INTERNATIONAL JOURNAL OF SOFTWARE ENGINEERING & COMPUTER SYSTEMS (IJSECS)
ISSN:2289-8522 e-ISSN:2180-0650
VOL.8, ISSUE 1, 69 –78
DOI: https://doi.org/10.15282/ijsecs.8.1.2022.7.0097

ORIGINAL ARTICLE

# Optimized Genetic Algorithm and Extended Diffie Hellman as an Effectual Approach for DOS-Attack Detection in Cloud

Himanshi Chaudhary[1], Himanshu Chaudhary[2], Awadesh Kumar Sharma[3]

[1]Department of Computer Science & Engineering, Madan Mohan Malaviya University Of Technology, Gorakhpur, U.P., India.
[2]Department of Information Technology, Indian Institute Of Information Technology, Allahabad, U.P., India.
[3]Department of Computer Science & Engineering, Madan Mohan Malaviya University Of Technology, Gorakhpur, U.P., India.

**ABSTRACT**– Cloud computing is a mode to increase competence and capabilities devoid of investing in any infrastructure. It seems that in cloud computing environment the major problem that ensure the secure communication and protect responsive data in open networks from unauthorised access. These days it seems the headlines are jam-packed with stories about security breaches to these services; that result in the leak of a large amount of private data of the users. As cloud computing can offer new computing benefits, but it faces soaring risks, specifically on the security side where DOS attacks can make cloud services unavailable. This paper aims to turn up an effective method of detecting DOS attacks with an optimized Genetic algorithm and extended version of Diffie-hellman algorithm. To prevent data loss or corruption caused by the insiders in the cloud, Optimized Genetic Algorithm (OGA) is utilized, which effectively recovers the data and retrieve it if the missed data without loss. It is then followed with the decryption process as if requested by the user. An optimized path assortment for information broadcast proves to be an effective method in the cloud computing atmosphere. The proposed framework ensures certification and paves way for secure data access in an unauthorized network, with improved performance. It successfully assure the high level of protection of the transmission and data transmitted. And concurrently reduce the communication complexities.To reduce time complexity and detect the attackers by mutual secret key that is brought on using extended version of Diffie-hellman to endorse available key generation.

**ARTICLE HISTORY**
Received:10 June 2021
Revised: 27 March 2022
Accepted: 5 April 2022

**KEYWORDS**
*Genetic Algorithm;*
*Extended Diffie hellman Algorithm;*
*Encryption time;*
*Decryption time;*
*Cloud Computing;*
*Intruders;*
*Intrusion detection;*
*Middle-man attack;*
*Denial of services*

## INTRODUCTION

In everyday life, cloud computing is broadly used to store a large amount of data with some more advanced forces. An authorized NIST introduces Cloud computing in their definition as "Cloud computing is a replica for allowing pervasive, expedient, on-demand set-up access to a mutual pool of configurable computing resources (e.g. networks, servers, storage space, applications, and services) that can be quickly accosted and unconfined with nominal administration endeavour or overhaul source interface".

With today's covid pandemic, we can observe that cloud computing is becoming a new normal now. The organization and entities, the bigger organization, and the smaller one are planning to move towards the cloud. It means the entities which have the traditional infrastructure had to face some problem before move towards complete work from home. As most of the organization since they had the traditional infrastructure could not move 100% towards work from home while for the entity which were on the cloud or which were leveraging the services from the cloud could utilize the cloud services and up to some extent they were able to move towards work from home and that was quite efficient and quite quick as well. Although cloud security is always an important issue for cloud providers and users. The risk and errands will be shared, flanked by the cloud provider and customer, the eventual permissible responsibility for unofficial and illegitimate data disclosures will stay with the customer as the data proprietor. But, while transferring, storing, and retrieving information from the cloud fail to clinch safety and solitude. Each time a user uploads or makes any move of their data or file, it gets destroyed or attacked by several malicious software variants like viruses, ransomware, spyware, trojan, etc. In case the information is uploaded effectively in the cloud. Then, safety issues arise with the third revelry. The third-party gets access and acts as a user for the server or acts like a server for a real user. Which results, that they can destroy the data or they can misuse the pieces of information.

Hence, many researchers focus on the security issues and come up with many solutions such as ERGOT, HSDRT, PCS, Cold and Hot backup technique, SBBR, Linux box, which gives a great response to this issue but the implementation of this solution was quite expensive and also complex. And these drawbacks result, the cloud lost its total security and loss of trust of the users.

*CORRESPONDING AUTHOR |Himanshi Chaudhary | ✉Himanshichaudhary1805@gmail.com

Hence, the problem associated with the Denial of services (DOS) attack is that once the intruders enter the transmission network, it will harm the stream of packets that will dislocate the entire diffusion. This is because of the less optimized path that attacks happen like denial of services. The main crucial point will be on intruders that identified the areas where network interruption was caused. If the networks are not optimized, verdict such kinds of attacks would have been complicated i.e., with hefty communication time with the longer trail, inferior communication haste. Thus, to tackle the above scenarios, this commentary seeks to recommend a framework for an unoptimized network with a Genetic algorithm and Diffie Hellman algorithm to make certain safety and solitude for the data stored in the cloud by fixing maximum cloud security threats with reducing computational overhead.

