International Journal of Future Generation Communication and Networking
Vol. 13, No. 4, (2020), pp. 4161–4173

Fog-based SDN for DDOS Attack Mitigation in IoT Systems: A Survey

D.Kavitha[1] and R. Ramalakshmi[2*]

[1]Department of Electronics and Communication Engineering, Kalasalingam Academy of Research and Education, Anand Nagar, Krishnankoil, Tamil Nadu 626126, India
[2]Department of Computer Science and Engineering,Kalasalingam Academy of Research and Education, Anand Nagar, Krishnankoil, Tamil Nadu 626126, India

Abstract.

Distributed Denial-of-Service (DDoS) attacks constitute a severe threat to academia and industry, with unfettered access by end-users to resources from cloud data center services. DDoS attacks, discussed and resolved with varying degrees of success by researchers in the recent past, have been detected and mitigated successfully in SDN environments. Given the rapid rise of edge devices like sensors, cloud storage access has become a serious concern, with fog computing stepping in to play a major role in sharing such resources as links between the cloud and edge computing devices. The fog is the middle layer of cloud and edge devices. This paper deals with DDoS attack detection and mitigation approaches between IoT devices and a cloud server via an SDN controller in a fog layer. It also discusses the roles and responsibilities of fog computing in an SDN-based testbed, as well as the challenges involved in DDoS attack detection using a fog- based SDN to protect the cloud server from edge devices.

Keywords: *DDoS, SDN controller, Cloud, Fog computing*

1 Introduction

The Internet of Things (IoT) connects all available devices to provide secure services for entire applications. The IoT can be defined as "a pervasive and ubiquitous network that incorporates monitoring and controlling of the physical environment by collecting, processing, and analyzing the data created by sensors or smart objects." In industrial surroundings, it is termed the Industrial Internet of Things (IIoT), where industrial devices like controllers, sensors, processors, actuators, and all related types of equipment are connected, and the intelligence at hand raised with the combined use of other devices. IIoT systems are susceptible to distributed denial-of-service (DDoS) attacks, as a massive number of electronic devices with little computation power are distributed in vast locations with little security.

Such components are unprotected in a DDoS attack, which exploits devices to seize network resources for its normal operations. However, a DDoS attack is a significant example of an attacker successfully flouting the system [28].Fog computing is being projected as a new computing prototype for the cloud, working in the same fashion as the cloud, though not centralized like it. Fog systems undertake local data investigations on edge nodes. DDoS attacks destroy a target client's available resources. Nevertheless, certain SDN characteristics help detect and safeguard both cloud and fog environments against DDoS attacks. The presence of a centralized SDN controller maximizes the chances of DDoS attacks on the controller to leverage the cloud to the fog [23].

At the Open Fog Consortium, a preliminary approach such as the Fog-to-Cloud (F2C) has been recently proposed for a coordinated fog-cloud framework to offer the IoT benefits in terms of management and service allocation, among others. However, F2C deployment has a few security and privacy-related challenges and demands strong security mechanisms in place in both the cloud and the fog, with help from SDNs. Another key issue in the cloud is ensuring that data storage is not drained by external or internal attackers. Owing to huge storage processing requirements, security mechanisms for FC cannot fully be applied to the cloud. Besides, the gap between end-users and the cloud has cre-

ISSN: 2233-7857 IJFGCN

ated weaknesses in the form of data breaches, data loss, and denial-of-service attacks. This, therefore, calls for a new and coordinated F2C architecture that can effectively handle cloud and F2C security issues. This paper proposes a novel, secure set of SDN-based distributed controllers for F2C distributed systems as middleware [14].

