Dragonfly Algorithm-based Detection Technique for Man-In-The-Middle Attack in Fog Computing Environment: A Conceptual Framework

Yakubu Jimoh[1], Shafi'i Muhammad Abdulhamid[2]
[1]Department of Computer Science,
[2]Department of Cyber Security Science,
Federal University of Technology Minna, Nigeria.
jimm.yack@futminna.edu.ng, shafii.abdulhamid@futminna.edu.ng

ABSTRACT—Fog computing is a recent model of computing, in a distributed way that extends the cloud computing operation to the network edges. Fog computing enables storage execution and tasks processing, which relies on the cooperation of users and resource sharing among various devices. The fog being the new shift to cloud computing addresses some critical challenges associated with cloud model by providing notable advantages which are location sensitivity, latency minimization, geographical accessibility, wireless connectivity, mobility support and improved data streaming. Nevertheless, fog computing concept is never an option for replacing cloud computing model. In spite of the attractive solutions found in fog computing, it also inherited some security problems from the cloud. Most of the proposed techniques to solve security issues in fog computing could not completely addressed the security challenges due to the limitation of the various techniques. A fog computing security approach that is based on man- in- the middle attack using Dragonfly algorithm (DA) detection algorithm is conceptualized here. This paper is a framework for detection of MITM attacks that exist between the fog nodes and the cloud and vice versa using swarm intelligence optimization techniques called the DA algorithm which is be implemented on the platform of ifogsim simulator.

KEYWORDS: **Fog computing, DA, MITM attack, Cloud computing, Fog security**

I. Introduction

Cloud computing model is viewed as the main integration of internet system because it possessed computational and storage ability, which does not exist in other devices. The increase in internet computation leads the web expansion, and is growing with complexity because of the addition of new technologies and solutions. The need for data processing and storage demands is astronomically on the increase. To address this phenomenon, Web architecture must be developed to meet user's data processing need [1]. Fog computing paradigm is a new concept developed to meet the latency requirement of the web architecture. The design greatly reduces latency and enhances network performance[2].

Fog computing emergence is still very new; this technology has already been embraced by the modern data center and the cloud. The technology is built upon the distributed computing paradigm especially the network's content delivery which ultimately paves way to additional complex services delivery through the use of cloud model technologies. Nonetheless, the distinction of fog computing from cloud is therefore, it nearness to the end user since they offers computation, data storage and provision of application services to the client. Fog computing model is never a replacing option of cloud computing rather, it is viewed as complementary to many applications and services in order to eliminate the inadequacies of the cloud [3].

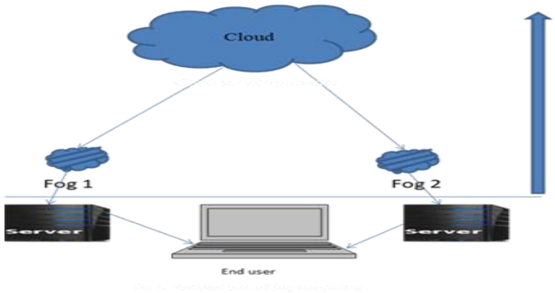


Figure 1: Fog and the cloud

The major contributions of our conceptual framework paper include:

i. We compare the fog and cloud computing environment and show case the structural design of fog architecture.
ii. We present and analyze the scenario of MITM attack in fog environment.
iii. We proposed swarm intelligence optimization techniques (Dragonfly algorithm*)* framework to detect MITMattack in fog computing environment.

The major purpose of our proposed paper is to develop a conceptual framework that will use swarm-intelligence optimization techniques called DA to detect Man-in-the-middle attack in fog computing environment using ifogsim simulator. The remaining section of this framework is structured as below: the Section II gives the overview of fog computing, section III summarized the reviewed similar research works, while section IV described the problem formulation and design model. Section V presents the Proposed DA Framework for MITM Attack, section VI introduced the dragonfly algorithm (DA) optimization and the associated equations, section VII describe the expected outcome of the model, section VIII recommends the future research direction and finally, section IX contain the conclusion of the paper.

II. FOG COMPUTING OVERVIEW

Fog computing idea was put forward by CISCO team of researchers in year 2012. The term was used to imply extension of cloud computing[4]. The main purpose is to deviate from the usual computing from cloud datacenters to heterogeneous users and edge devices. Fog computing enhances the operation of computation, data storage, and linking of datacenters with networking services between user devices and the cloud. Cloud computing has solutions of protecting network but these solutions in most cases might be unfit to fog environment. Fog computing is generally nearer to the end users and operated in a distributed approach since the various devices are working together at the network edge [5].