## RELATED WORK

The topmost threat in the cloud is the security measures, according to a survey that is being conducted by the IDC survey about Cloud computing challenges. Many existing issues are not introduced yet. Moreover, disturbing the service of Cloud computing still new challenges persist to materialize. These challenges become the well-known Cloud computing paradigm. Hence, this related work has been carried out in chronological order to review the existing work on the challenges faced by the cloud provision contributor and the user.

**Kangchan Lee,** [6] introduces some of the technical components of the CC in layered approach and conditions of CC safety measures topic based on scrutiny of cloud safety measures intimidation. In which he made aware of some threats of cloud service users together with providers. As when service is served on the cloud then cloud service contributors also need to maintain their network from unauthorized access.

**Te-Shun Chou**, [4] approaches by introducing the cloud service models like SaaS, PaaS, and IaaS with naming their providers along with the models. It gives a scientific process for the arrangement of the discussion. It introduces the abusive use of CC resources in which it discusses the DOS attack. Data breaches and online cyber theft are also introduced by the author as one of the most important issues. He makes a small discussion on the safety measures, attacks also like Malware inoculation attack and covering attacks. In the end it comes up with the solution measures like safety measures policy enhancement, admission management, and data defense and safety measures techniques functioning.

**Mohd Nazri Ismail et al.,** [7] discuss their study on the CC architecture along with the challenges that affect the CC users and providers too. A small discussion of related work along with the detecting method was also there. They proposed a framework that depends on the covariance matrix mathematical modeling with three stages and it is further discussed with the detection and prevention stages.

**Ather Sharif et al.,** [8] discuss the current security measures along with their solution to attacks relating to big data, Hadoop, and the cloud services. They identified some major attacks of the cloud which has been studied with the cloud safety measures coalition as the nine notorious CC. They give a tabular representation of the threats along with their relevance. Introduce Verizon's cloud infrastructure with a layered approach. A brief discussion is made by them on big data and also a sticky policy. Hadoop's introduction is given in their study.

**Deyan Chen and Hong Zhao,** [9] briefly discussed on the solitude and information safety issues in the cloud. They additionally divide the whole discussion into two phases. In phase II they discuss the security-related issues in brief along with the cloud security architecture. In phase III they discuss the safety method and solitude protection issues in CC across all stages of the information life phase. In section IV they discussed the solution to the privacy and security issues in the cloud.

**Md Tanzim Khorshed et al.,** [10] is a special-issued paper in which they discuss the classification of DOS attacks in the cloud. In their first section, they describe the main aspects of the CC. After that section they discuss the gaps that hinder in slowing down the cloud adoption by the users, as users are still unaware of CC services. As they feel insecure about their data to use the services of the cloud due to the threats that are introducing day by day. In the next section, they narrate the challenges of hazard remediation. By this, they proposed a model to recognize the DOS attacks in CC by using the ML technique that is rule-based supervised learning. They have done the further implementation to execute the proposed work by using a statistical ranking approach and found that C4.5 and PART technique both are efficient to get the solution for the task of DOS attack.

**Tanya Singh et al.,** [12] discusssion on cloud challenges and attacks that occur in the CC environment. They discuss the CC introduction along with the attacks that occur in the cloud services. They give a brief discussion on the comparison of the different algorithms with the genetic algorithm. A tabular discussion on the comparison between Aho-corasick algorithms, split ac algorithm, Rabin-Karp algorithm, and genetic algorithm. They prefer a genetic algorithm for their study because the conservative methods give the best result just by functioning only one solution, but in a genetic algorithm it takes several populations to get an optimal solution. They give a proposed methodology by enhancing the properties of the genetic algorithm. They took Microsoft Visual Studio™ application for their implementation on 10 nodes to discover the most excellent optimized conduit for the information transmission that make transmission secure, fast and intruder can easily detect in the transmission.

**Umar Hameed et al.,** [13] is a brief study on the interruption discovery and avoidance in CC using Genetic algorithm. They give a discussion on the CC introduction and genetic algorithm introduction. They give a proposed model by giving a framework of intrusion detection system by representing the working of the genetic algorithm unit. Their proposed model focuses on voice data legitimacy with the use of genetic algorithm features.

**Shivani Atish Gaonkar and H. Manjunath Pai,** [14] is a brief discussion on the Diffie-Hellman algorithm and give a comparative study of the Diffie-Hellman algorithm and the extended version of the Diffie-Hellman algorithm for

manifold participants. They give a software implementation on both the studies with MATLAB, and a hardware implementation by using the DSP TMS320C6713 kit processor. Their study comes up with the result that the extended Diffie-Hellman algorithm gives fewer steps and exponentiation for the key exchange than the Diffie-Hellman algorithm.

**S. Subashini and V. Kavitha,** [15] it is a brief survey in which the author discussed the complexity of security in the CC environment. They discuss the issues which occur in the service model of the cloud that is related to the safety measures. A brief discussion on the SaaS, PaaS, and IaaS security-related issues. Along with the security issue, they give the current solution for the issues of the cloud safety measures.

## PROPOSED FRAMEWORK

### Hybridization of Genetic algorithm and extended version of Diffie-hellman algorithm

Based on our literature survey, we find that there are still some issues related to cloud security attacks. As the demand for the cloud increases day by day as it becomes exposed to various attacks. People are still unaware of using cloud computing due to the gaps that hinder to use of the cloud. The gaps indicate the attack issues and threats that make users think twice before using the cloud service.