Today, a major drawback of the IoT is the inadequate defense and vulnerability of metadata systems, owing to which hackers generate botnets and DDoS attacks against a third party with consummate ease. Consequently, improvements in industrial security service and the entire ICT ecosystem are called for. HP and Gamer predicted that by 2020, almost 60% of around 26 billion IoT-based components would be insecure and susceptible to DDoS attacks, including highly-protected networks. Merely mitigating DDoS attacks is simply not adequate for today's large-scale IoT heterogeneous networks, though SDNs play a vital role in resolving IoT-based DDoS attacks using fog computing. This paper proposes an FC approach with an SDN controller in edge IoT networks that are capable of detecting IoT-based DDoS attacks[21].

The rest of this paper is organized as follows. Fog computing and cloud-based research and questions are discussed in Section II. Section III explores fog computing and IoT-based problems. Section IV deals with FOG-SDN-IoT concerns, while Section V discusses FOG-SDN-DDoS and IoT-based topics. Finally, Section VI concludes the paper.

1.1 Motivation

In recent times, [25], [15] several studies have been carried out on the IoT by both academia and industry in medicine, agriculture, and government sectors, as well as the huge mass of information in the public domain. The focus of ongoing technology and research is on managing all the sensor data produced worldwide so it can be effectively stored in a cloud database via the IoT and assorted edge computing devices[19], [5], [26]. This calls for a deep analysis of security aspects such as malicious attacks from end devices to the cloud database[27].

This study discusses related surveys on all aspects of security in the IoT using the SDN and fog environments, based on machine learning techniques and tools like the iFogsim[10] and Mininet [22]. Finally, this review offers insights into possible challenges, examines existing reviews, and presents new research guidelines.

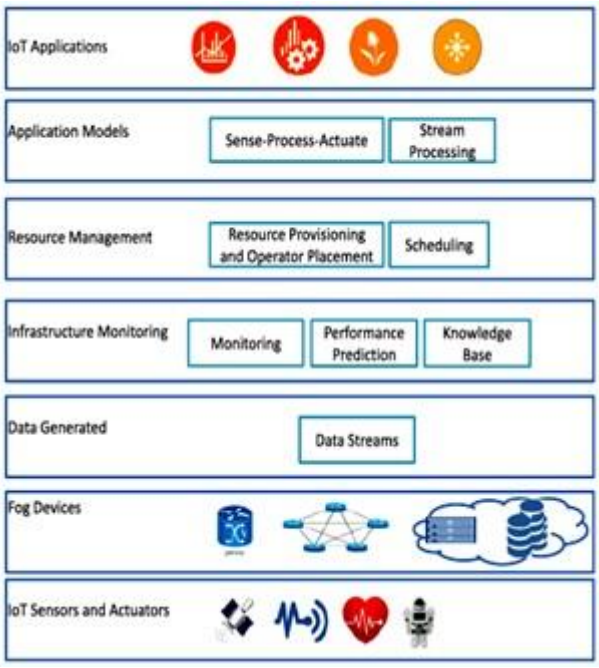

Fig. Error! No sequence specified.. Fog computing architecture

ISSN: 2233-7857 IJFGCN

2 Cloud with Fog Computing

Section II discusses how fog computing evolved from cloud computing in the last few years. Fig.1 and 2 depicted the basic architecture of the end user-fog-cloud architecture with bottom, middle, and top layers [18].

Firdhous et al. (2014)[9] discussed the basics of fog computing issues stemming from cloud computing. FC developed as a result of problems in existing cloud and sensor networks in terms of latency, security, and processing speed. Fog computing, which is carried out by cloud computing, is centered around the region near the end-user network, or just above it, or very close to the edge of the cloud network.