However, implementing fog computing technology introduces more number of security challenges. Although there are presently several techniques for detecting and handling the data security and also privacy problems in cloud environment. But these challenges are inherited in fog computing and it remains a major problem[6]. Organizations and data processing center need to find a medium through which more centralize distributed architectural design transmit data and information to the end-users. Fog computing idea was generated to distribute data in order to move it closer to the end-user, and to remove latency issues and give support to mobile computing as well as streaming of data [7].

III.RELATED WORKS

Stand-alone authentication mechanism to authenticate user when connection is not available to the cloud server was introduced by [3]. This was achieved through hybrid-encryption and attribute-based encryption. The former is a procedure to share data with a particular party in encryption while the latter is information like smart grid. Extending hybrid-encryption into one -to-many setting can address the connection issue if the two fog devices are in different areas. This authentication method enables users to be authenticated and have permission to establish connection between the fragile cloud and the fog devices. The team pointed out that this approach create another problem of calculating increase in smart users card especially if a new equipped devices that is to act as stand-alone is added. This problem according to the authors can be subdued through cryptographically primitive – Attribute-based encryption method. The authors described the attribute-based encryption as a viable tool, for providing data without necessarily having the fore-knowledge of the receiver of the data. This provides flexible sharing of data in flexible way more than the usual end-to-end encryption. However, the proposed technique is not capable of authenticating and authorizing user in a setup that is being distributed.

In fog environment, There exist gateways that represent fog devices that can be compromise by the activities of man-in-the middle attack[8] .The authors explained that it is difficult to use encryption and decryption algorithm to secure communication between the fog devices and IoT devices because the formal and the later consumes large amount of battery on mobile devices. As a result, it becomes difficult to detect the rootkit and the various types of malicious code that is present in the fog nodes. The team combined a fog node and the cloud to visualized a fog computing paradigm that produce high quality of services to the users to make up for the lapses of cloud in internet of things environment. Conversely, the result of the experiment conducted could not address MITM attack.

Insecure authentication protocols are viewed as the major security threat to fog computing platform and the end – user application devices [9]. The authors stressed that spoofing attack and data tampering are exposed to IoT devices that exist in smart grids which ultimately can prevent using infrastructure, intrusion detection techniques and Hellman key exchange. The investigation of Video call between 3g and Wireless LAN users in a fog network was conducted for Man-in-the middle attack which result shows that the attack did not reveal obvious changes in the memory utilization and CPU consumption of fog node. Also, Authentication scheme through securing communication channels between the fog environments was suggested by the authors to be adopted as preventive measure. Similarly Advanced encryption standard (AES) was also recommended as a viable encryption techniques for fog platform. Conversely, the security solutions put forward by the team are individualistic and therefore, not dynamic enough to secure fog platform in terms of confidentiality, integrity and availability.

IV. PROBLEM FORMULATION

Man-in-the middle attack (MITM) is demonstrated in Figure 2where the attacker inserted himself in-between the flow of traffic, the fog node and the cloud. The attacker can then inject false information and intercept the data transferred between them. More so, from the survey and the research analyses, Man-in-the-middle attack investigation remains a top priority for researchers due the stealthy nature of the attack

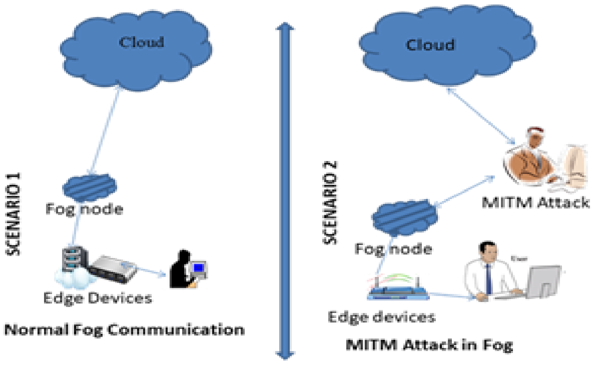
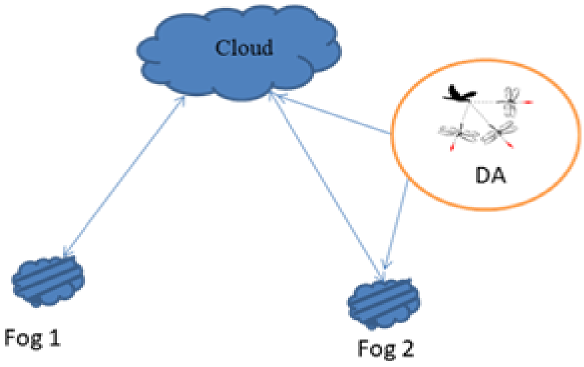