An explore-based optimization algorithm is a genetic algorithm. Natural selection and genetics are the two aspects on which genetic algorithms are based. The best explanation on the dilemma of crossway approach, by absolute changes to produce new one and selecting the best individual is termed optimized Genetic algorithm as heuristic search method. Some work is ended by J.H. Holland for the optimized Genetic algorithm. They endow with a latest facet and strive to pull towards you the awareness of numerous scholars, engineers, and scientists.

This move towards based on Darwin's continued existence of the fittest and bio-inspired operators such as combination crossover and mutation are being processed in it. From that population children get produce, and every child produced, gets assigned a fitness number. From that fitness number of the children best parent are being chosen. It is recurrently used to find the best or near-best solutions to hard exertion.

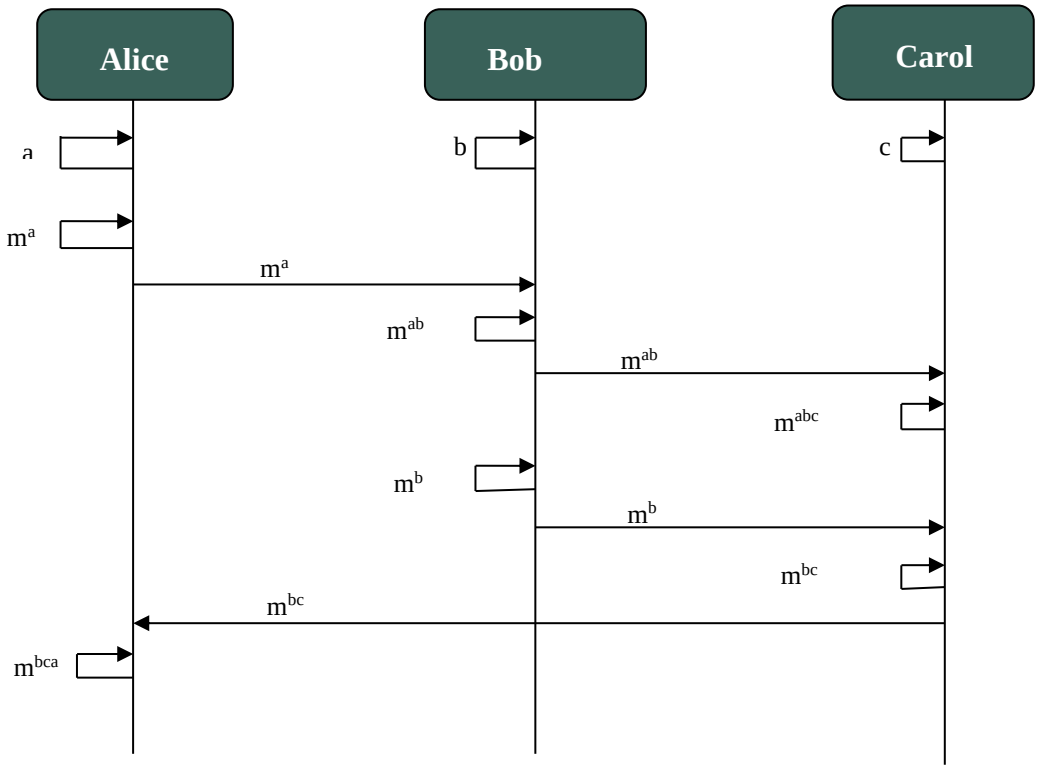


**Figure 1.**Three parties extended Diffie Hellman key exchange

As in Diffie Hellman the communication is created between sender and receiver only, but extended version of Diffie Hellman allow a number of users to communicate with each other. One private key is used in encryption time by the sender and other one in decryption time by the receiver. For communication with multiple users in the extended version of the Diffie Hellman algorithm , every participant gets an identity key which is the private key to create a secret key between them so that the server can send the data to those users who have that secret key. As it result in key swapping between the users and it is approved in such manner that in last stage every user should get secret key by adding their identity key. In extended version of Diffie Hellman algorithm, numberof steps and exponentiation is reduced from N^2 to 3N-2 and N to log 2(N)+1 as compared to traditional one.

In DOS (Denial of service) attack, the outsider or unauthorized person aims to render a computer or other available device to its intended users, so that it can interrupt the device function. It is a type of attack in which it tries to make the network busy by requesting continuance, so that authorized users can not be able to process. It oversaturates the capacity of the targeted machine or network to make the whole function unavailable. The proposed work aims to design a technique in which maximum intruder can be detected even for the long transmission also whenever an intruder gets detected.