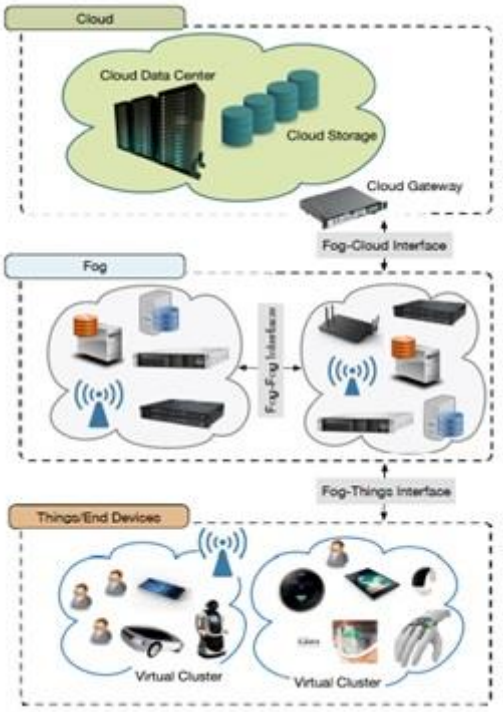

Fig. Error! No sequence specified.**.** Fog basic architecture

"Fog computing" was introduced by Cisco Systems for easy data communication and data transfer to distributed components in the Internet of Things (IoT) network model. FC is a virtualized, programmed platform for all end-user devices and cloud data storage centers within the Internet. The prime feature of fog computing is its ability to support low latency, location awareness, and mobility. FC-distributed nodes must have adequate computing and storage facilities, like power and capacity, to handle user requests.

It also overrides cloud computing restrictions to include cloudlets and edge computing. Cloudlets (fog nodes) are rich clusters that provide mobile users services backed by strong Internet connectivity Cloudlets eliminate all of the cloud's drawbacks and have applications in security and distributed load balancing; resource management and accounting; billing and testing and are also less prone to DOS attacks.

That's Jalali et al. (2015)[12] discussed energy savings in the cloud-based fog. They used centralized servers as data centers (DCs), and intermediate fog nodes or small servers as Nano data centers (nDCs). Energy consumption is based on the number of hops between end-users and data servers. Additionally, the total energy consumed includes the types of applications running on the nDCs, such as

ISSN: 2233-7857 IJFGCN

the aggregate number of downloads, copies, and updates. Energy consumption in the network is described by two models, *flow-based* and *time-based.*

In the flow-based model, energy consumption is calculated based on the proportional rate of allocation of power in all equipment flows in the network. The power consumed includes both idle and active component power.

In the time-based energy consumption model, energy is calculated based on the time taken for end-users as well as all the equipment, including nano servers, to access their service.

Deng et al. (2016) [7] proposed optimal workload allocation using fog computing. FC or edge computing supplies cloud data to mobile end users. FC acts as a middle layer, pre-storing cloud data, and allocating it between the cloud and mobile users with minimal power consumption and delay. The optimal workload allocation problem is divided into three subproblems using modern computational alternatives that save communication bandwidth, reduce delay, and improve cloud performance. Using existing optimization techniques, the primary problem (PP) is split into three subproblems (SP). SP1 is considered the replacement between delay and power consumption in a fog computing subsystem. SP2 is considered the replacement between delay and power consumption in a cloud subsystem.

Finally, based on the above-mentioned results, the overall communication delay, which is SP3, is calculated. The three decomposition problems are resolved using the Generalized Benders Decomposition (GBD) algorithm. Finally, the paper suggests that when the fog tasking load is low, fog power consumption and delay are correspondingly low, owing to the fog-cloud computing system. The researchers used optimization techniques in a centralized model.

VM migration concepts in fog and cloud computing were explored by Osanaiye et al. (2016) [20]. Virtualization is progressive technology in fog and cloud computing that coexists with the physical layer to share resources. Since VMs are also susceptible to malicious attacks in the physical layer, a smart pre-copy live migration method that minimizes system downtime for fog computing end users is projected for VM migration.

The paper discusses the smart pre-copy approach, estimates the downtime after repetition, and determines whether the data in the fog layer is to be stopped or copied, using virtualization to access cloud resources. The paper concludes that fog computing can be extended to include DDoS and green computing as well. The sample review papers above have dealt with the basic research on fog computing in the recent past.

3 Fog Computing with IoT

Section III of this paper elaborates on research in fog computing with the IoT. The Internet of Things has applications in health, learning, agriculture, food, green energy, emergencies, smart homes, the automotive industry, disaster management, aerospace, tourism, and telecommunications.