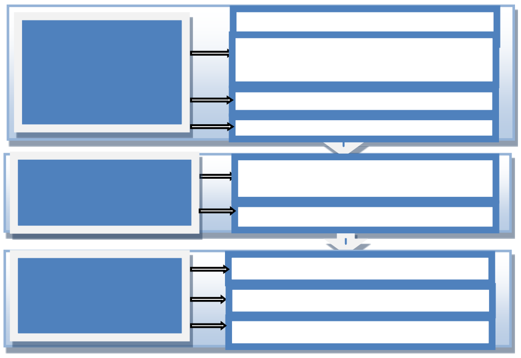
Figure 2. MITN attack scenario in fog environment

In the proposed model in Figure 3, the DA detects any malicious attacker, whose intention is to intercept all relevant information that is moving from fog node to the cloud or vices versa and inject false information in fog computing environment.

V. PROPOSED DA FRAMEWORK FOR MITM ATTACK

The proposed framework consists of 1st, 2nd and 3rd phases. The first phase contains problem formulation, planning and dataset description. The second Phase contains design and implementation which include Dragonfly Algorithm (DA) detection on ifogsim Simulator Platform, Model flowchart and Pseudocode. The third phase of the framework is the implementation, testing performance evaluation stage. This includes experimental setup, performance metric, and testing, and performance evaluation. Figure 3 shows the proposed DA detection framework for MITM attacks.





I.

VI.D

VI. DRAGONFLY ALGORITHM (DA) OPTIMIZATION

*D*ragonflyin comparison to other insects has exceptional good vision. It possesses two huge compound eyes, which has about 360 ° visions. Each of the compound eyes contains almost 30,000 lenses. A dragonfly uses almost 80% of the brain to process all the information within it view. The vision assists the insect to detect how the other insects move in order to avoid collisions when flying. Dragonfly possesses an active gaze control, with fixed eyes which enable them rotate their heads. This compels it to focus its target within five degree from the central view.

Seyedali Mirjalili proposed (DA) in 2015. It was derived from static and dynamic swarming insert behaviors. These behaviors are synonymous to the two main phases of optimization that uses meta-heuristics. They are exploration and exploitation. Dragonflies create sub swarms and then usually fly over different areas in a static form, which is the major objective in the exploration phase. The algorithm, described and model dragonflies social behavior in interaction when navigating, foods exploration and dynamically avoid enemies when swarming. There are two versions of the DA which are: binary DA (BDA) and multi-objective DA (MODA).There are five existing principles of swarming in dragonfly which have been utilized for aiding the swarming behavior of insects: separation, alignment, cohesion, attraction to food source, and distraction from enemies [10-14].

Separation indicates the static collision avoidance of the individuals from other individuals in the neighborhood. **Alignment** shows the velocity matching of individuals to another individual in neighborhood. **Cohesion** is the ability of individuals moving along the center of the mass of the neighborhood. All swarm exhibit struggle for Survival which is the major purpose of swarm existence; all the individuals should therefore, be attracted towards food sources and distracted outward enemies.

The swarm’s behaviors approach is evaluating for each individual as follows.

The separation is obtained as

$$Si = -\sum_{j=1}^{N} X - XjSi = -\sum_{j=1}^{N} X - Xj \qquad \textbf{(1)}$$

X is the position of the present individual, Xj indicate the position j-th neighboring individual While N is the number of neighboring individuals.

Alignment is obtained as

$$Ai = \sum_{j=1}^{N} Xj/NAi = \sum_{j=1}^{N} Xj/N \qquad \textbf{(2)}$$

Where Xj shows the velocity of j-th neighboring individual.

Cohesion is obtained as

$$Ci = \sum_{j=1}^{N} Xj/N - XCi = \sum_{j=1}^{N} Xj/N - X \qquad \textbf{(3)}$$

X is the position of the present individual; N is the number of neighborhoods while Xj indicate the position j-th neighboring individual.

The Attraction of the insect moving along a food source is obtained as;

X is the position of the current individual, and X^+ shows the position of the food source.