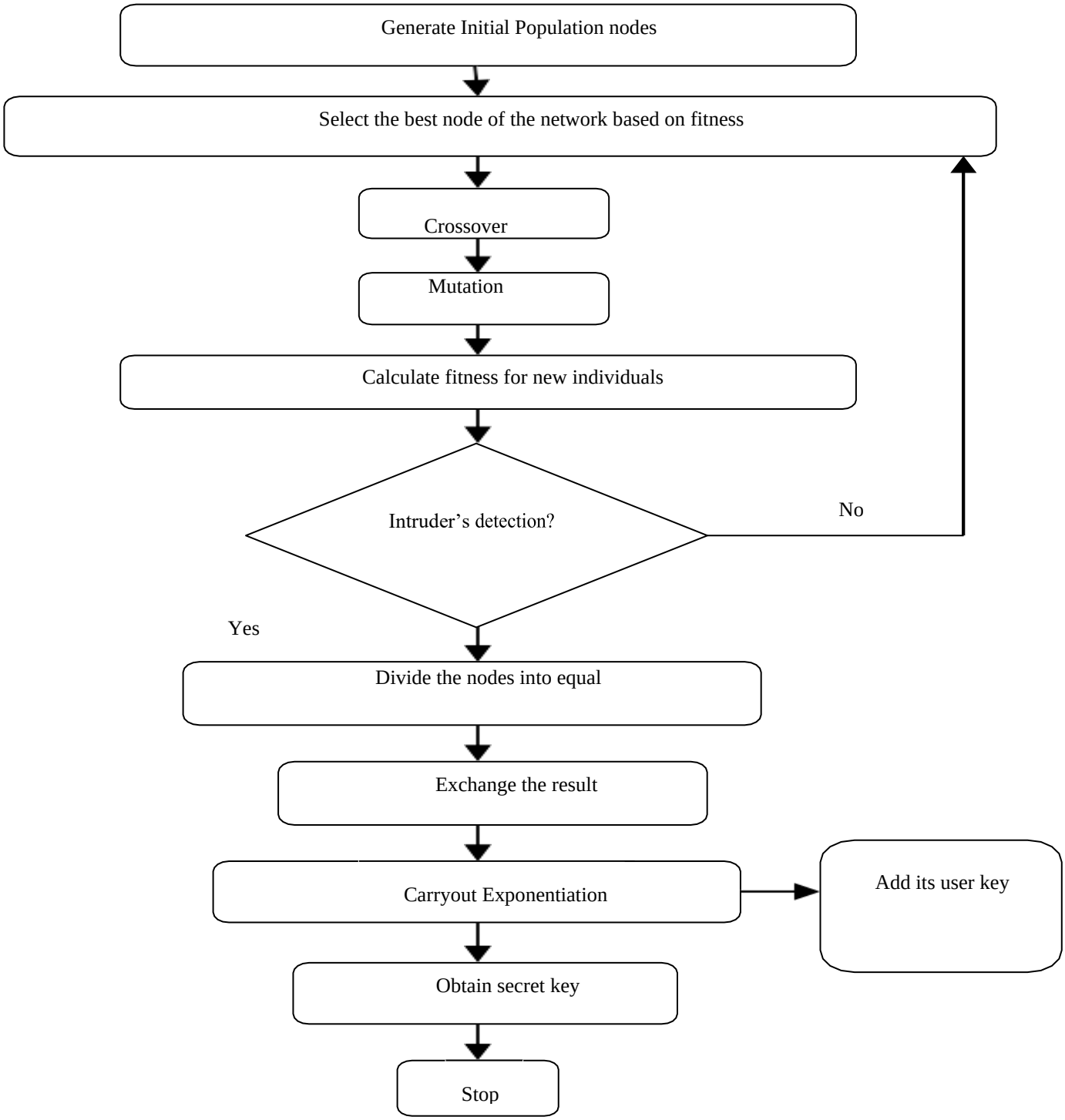


**Figure 2.** Flow diagram of the proposed framework [21].

The main crucial point will be intruders that identified the areas where network interruption was caused. If the networks are not optimized, verdict such kind of intrusion would have been complicated i.e. with hefty communication time with the longer trail, inferior communication haste. Hence, as compared to our optimized network, any disturbance in the set-up would not be tinted as rapidly and obviously.

Based on Figure 2, the algorithm a secure path can be obtained in the unoptimized network by the hybridization of the optimized Genetic algorithm and extended version of Diffie Hellman algorithm techniques. It detects the intruders during transmission and repeat the process again and if intruders is not detected, then transmission get continue as constant and safe transmission.

Explanation of flow diagram given below

- At begin, the number of populations is considered to go through the selection procedure so that an optimized path can be obtain among them.
- Then that optimized paths go through the crossover method so that more optimized one can be obtained.
- After the crossover procedure between the optimized paths, it will result with the optimized one and mutation is performed on the optimized one by some changes made in the individual to make the path unique.
- After getting the unique one, to check whether the individual is up to our expectations or not, the fitness function is used in further process.
- During the fitness function check of the individuals, if any intruders or any disturbance is been detected in the transmission. It will restart the process and if any disturbance will not occur, it will divide the number of users separately in two divisions and each user get a private key/ user key as an identity.
- Each user exchange their private key with each other to generate a secret key from beginning to get the unique result. Those users get that secret key the server will transmit the data only to that user even in unoptimized network. It will be a secure transmission within insecure network.

Our projected methodology consists of two phases that are as follows.
Phase I: Detect the intruders, if no intruder gets detected, it keep on selecting the best for the transmission.
Phase II: Applying the divide and conquer method to detect the intruders and generate a secret key for all the nodes of the path to get secure transmission.

