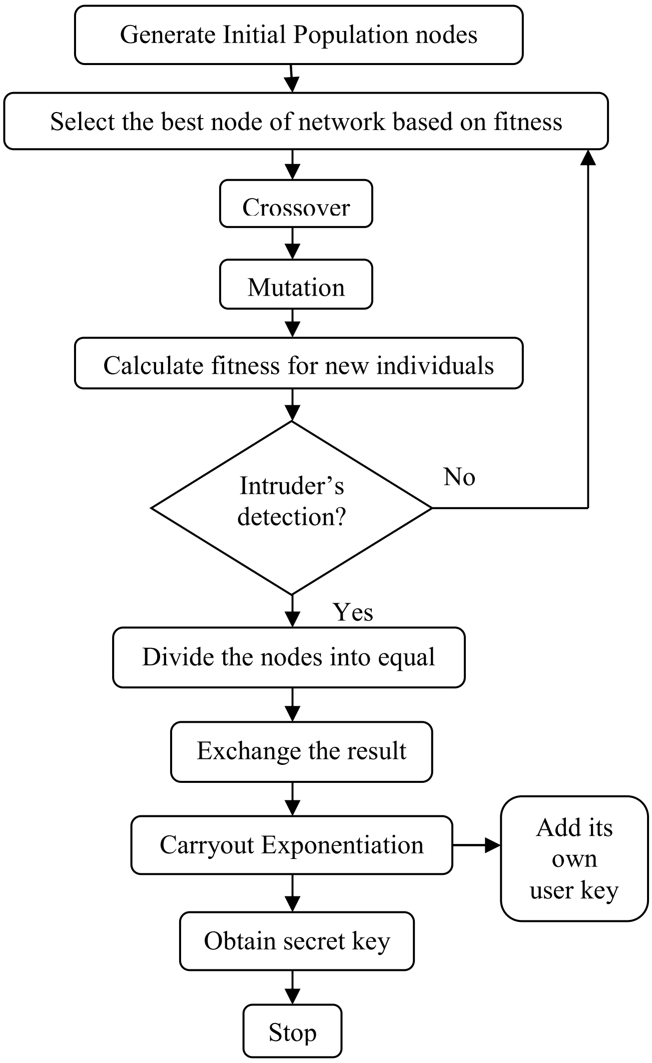
Generate Initial Population nodes
Select the best node of network based on fitness
Crossover
Mutation
Calculate fitness for new individuals
Intruder's detection?
No
Yes
Divide the nodes into equal
Exchange the result
Carryout Exponentiation
Add its own user key
Obtain secret key
Stop

Fig. 3: Flow Diagram of proposed hybrid Genetic algorithm and extended Diffie Hellman algorithm.

VI. ANALYSIS AND DISCUSSION

This paper studies various algorithms, the genetic algorithm with extended form of Diffie Hellman algorithm tries to give the optimized path by selecting the best path for data transmission without any interruption. This may result as finding best optimized path is best way to find intruders.

VII. CONCLUSION

In this paper, it tries to conclude that use of genetic algorithm and extension of Diffie Hellman algorithm give a most optimized path for data transmission in insecure network by detecting intruders before it disrupts the transmission or data. By using this algorithm it do not allow any intruders to make the server busy. In future scope it can have an enhanced implementation of our current proposed model with other algorithms.

VIII. REFERENCES

[1] Frederick Hayes-Roth, "Adaptation in natural and artificial systems by John H. Holland," University of Michigan Press, Ann Arbor, 1975.

[2] Shivani Atish Gaonkar and H. Manjunath Pai, "Extension of Diffie Hellman Algorithm for Multiple Participants," IJIREEICE, vol-3, April 2015.

[3] Whitfield Diffie and Martin Hellman, "New Directions in Cryptography," IEEE transactions on information theory, vol-22, pp. 644-654, November 1976.

[4] Steiner M, Tsudik G, Waidner M, "Diffie Hellman key Distribution extended to groups," Conf. computer and communication security, pp. 31-37, 1996.

[5] G.P. Biswas, "Diffie Hellman technique: extended to multiple two party keys and one multi party key," IET Information Security, vol-2, pp. 12-18, September 2006.

[6] Tanya Singh, Seema Verma, Vartika Kulshrestha and Sumeet Katiyar, "Intrusion Detection System Using Genetic Algorithm for cloud," ACM, March 2016.

[7] Umar Ahmed, Shahid Naseem, Fahad Ahamd, Tahir Alyas and Wasim-Ahmad Khan, "Intrusion detection and prevention in cloud computing using Genetic algorithm," International Journal of Scientific & Engineering Research, vol-5, December 2014.

[8] Ather Sharif, Sarah Cooney, Shengqi Gong, Drew Vitek, "Current Security Threats and Prevention measures relating to Cloud services, Hadoop Concurrent Processing, and Big Data," IEEE 2015.

978-1-7281-5846-4/20/$31.00 ©2020 IEEE