Increased Security on Software Defined Network SDN to mitigate attack in Fog Environment Based on Using Artificial Intelligence

Asmaa M. Munshi[1] Afaf D. Althobiti Rabab M. Al Mohayawi

[1]Department of Cybersecurity Collage of Computer Science and Engineering
University of Jeddah, Saudi Arabia

Abstract

Fog computing is a decentralized cloud infrastructure provides an accurate solution to the trouble of data processing. The most important security requirement of fog technology is service and data availability. One of the most devastating cyber-attack is the Distributed Denial of Service attacks which are the most common and dangerous cyber-attacks, this type of security attack affecting the information integrity and service availability. This paper propose and focus on the development of fog cloud by conducting a contribution study on two different security mechanisms that is SDN with ANNs network algorithm as anomaly-based IDS via merged with a signature-based IDS detection to provide the maximum-security requirements and provide the required machine learning that well supports the fog to define and detect all upcoming and new issue cybersecurity. Moreover, provides the systems with the ability of automatic learning and improves the data and information experience process without being programmed.

Key words:

Fog, DDoS attack, Software defined network SDN, Artifice neural Network ANN, IDS

1. Introduction

Fog computing is a decentralized computing infrastructure. It provides a good solution to the data processing issue. It also allows access to data, storage and applications. It is located between the network and end devices. Fog consider to be the nearest to end point devices. Moreover, it's had the ability to reduce the applications latency [2]. Figure 1 illustrates Fog Computing Architecture.

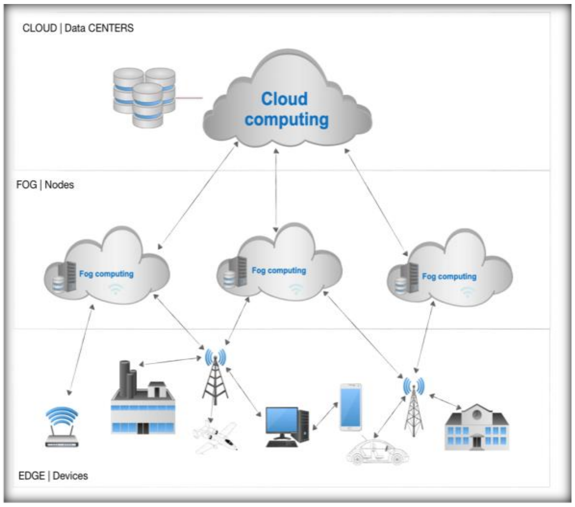

Fig. 1 Fog Computing Architecture

The most important security requirement of fog technology is service and data availability. Most attacks type such as Cyber-attacks can destroy this property. In recent years, DDoS attacks are rising popular and it constituted a large and significant type of attack on the cloud that proved extremely damaging the services. DDoS attacks refer to the techniques employed through hackers to make data unavailable to its owner [1]. In current years, researches have devoted its efforts in trying to protect systems against Cyber- attack and they have developed different methods by use Artificial Intelligence. Researchers suggested to use software defend network SDN in which the DDoS protector module is were used to defend against cyber- attacks. Further, gives DL based detection method which it proved successful in disclosure the denials of service infected packets and can disallow packet to be spread on the web cloud server [7]. On the other hand, others developed algorithm based on an allocated artificial neural network as anomaly-based intrusion detection system. It is merged with a signature-based IDS detection to discover cyber- attacks on a cloud platform [1].

Manuscript received January 5, 2020
Manuscript revised January 20, 2020

In this paper, we suggest building technical defense mechanism to define and analyze the attacks. The following contributions towards this research are:

1. Proposal of building defense against cyber-attacks applied on Fog layer.
2. Build a security mechanism to handle cyber-attacks by merge two methods mechanisms that is SDN with ANNs network algorithm as anomaly-based IDS via merged with a signature-based IDS detection.
3. Support and provide artificial based intelligence to detect new coming attacks. By using network traffic analysis mechanisms to filter and forwards the uninfected packets to the cloud and block the infected one.

2. Background

To complete the analysis and build a secure infrastructure for fog clouds in an attempt to address the largest number of attacks such as DDoS, hijack, shutdown, etc. that may infect the cloud and cause its work to be obstructed. By discussing several works and researcher investigations done to deduction and prevention this attacks issues by using artificial intelligence approaches and software defined network (SDN).