**Algorithm (Phase I)**

```
{
Begin
Initialize the generate population
For      Choose best node path
        Apply Fitness Function
         {
Begin
                        Exchange of different node path
                        Get a change in value
                         Fitness value = 1
          If        intruders detected
                    Go to Phase II
Else
                     Choose the best node path
                     }
End
 End
}
```

**Algorithm (Phase II)**

```
{
  Begin
  For       Best Node Path
            Apply Divide & Conquer Method
     Then       Exchange the result
     {
     If         User add the user's key
     Then
                Carry the exponentiation
                 Obtain the secret key
           }
       End
    End
}
```

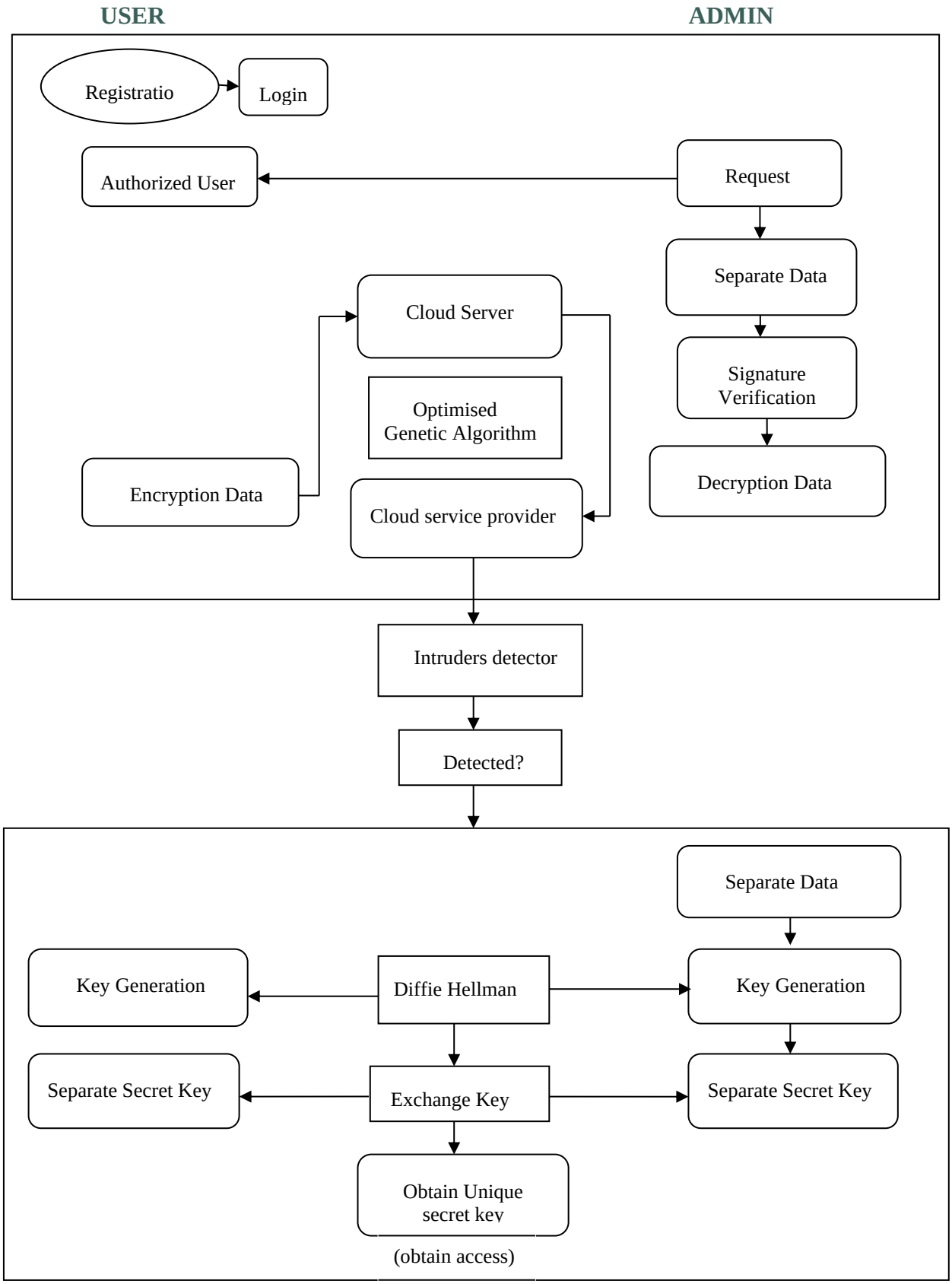


**Figure 3**. Our overall proposed framework

A verification configuration of cloud computing architecture is predictable by depending on the uniqueness of the verification. However, not more than some of the verification protocols in cloud computing have been predictable, but some of the protocols are predicted as the issue arises that an eavesdropper watches the data or information that is being transmitted or make the connection disabled for the users to access. They make the service failure so that transmission of the data can not become possible. In this paper, each and every structure is developed in such a way to highlight the above

mentioned issue with some previous methodology and knowledge. It successfully assures the highest level of protection of the transmission and data transmitted. And concurrently reduce the communication complexities.

## FINDINGS AND ANALYSIS

Cloud Computing has turned into a helpful computing technology for a huge quantity of data analysis and data storage. But, it is identified that there is a risk information broadcast and the number of intrusion is well known. Hackers include an assortment of methods to increase access in an unconstitutional mode. This study tries to come up with the brief explanation and solution to DOS (Denial of Services) attack within cloud computing. Denial of service attack makes the server too busy for the authenticated users or, they triy to make the network failure. Authenticated users become unable to send or receive any data from the server as the network is occupied by the intruders. This paper come out with the challenge to identify the DOS threat from the network so that it can not able to make the network busy by the collaboration of optimized Genetic algorithm and extended version of the Diffie Hellman algorithm.