The combined cloud and IoT is termed the Cloud of Things (CoT). The rapid development of all end-user devices challenges real-time processing and its applications[27].

To address these challenges, diverse middleware technologies like mobile edge computing and the cloudlet have emerged. The fog plays a vital role in bringing together IoT end-users and cloud computing.

That's Elazhary (2018)[29] discussed IoT and research issues in fog computing, reviewing IoT use and its applications in all sorts of computing, including mobile, cloud, and pervasive depicted in Fig.3.

ISSN: 2233-7857 IJFGCN

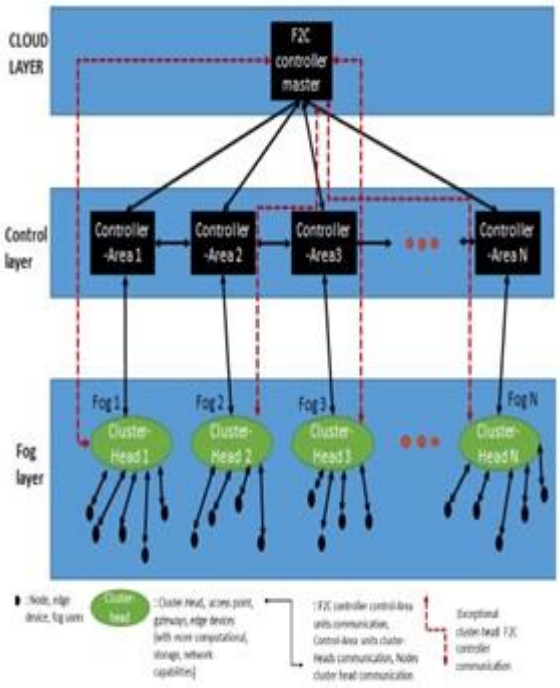

Fig. Error! No sequence specified..SDN-based F2C architecture

That's Mutlag et al. (2018)[30] advanced the use of fog in health care IoT systems. The paper considered health care data and simulated the use of fog computing as a middle layer to provide low latency, better security, fault tolerance, and scalability. Chiefly, it focused on shared resources from other review articles and asserts that fog computing reduces latency better than cloud computing in health care systems. Resource management and latency in health care systems are managed by computation overloading and load balancing.

Aazam et al [1] discussed offloading technologies in fog computing for the IoT. All online applications have computation communication and intelligent capabilities. Offloading is a technique to execute tasks and return results for all applications with IoT nodes, sensors, and fog edge devices. Offloading incorporates load balancing as well as energy and latency management. The contributions of the paper, chiefly, include measures for offloading in a fog environment, IoT middleware methodologies, and applications.

The paper used the offloading criteria of excessive computation, latency requirements, and long-term storage. IoT middleware technologies include the cloudlet, mobile edge computing, micro data centers, nano data centers, delay-tolerant networks, and the Femto cloud. iFogsim, a tool to implement fog computing technologies, acts as a gateway between IoT edge devices and the cloud database in terms of energy consumption. It uses the fog middle layer and analyzes the number of devices and their characteristics for reduced power consumption[10]. The IoT and fog computing have applications in industry and real life, as indicated by the research above.

4 Fog - SDN for IoT Systems

Kahvazadeh et al.[14] discussed a combination of the Fog to Cloud through SDN approaches. The future IoT is a comprehensive combination of cloud and edge resources shown in Fig.4. Their paper also used an SDN-based centralized controller on the upper end of the cloud and distributed controllers on the edge of the network. The method reduces the distance between the cloud and its users and offers security by reducing the number of man-in-the-middle attacks. This work has an SDN

ISSN: 2233-7857 IJFGCN

control layer situated above the fog layer. Fog to Cloud communication reduces authentication-related security issues, as also the delay between the cloud and end-users.