In [7], They installed SDN that called Software-defined network controller on fog cloud and employed on examine and filtered all the packages that came from the end users before passed to cloud services, If the packet is found to be the benign, it is transmitted to the cloud server. But if found any suspicious, then the IP address of the identical packet is transferred to the blocked listing of the table on the software-defined network controller. The fog server has already been trained with the deep learning algorithm. They used the DL algorithm and LSTM from other studies to create a solution for distributed denial of service mitigation which is especially tested in a fog and cloud environment. This model seemed to us by the percentage of 98.88% of accuracy on the testing data set.

In [5], SYN flooding attack, a common type of attack that causes a denial of service. The study showed that this type of attack sends a huge number of packets continuously during institute the connection via the triple handshaking procedure of a TCP protocol. The SYN flooding attack can penetrate and destroy the SDN controller, that lead to loss the functions for SDN. They found some techniques to detection and mitigation this attack by “using adaptive threshold algorithm (ATA) based on the Exponential Weighted Moving Average (EWMA) formula, which a simple modification it is made to signal alarm after a minimum number of consecutive violations of the threshold. In this way, they were able to improve educes the false negative rate from 6.15% to 0.59% and raise the accuracy from 94.3% to 99.47%” [5]. but this method is still considered difficult work on a network administrator. On the other hand [9], they are briefly discussed the most important challenges and issues that may adversely affect the performance of the software defend network (SDN) and that may have caused it to be stopped such as reliability, Scalability, and the attacks on the network like DDoS attacks. In [1], they have submitted a proposal on protecting cloud from attacks, especially DDOS attack due to its heavy impact, using artificial intelligence that depends on anomaly and signature-based detection. They keep track of the network traffic via compared the known attack with the behavioral study. This process is done by using signatures of attacks and matching it with the signature database of known detection of distributed denial of service attacks. If any unknown pattern is discovered. Accordingly, it will be used the anomaly detection distributed neural networks to discover the unknown distributed denial of service attack. Once its recognized, the signature of this attack will be improved. Also, to the signatures database will be refreshed. They have used (BigDL) library [10] on Apache Spark [11] and Suricata [12] as an open-source IDS to create a signature against, to try it their proposal. In this way, they were able to improve the accuracy of the results. This model appeared to them 99.98% accuracy, 98.15% of detection rate, and 0% of the false-positive rate.

3. Research Gap

We observed that the first study, cannot detect any new type of security attack because it relies on the trained data and information Stored in the database in advance. This indicative no early deduction of any new unknown attacks. Moreover, the studies of software-defined network still present many procedural and operational challenges [4]. Due to the presence of threats of other attack types on Software-defined network Controller [9], such as virus designated specifically to avoid and stop this Software like hijack, shutdown, or corrupt software-defined network controllers, also, the impact such a virus could have on a network. These attacks make us unable to rely entirely solely on this service. As we mentioned earlier, the most important security requirements of fog computing are making it always available to provide service. So, we need to add more security layers to make sure if any attack occurs on this system, there will have an alternative to detect the defect and address it. In order of this, we suggest implementing a new security layer to provide information and data security from all possible cyber-attacks and ensure the security requirement by providing the data and resources integrity and availability.

4. Recommend Sulution

We proposed to build a defense mechanism to deduct the distributed denial of service attack by merge two methods running in a fog cloud. We assume that this tow suggested mechanism well provide the best security result. See Figure 2.

First, behavioral comparison is applied to network from the end user devises. When a network traffic sent request into fog cloud, protection system turned on and a comparison procedural start to analyze and compare the traffic behavior, with pre-defended traffic behavior (known and unknown attack signatures) based on behavioral matching procedural of the signatures IDs detection database for each known attack if matching is found then this request should be automatically retransmitted to block list server and it well prohibited from accessing the fog services finally, alert well be sent and no request will be processed. At the end signatures IDs detection database well be updated.

Second procedural is related to unknown traffic pattern. It will be redirected to an anomaly IDs detection that uses two detectors Anomaly and Signature based Detector, data training procedural well start the process of define and analyses the packet based on ANN parameters and technique; we have explained how to use it in the second section. Once an unknown attack is discovered, then the signature of this attack will be developed, and the database will be updated [1]. After that, the attack is relayed on the prevention zone which is the block list server.

The last type is the normal traffic patterns that will pass after behavioral study finish matching and comparing of the analyzed request. Packet well redirected to the software-defined network controller as a last defense line on the fog cloud. The parameter structure of the SDN provides other layer of protection in order to increases the required security. Software-defined network supports extra inspection to support the confidentiality and integrity of the package by performing a deep learning algorithm and events correlation. If it has a suspicious behavioral, then the IP address of this packet will be added to the IP block list in the switch table of the Software-defined network controller. Then data and information on switch table well be sent to block list server for enhancement of the future inspection and data correlation. Finally, all packets found benign are allowed to pass the cloud.