With this projected method, the hybrid technique of the two algorithms gives a way to make a safe and secure communication for the user even in the busy network. The hybridization of optimized Genetic algorithm and Diffie Hellman algorithm is able to give a great framework to identify the intruders before establishing the transmission within the network and allow authenticated user to transfer the data in a safe and secure manner.

This framework selects the best optimized path for data transfer without any interruption in the transmission to locate the intruder before it do any harm to the transmission.

To analyze the effectiveness of our projected model, the following factor is evaluated.

**Encryption time**

In an Encryption algorithm exchange of the plaintext into the ciphertext results within an exacting duration which is believed to be an Encryption point. The estimated framework with an optimized DHA (Diffie Hellman Algorithm) technique is associated with the Encryption measures that Encrypted the Encryption duration of the data.

$$\text{ENCRYPTION TIME} = \frac{e_T}{R_T}$$

Where Encryption time is at the, $e_T$ the computational time of Encryption by $R_T$ the reply time of Encryption. This duration is the differentiation between the submission of the demand until reply that starts to receive.

**Table 1.** Encryption Time for the proposed framework

| FILE NO. | FILE SIZE (KB) | ENCRYPTION TIME (MS) |
|---|---|---|
| F1 | 18 | 294 |
| F2 | 24 | 301 |
| F3 | 40 | 315 |
| F4 | 49 | 325 |
| F5 | 56 | 342 |

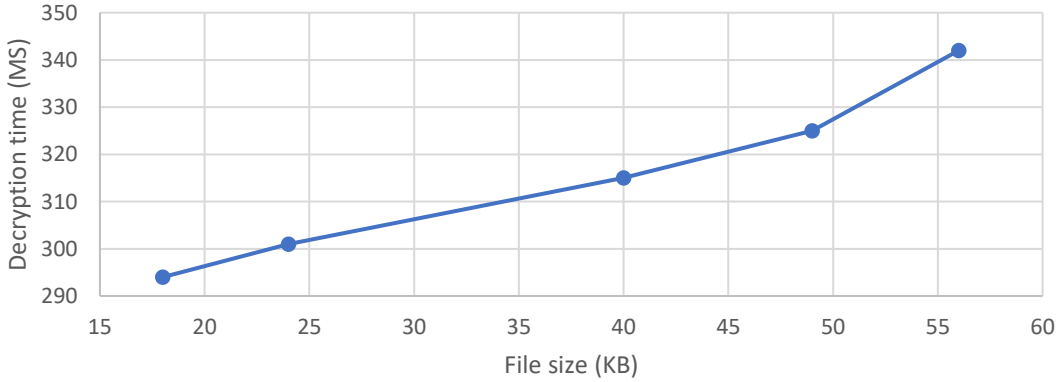


**Figure 4.**Encryption time

In table 1, it is identified that encrypting time for a framework proposed for different files F1, F2, F3, F4, and F5 with file size 294, 301, 315, 325, and 342.

In figure 3, shows that various files are used in encryption time in the projected method. It is accessed based on the division of the $e_T$ and $R_T$. Encryption ciphertext policy quality, access the encrypted text. As file dimension increases, it also increases the encryption time.

**Decryption time**

In the Decryption algorithm exchange of the ciphertext into the plain text results inside a exacting period which is said to be Decryption time. The Decryption duration of the data after decrypting it by the predictable framework relates to the Decryption measures.

$$\text{DECRYPTION TIME} = \frac{d_T}{S_T}$$

Where decryption time is the, $d_T$ the computational time of decryption by $S_T$ the reply time of Decryption. This duration is the variation between the submission of the request until response that starts to receive.

**Table 2.** Decryption time for the proposed framework

| FILE NO. | FILE SIZE (KB) | ENCRYPTION TIME (MS) |
|---|---|---|
| F1 | 18 | 256 |
| F2 | 24 | 295 |
| F3 | 40 | 310 |
| F4 | 49 | 321 |
| F5 | 56 | 335 |

In table 2, it is identified that decrypting time for a framework proposed for different files F1, F2, F3, F4, and F5 with file size 256, 295, 310, 321, and 335.