Bendouda et al. (2017)[4] proposed an SDN-based IoT network approach. They used SDN functionalities in the IoT using connected dominating sets (CDS). To deal with a single point of failure (SPOF) in the centralized controller, levels of control are put in place, as with a principal controller (PC), a secondary controller (SC), and a local controller (LC). Their architecture considered the following five SDN-based modules: control; data; cloud and fog; security and privacy, and, finally, end-users themselves. The paper demonstrates that the DLC-CDS algorithm outperforms the DSP-CDS algorithm concerning high performance in network size and density.

The paper used MATLAB and fuzzy logic approach-based, energy-efficient concepts in SDN–FOG computing using vehicular networks. Today, with the rapid rise in vehicle population and communication networks, vehicular networks need effective routing protocols for unicast, multicast, broadcast, and miscellaneous communication transmission modes. A simulation was undertaken with 49 nodes and a gateway node for its implementation.

Kadhim et al. (2018) [13] presented an energy-efficient multicast routing protocol based on the SDN network and fog computing for vehicular networks. It primarily considers bandwidth and quality of service with a priority scheduling algorithm and a classification algorithm.

The studies above have discussed IoT-based research, ranging from the fog and SDNs to cloud computing, with a focus on the computational delay, security, and area complexity of IoT devices in SDN-based fog computing networks.

5 DDoS Attack Detection and Mitigation in IoT Systems

Section V discusses the DDoS attacks in fog computing. Denial-of-service attacks may be generated and forwarded from edge nodes (IoT devices, all sensor nodes, and mobile phones) to cloud resources. The data is entered into the fog module for pre-processing before it reaches the cloud, where it can be accessed. Pre-processing includes segregating and filtering irrelevant data, followed by a quick selection of the appropriate data that can be accessed from the cloud server with reduced complexity. As a result of frequent network congestion and denial-of-service attacks, an additional security layer above the fog, termed the SDN, is developed. Thus, the SDN-based fog offers secure data transmission, commencing from the nodes at the end to the cloud resources at the center, utilizing a reduced number of malicious attacks.

Deepali and Bhushan(2017)[6]discussed security against DDoS attacks using fog computing. Attack data is generated from the network's edge nodes and forwarded to the cloud DB. The attack data unit passes through the fog defender module, which applies the rule and detects DDoS attack traffic targeted at resources in the cloud. For the experimentation, the paper used the Kali Linux and VMware tools for the fog module traffic capturing process.

The attack is generated and processed via three different tools, Metasploit, Ettercap, and LOIC. Since the packets are blocked by the fog defender after the DDoS attack is identified, the overall cloud performance shows improvements with better resource use and a quicker response time.

Priyadarshini et al. (2018) [23] proposed DDoS attack mitigation in a fog-based environment using an SDN Controller with a deep learning method. They proposed a novel source-based DDoS defense mechanism where the SDN controller is deployed in the fog to detect anomalous behavior in the network.

A deep learning-based attack detection technique to filter and forward data to the server is proposed. Both benign and malignant packets are transferred from the client's side or edge devices. The packets of data are transmitted to the cloud server via the fog layer. The SDN centralized controller in the fog layer captures incoming traffic and ascertains if the packet is legitimate or malicious. Malicious packets are transmitted by assorted scripts and tools. A packet that is identified as malicious has the corresponding packet's IP address sent to the controller.