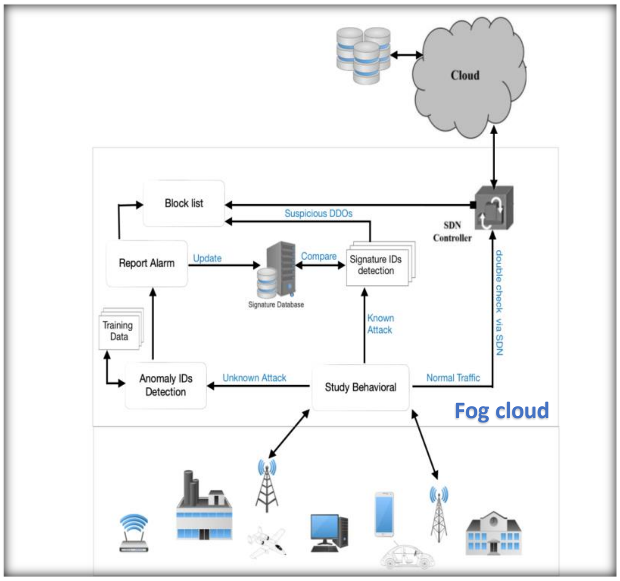

Fig. 2 proposed system on fog computing

5. Conclusion&Future Work

This paper presents deep learning-based model to protect a fog computing from cyber-attacks. We increased security layers on fog cloud by using software defined network technology to control fog with ANN which includes anomaly detection algorithms and signature-based detection. The proposed could provide a high level of protection to detect Denial of Service attacks and similar attacks on Fog cloud. In order to implement this proposal and obtain realistic results, we suggest using and implementing the following requirements which will help in turn to run the procedural carefully and step by step to ensure the maximum-security roles. We need to study fog Computing architecture [6] and the correct ways to connect the Software-defined Network (SDN) with an intrusion detection system in order to achieve the desired goal.

Finally, we have to declare that, it will be some obstacle to the implementation and running regarding the proposed solution. we Inability to determine the time required to train these software's on different types of attacks and it improved its ability to detect and prevent attacks as well as alert

Acknowledgments

We would like to thank Dr. Asmaa Munshi, Assistance professor of Information Systems at Faculty of Computing and Information Technology at King Abdul-Aziz University. for her support and assistance in this research.

References

[1] Alzahrani, S. & Hong, L., 2018. Detection of Distributed Denial of Service (DDoS) Attacks Using Artificial Intelligence on Cloud. 2018 IEEE World Congress on Services (SERVICES).

[2] Buyya, R. & Dastjerdi, A. V., 2016. Internet of Things: Principles and Paradigms. 1 ed. s.l.:s.n.

[3] Cepheli, Ö., Büyükçorak, S. & Karabulut Kurt, G., 2016. Hybrid Intrusion Detection System for DDoS Attacks. Journal of Electrical and Computer Engineering, Volume 2016, pp. 1-8.

[4] Cox, J. H. et al., 2017. Advancing Software-Defined Networks: A Survey. IEEE Access, Volume 5, pp. 25487-25526.

[5] Htein Maw, A. & Oo, N. H., 2019. Effective Detection and Mitigation of SYN Flooding Attack in SDN. International Symposium on Communications and Information Technologies (ISCIT).

[6] Liu, Y., Fieldsend, J. E. & Min, G., 2017. A Framework of Fog Computing: Architecture, Challenges, and Optimization. IEEE Access, Volume 5, pp. 25445-25454.

[7] Priyadarshini, R. & Barik, R. K., 2018. A deep learning based intelligent framework to mitigate DDoS attack in fog environment.. Journal of King Saud University - Computer and Information Sciences.

[8] Priyadarshini, R. & Barik, R. K., 2019. A deep learning based intelligent framework to mitigate DDoS attack in fog environment. Journal of King Saud University - Computer and Information Sciences, pp. 859-868.

[9] Rana, D. S., Dhondiyal, S. A. & Chamoli, S. K., 2019. Software Defined Networking (SDN) Challenges, issues and Solution. International Journal of Computer Sciences and Engineering, 7(1), pp. 884-889.

[10] Sergey E., 2018. BigDL: Distributed Deep Learning on Apache Spark*. [Online] Available at: Software.intel.com [Accessed 26 11 2019].

[11] Spark.apache, 2018. Apache Spark™ - Unified Analytics Engine for Big Data. [Online] Available at: https://spark.apache.org [Accessed 26 11 2019].

[12] Suricata, 2018. Suricata. [Online] Available at: https://suricata-ids.org [Accessed 26 11 2019].