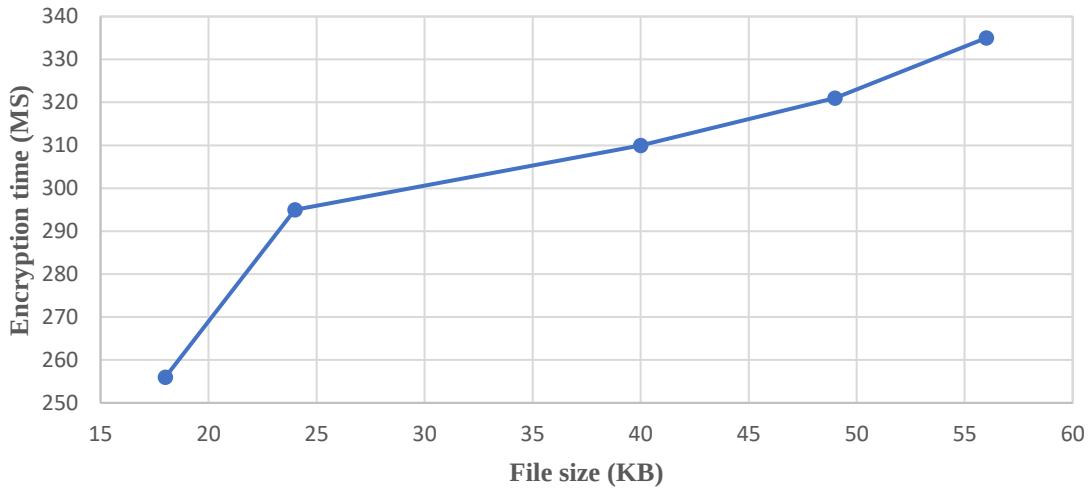


**Figure 5**. Decryption Time

In figure 3, shows that various files are used in decryption time in the proposed technique. It is accessed depends on the division of the $d_T$ and $S_T$. Decryption ciphertext policy quality, access the decrypted text. As file size increases the decryption time also increases.

Due to probable data exploitation by interior outbreaks i.e., insider attacker adds in clambered data into the encrypted data or even to the encrypted index, the search result can be a fault result. So there is a need for a security mechanism to verify and retrieve the desirable file. The Optimized Genetic Algorithm (OGA) is an advanced file hold-up concept that uses an operative ultra-widely distributed data transmission mechanism and high-speed encryption technology. The backup sequence and Recovery sequence are used in the proposed system. In the Backup sequence, it accepts the data to be backed-up and in Recovery Sequence, when some mischance happens the Cloud Server (constituents of the Optimized Genetic Algorithm) begins the recovery arrangement. Though there are some restrictions such as security issues. To secure these issues, the OGA method performed in figure 6.

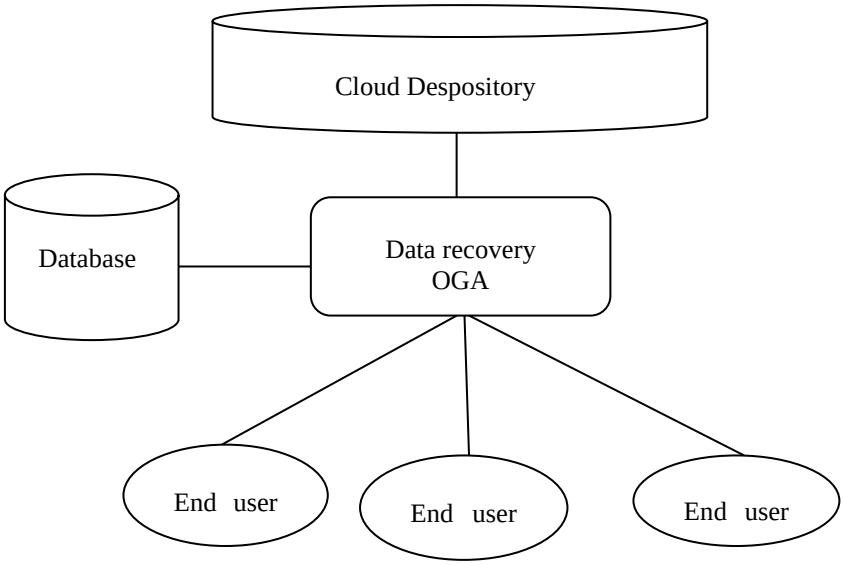


**Figure 6.**Securing data with oga(optimized genetic algorithm)

## DISCUSSION

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 a variety of techniques to gain in access an unauthorized manner. In this study, it tries to recognize the denial of services (DOS) threat inside Cloud Computing. Denial of Service (DOS) makes the server too busy and attempt to prevent the users from access to the network for data information.

It sends excessive messages to the server and did not allow a server to close the connection by sending messages, this make the user unable to access the server. This paper make an attempt to give solution to identify this threat by the hybrid techniques of Genetic algorithm and extension of the Diffie Hellman algorithm.

In this proposed method, the hybridization of the Genetic Algorithm and extension of theDiffie-Hellman Algorithm is worn to come across with the optimized way for information communication within insecure network. Without getting interrupted by any intruders it may give an optimized path without data damaged or without getting a server busy transmission may continuous and secure.

The genetic algorithm with extended forms 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 the best optimized path is the best way to find the intruders.

## CONCLUSION

As cloud computing faces elevated risks and most of them give more awareness to one side either detecting or track backs or prevention as they can offer new computing benefits, but specifically in the security phase where DOS (Denial-of-service) attack can make cloud services unavailable, and several methods have suggested. All the aspects of the problems are focused on by our new framework.

It tries to wrap up that the utilize of optimized genetic algorithm and extended version of the Diffie Hellman algorithm gives a nearly all optimized path for information transmitted in the timid network by identifying intruders earlier than it intrupted in the tranferring of the data packets. This algorithm results with not permitting the intruders to make the server or network busy.

Using an extension of DHA (Diffie Hellman algorithm) as fewer numeral of exponentiation is present with a fewer number of steps are that is involved rather than a Diffie Hellman algorithm. Thus, in our projected work the security threats are extremely under arrest, which ensures a protected data storage and transmission with condensed computation time and cost.