ISSN: 2233-7857 IJFGCN

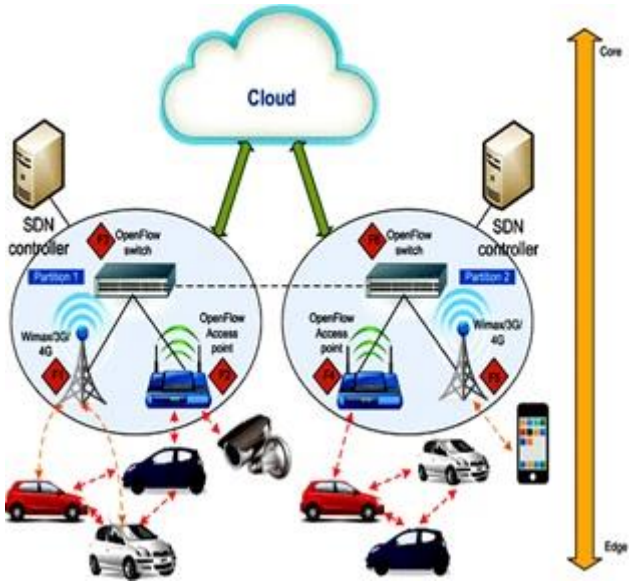

Fig. 4. A sample smart city with multiple SDNcontroller-based secure fog architecture

The controller takes action, based on the ruleset, and the packet is shifted to the block list to prevent access to the cloud server. The fog layer has multiple VMs, each of which can send both normal and attacked packets within a stipulated period, t, built on the SDN architecture.

The SDN controller forwards or drops packets, based on a packet's characteristics. The packets are passed on to the SDN-based deep learning detector module that is already pre-trained with existing or ancient data and has learned to differentiate between DDoS-infected or normal packets.

Based on the collected features, the detector module drops or forwards packets to the cloud server. The following simulation setup is used in this work: packet capturing is done by the HPing-3, Apache web server for own Cloud, MySQL database, Mininet emulator, Floodlight controller, and the deep learning Python library, Keras, on a Tensor Flow background. The experimental setup has shown 98.88% accuracy in terms of the protection offered by the SDN controller to the fog layer from a DDoS attack on a cloud server.

Distributed deep learning-oriented attack detection in a fog computing environment was proposed by That's Diro and Naveen (2018)[2]. Machine learning-based attack detection was a huge success in the past, though the massive growth of IoT devices has resulted in a proliferation of attacks, calling for an efficient deep learning-based attack detection method.

Their paper proposed a distributed deep learning method that detects malicious packets from edge IoT devices in the fog layer to protect the cloud server. Their work considers multiple fog nodes and the NSL-KDD dataset and produced better accuracy, detection, false alarm rate, and scalability. The researchers conclude that attack detection can be carried out on different datasets.

Ozceliketal. (2017)[21] proposed an IoT-based DDoS attack defense in the SDN environment. Their study dealt with security against DDoS attacks in a mass of IoT-connected devices affected by a botnet called Mirai. They proposed DDoS mitigation in four phases involving a packet handler, a flow handler, a synqueue updater, and a detection unit. Their work explored attack detection and mitigation by the SDN and fog computing for IoT networks.

That's Imran et al. (2018)[11] discussed the results of denial-of-service attacks in software-defined networks. SDNs have key features like scalability, flexibility, and monitoring, and yet are susceptible to flooding, spoofing, and denial-of-service attacks.

ISSN: 2233-7857 IJFGCN

The paper showcases the different types and classes of mitigation approaches and the methodologies of attack packets. Based on the methodologies, malicious traffic is classified into three: blocking, delaying, and resource management. In the blocking approach, when a malicious packet arrives, the controller blocks or drops it. In the delaying approach, the detection system does not directly block the malicious packet; instead, the unwelcome traffic is assigned a low priority or low trust values. The paper recommends SDNs for their security and reliability, with fewer control messages between the controller and of switches for decreased congestion.

That's Zhou et al. (2018) proposed a DDoS attack on all edge-side IoT devices as a result of a large number of low-power devices. They applied a firewall-based mitigation process and virtualized network activity in a local server. Their work used an industrial control system real-time experimental setup and evaluated detection time and DDoS attack rates. Their fog computing-oriented DDoS mitigation the approach uses the SCADA system with three levels of architecture: i) packet filtering based on Rule 2, ii) DDoS detection schemes based on specifications, and iii) a central consolidation analysis.