Dist fraction outwards an enemy is calculated as;

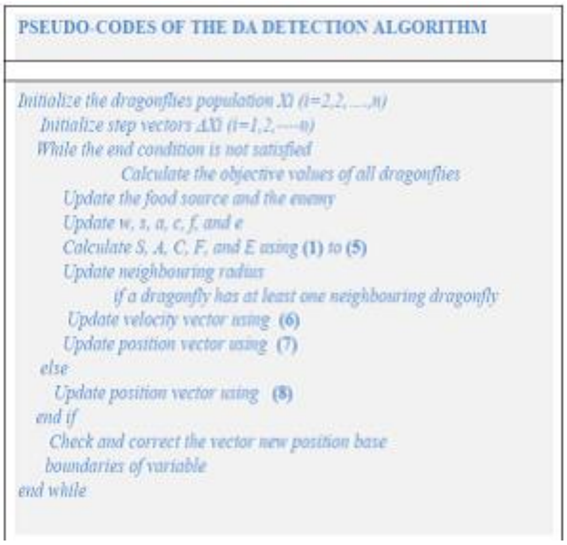
X is the position of the present individual, while X^- shows the position of the enemy.

The step vector indicates the direction of the movement of the dragonflies and obtained as;

the separation weight, Si shows the separation of the i-th individual, shows the alignment weight, A is the alignment of i-th individual, c shows the cohesion weight, Ci indicate cohesion of the i-th individual, f is known as the food factor, Fi is the food source of the i-th individual, e is the enemy factor, Ei is the position of enemy of the i-th individual, a is the alignment weight, A is the alignment of i-th individual, c indicates the cohesion weight, Ci is the cohesion of the i-th individual, Fi is the food source of the i-th individual, e is the enemy factor, Ei is the position of enemy of the i-th individual, w is the inertia weight, and t is the iterationcounter.

The position vector can be calculated as follows;

In order to enhance the randomness, stochastic behavior, and exploration of the artificial dragonflies, using a random walk (Le´vy flight) when there are no neighboring solutions the position of dragonflies is updated using the following equation:



PSEUDO-CODES OF THE DA DETECTION ALGORITHM

```
Initialize the dragonflies population Xi (i=2,2,....,n)
   Initialize step vectors ΔXi (i=1,2,----n)
  While the end condition is not satisfied
              Calculate the objective values of all dragonflies
      Update the food source and the enemy
      Update w, s, a, c, f, and e
      Calculate S, A, C, F, and E using (1) to (5)
      Update neighbouring radius
             if a dragonfly has at least one neighbouring dragonfly
       Update velocity vector using  (6)
      Update position vector using  (7)
   else
     Update position vector using  (8)
  end if
    Check and correct the vector new position base
    boundaries of variable
end while
```

Figure 5. Pseudo-codes of DA detection algorithm

VII. INITIAL RESULTS AND EXPECTED OUTCOME

To demonstrate the workability of our proposed framework, we test the threshold consumption of CPU in MITM attack based on the percentage of CPU utilization in scenarios 1 and 2 illustrated in Figure 2. It shows that the CPU utilization of memory usage is less in a normal communication between the fog and the cloud environment [15-18]. This is as compared with the CPU usage when there is a MITM attack taking place. Figure 6 shows the results of an initial or preliminary experiment in the two scenarios depicted above. This implies that, the CPU usage can be used as a threshold value in detection of MITM attack in a Fog computing environment.

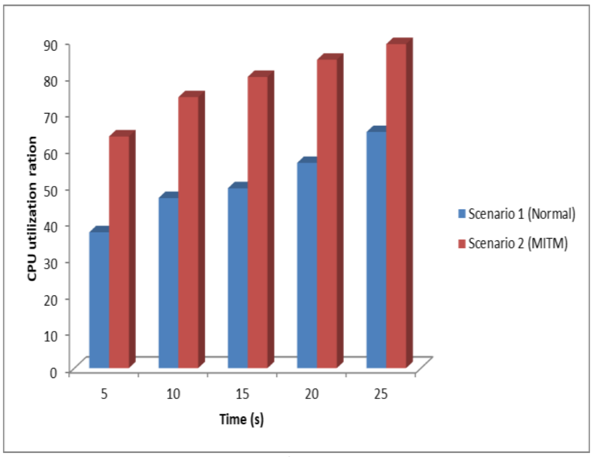


Figure 6. Initial results of CPU utilization with time

The DA detection model is expected to detect MITM attacks in fog computing environment. The introduction of DA algorithm in the proposed model would help significantly to detect MITM attack, as information moves from the cloud to fog environment and vice-versa without visible feature of the attack when collected from the fog. The experimental setup will be achieved through ifogsim simulator to determine the stealthy nature of Man-in-the middle attack.

VIII. FUTURE RESEARCH WORK

Future direction is to extend the DA algorithm to detect MITM attack at the edge of fog devices in fog computing environment. Traditional anomaly detection algorithms are not capable enough to expose MITM attack in fog to cloud scenario. Therefore, application of swarm intelligence optimization techniques using ifogsim simulator is expected to properly classify and detect the MITM attacks in fog devices.