## ACKNOWLEDGEMENT

We thank all sponsors in the footnote on the first page for funding this ongoing research project. And thanks to all volunteers for their involvement in this research project, especially to Dr. Awadesh Kumar Sharma, Professor of the Department of Computer Science, Former H.O.D. at Madan Mohan Malaviya University of Technology (MMMUT, Gorakhpur, India) for his continued support, guidance and the knowledge conveyed.

## REFERENCES


[1] A. T. H. Ibrahim, Ibaryaqoob, N. B. Anuar, S. Mokhtar, A. Gani and S. U. Khan, "The rise of 'Big Data' on cloud computing," Elsevier publication, pp. 98-115, 2015, DOI:10.1016/j.is.2014.07.006.

[2] A. Giuseppe, B. Alessio, D. Walter, P. Antonio, "Survey cloud monitoring: a survey," Computer Network, pp. 2093-2115, 2013, DOI:10.1016/j.jpdc.2014.06.007.

[3] T. Gunarathne, B. Zhang, T. ~L. Wu and J. Qiu, "Scalable parallel computing on cloud using twister azure iterative mapreduce," Future Journal Computer System, pp. 1035-1048, 2013, doi: https://doi.org/10.1016/j.future.2012.05.027.

[4] C. Te-Shun, "Security threats on cloud computing vulnerabilities," International Journal of Computer Science & Information Technology (IJCSIT), Vol. 5, No. 3, June 2013, DOI:10.5121/ijcsit.2013.5306.

[5] D. Catteddu and G. Hogben, "Cloud computing benefits, risks and recommendations for information security," The European Network and Information Security Agency (ENISA), November 2009, DOI:10.1007/978-3-642-16120-9_9.

[6] L. Kangchan, "Security threats in cloud computing environment," International Journal of Security and its Applications, Vol. 6, No. 4, October 2012,

[7] M. N Ismail, A. Aborujilah, S. Musa and A. Shahzad, "New framework to detect and prevent denial of service attack in cloud computing environment," International Journal of Computer Science and Security (IJCSS), Vol. 6, Issue 4, doi: http://dx.doi.org/10.15520/ajcsit.v4i12.12.

[8] S. Ather, C. Sarah, G. Shengqi, V. Drew, "Current security threats and prevention measures relating to cloud services, hadoop concurrent processing, and big data," IEEE 2015.

[9] C. Deyan and Z. Hong, "Data security and privacy protection issues in cloud computing," International Conference on Computer Science and Electronics Engineering, 2012, DOI: 10.1109/BigData.2015.7363960.

[10] K. M. Tanzim, A B M Shawkat Ali and Saleh A. Wasimi, "Classifying different denial-of-service attacks in cloud computing rule-based learning," Security and Communication Networks in Wiley online Library, Vol. 5, pp. 1235-1247, September 2012, DOI:10.1002/sec.621.

[11] M. T. Khorshed., "A survey on gaps, threat remediations challenges and some more thoughts on proactive attacks detection in cloud computing," Future Generation Computer Systems 2012, DOI:10.1016/j.future.2012.01.006.

[12] S. Tanya, V. Seema, K. Vartika and K. Sumeet, "Intrusion detection system using genetic algorithm for cloud," ACM, March 2016, DOI:10.1145/2905055.2905175.

[13] A. Umar, N. Shahid, A. Fahad, A. Tahir and A. K. Wasim, "Intrusion detection and prevention in cloud computing using genetic algorithm," International Journal of Scientific & Engineering Research, vol-5, December 2014, doi: https://doi.org/10.1145/2905055.2905175

[14] A. G. Shivani and H. P. Manjunath, "Extension of diffie hellman algorithm for multiple participants," IJIREEICE, vol-3, April 2015.

[15] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," Journal of Network and Computer Applications, Vol. 34, pp. 1-11, 2011, doi: https://doi.org/10.1016/j.jnca.2010.07.006.

[16] H. R. Frederick, "Adaptation in natural and artificial systems by john h. holland," University of Michigan Press, Ann Arbor, vol-18 issue-3, July 1976, DOI:10.1137/1018105.

[17] W. Diffie and M. Hellman, "New directions in cryptography," IEEE transactions on information theory, vol-22, pp. 644-654, November 1976, DOI:10.1109/TIT.1976.1055638.

[18] M. Steiner, G. Tsudik, M. Waidner, "Diffie hellman key distribution extended to groups," Conf. computer and communication security, pp. 31-37, 1996, doi: https://doi.org/10.1145/238168.238182.

[19] 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, DOI:10.1049/iet-ifs:20060142.

[20] S. Jerald Nirmal Kumar, S. RavimaranandM. M. GowthulAlam, "An effective non-commutative encryption approach with optimized genetic algorithm for ensuring data protection in cloud computing," CMES, 2020, DOI:10.32604/cmes.2020.09361.

[21] C. Himanshi, A.K. Sharma, "Hybrid technique of genetic algorithm and extended diffie hellman algorithm used for intrusion detection in cloud," ICEEE, 2020, DOI: 10.1109/ICE348803.2020.9122978

[22] C. M. Dan, K. Morgan, "Cloud Computing Theory and Practice," books.google.com, 2017.