IX. CONCLUSION

We have discussed the concept of fog computing paradigm and the security challenges. We observed that MITM attack remain security threat in fog computing environment as previous researcher's result shows insignificant effect. It is therefore difficult to detect MITM attack without visible feature of the attack when collected from the fog. This framework proposed the introduction of Dragonfly algorithm detection in MITM which it implementation through ifogsim simulator would help significantly to detect MITM, as information moves from the cloud to the fog environment and vice-versa. The DA is expected to detect any malicious attacker, whose intention is to intercept all relevant information that is moving from fog node to the cloud or cloud to the fog node and inject false information in fog computing environment. We recommend the extension of the DA to detect MITM attack at the edge of fog devices in fog computing environment.

REFERENCES

[1] J. Shropshire, "Extending the Cloud with Fog : Security Challenges & Opportunities," *Am. Conf. Inf. Syst.*, pp. 1–10, 2014.

[2] R. Rios, R. Roman, J. A. Onieva, and J. Lopez, "From SMOG to Fog: A security perspective," *2017 2nd Int. Conf. Fog Mob. Edge Comput. FMEC 2017*, pp. 56–61, 2017.

[3] I. Stojmenovic, S. Wen, X. Huang, and H. Luan, "An overview of Fog computing and its security issues," *Concurr. Comput. Pract. Exp.*, vol. February, no. April 2015, pp. 2991–3005, 2016.

[4] I. Stojmenovic and S. Wen, "The Fog Computing Paradigm: Scenarios and Security Issues," *Proc. 2014 Fed. Conf. Comput. Sci. Inf. Syst.*, vol. 2, pp. 1–8, 2014.

[5] Y. Sun, F. Lin, and N. Zhang, "Saudi Journal of Biological Sciences Original article A security mechanism based on evolutionary game in fog computing," *Saudi J. Biol. Sci.*, vol. 25, no. 2, pp. 237–241, 2018.

[6] Y. Guan, J. Shao, G. Wei, and M. Xie, "Data Security and Privacy in Fog Computing," *IEEE Netw.*, pp. 1–6, 2018.

[7] P. Kumar, N. Zaidi, and T. Choudhury, "Fog computing: Common security issues and proposed countermeasures," *Proc. 5th Int. Conf. Syst. Model. Adv. Res. Trends, SMART 2016*, pp. 311–315, 2017.

[8] J. Kang, R. Yu, X. Huang, Y. Zhang, and S. Member, "Privacy-Preserved Pseudonym Scheme for Fog Computing Supported Internet of Vehicles," *IEEE Trans. Intell. Transp. Syst.*, pp. 1–11, 2017.

[9] S. Khan, S. Parkinson, and Y. Qin, "Fog computing security : a review of current applications and security solutions," 2017.

[10] S. Mirjalili, "Dragonfly algorithm: a new meta-heuristic optimization technique for solving single-objective, discrete , and multi-objective problems," *Neural Comput. Appl.*, vol. 27, no. 4, pp. 1053–1073, 2016.

[11] SM Abdulhamid, Latiff MS, Chiroma H, Osho O, Abdul-Salaam G, Abubakar AI, Herawan T. A Review on Mobile SMS Spam Filtering Techniques. IEEE Access. 2017;5, pp. 15650-66.

[12] SH Madni, Latiff MS, Abdullahi M, Usman MJ. Performance comparison of heuristic algorithms for task scheduling in IaaS cloud computing environment. PloS one. 2017 May 3;12(5): e0176321.

[13] MS Latiff, Madni SH, Abdullahi M. Fault tolerance aware scheduling technique for cloud computing environment using dynamic clustering algorithm. Neural Computing and Applications. 2018 Jan 1;29(1), pp. 279-93.

[14] I. Idris, Abdulhamid SM. An improved AIS based e-mail classification technique for spam detection. arXiv preprint arXiv:1402.1242. 2014 Feb 6.

[15] SH Madni, Latiff MS, Coulibaly Y. Recent advancements in resource allocation techniques for cloud computing environment: a systematic review. Cluster Computing. 2017 Sep 1;20(3), pp. 2489-533.

[16] Abdullahi M, Ngadi MA. Symbiotic Organism Search optimization based task scheduling in cloud computing environment. Future Generation Computer Systems. 2016 Mar 1; 56:640-50.

[17] Latiff MS, Abdul-Salaam G, Madni SH. Secure scientific applications scheduling technique for cloud computing environment using global league championship algorithm. PloS one. 2016 Jul 6;11(7): e0158102.

[18] Latiff MS. A checkpointed league championship algorithm-based cloud scheduling scheme with secure fault tolerance responsiveness. Applied Soft Computing. 2017 Dec 1; 61:670-80.