All three methods detect anomalous behavior by the network via the fog layer using the firewall implementation process. The work simulates the DDoS detection module in two steps: firstly, with an edge firewall scheme using a Linux-based environment and, secondly, with a virtualized process-based DDoS detection module. The paper compared the distributed DDoS mitigation process with and without the fog computing approach.

Sohal et al. (2016) [24] discussed malicious edge detection and cybersecurity issues using fog computing. Device security implementation is a huge challenge in an IoT-based fog computing environment. Fog computing has networking components like a router, switches, and hubs for processing and collecting data using the IoT. The paper explored a cybersecurity framework to detect malicious edge devices. The framework is classified into 3 types: the Markov system, an intrusion detection system(IDS), and a virtual honeypot unit device (VHD). Their work used a 2-stage Markov model to effectively categorize end nodes, as well as a virtual environment to reduce the false IDS alarm ratio and identify malicious devices using OpenStack and Microsoft Azure. Their work describes Markov models, and their various stages, at length. A Markov model predicts future outcomes based on the system's present outcomes. Another model, called the hidden Markov model, is capable of predicting the subsequent state of the system as well as a hidden state that is infeasible in the standard Markov model. These two stages of the Markov model analyze the attack generated in edge devices by an IDS alarm.

A traditional IDS produces plenty of false alarms because all IoT devices send multiple dimensions of data to edge devices for computation. So, to diminish the false alarm rate, the proposed 2-stage Markov structure framework is used to identify malicious attacks. Two-stage models work in two steps to detect malicious devices. Firstly, the edge device is classified with the support of the shifting probability (SP) and thereafter sent to the second stage, which is the hidden Markov framework. Here, edge nodes are shifted to a VHD that is not based on the SP and the type of attack.

The working framework of the proposed cybersecurity approach is classified into 4 edge device-based categories: legitimate devices (LD), sensitive devices (SD), under-attack devices (UD), and hacked devices (HD). Legitimate devices are privileged to access the system without a security breach, while sensitive devices are to be monitored carefully since they could be hacked and so end up sending false data. Under-attack devices are besieged by expert attackers and impact the entire system, while hacked devices are edge devices that are attacked by hackers and send continuous false alarms to the system. False alarms are to be eradicated from legitimate devices and shifted to a VHD.

In the proposed cybersecurity framework, security services are provided by the secure load balancing (SLB) option placed in the fog layer under a continuous IDS. When an attack is detected by

ISSN: 2233-7857 IJFGCN

the IDS, alarms are generated and processed by the 2-stage Markov process. Based on the detection phase, the alarms raised are shifted to a VHD and the log files generated are saved in the repository to prevent future attacks. The cyber framework constitutes the following 4 phases: an intrusion detection unit, an adaptive unit, an activity unit, and a VHD unit. It is anticipated that this work will be extended to include effective VHD implementation in the future.

That's Alharbi et al. (2017) [3] discussed security implementation against traditional cyberattack techniques. They deployed security appliances like a firewall and a load balancer to defend against DDoS attacks created by the high volume of traffic and limited hardware capacity. This work introduced a framework using the NFV and edge computing to mitigate attacks with a 2-stage process: a screening mechanism and resource allocation. In the screening method, packets are classified as normal or malicious, based on the service type, attack type, and VNF. In the resource allocation method, the resources for the VNF/VSF function are allocated, depending on on-demand services and availability.

That's Modarresi et al. (2017) [17] discussed the importance of fog and edge computing approaches in handling all IIoT-related traffic to facilitate the rapid processing of huge volumes of traffic headed towards the cloud. Further, fog computing efficiently manages, stores, and communicates near the bottom of the edge network, reducing delay and bypassing network traffic to access the cloud server. The work considered security and scalability while adding extra fog nodes without compromising on performance and response time, and autonomy in facing external disaster-oriented challenges by blocking malicious traffic with local decision making.

The paper also discusses the framework design using the SDN deployed above the virtual layer, with virtual machines connected to the SDN control layer. Sniffer packets are detected every second, using an SDN-based fog environment alongside an intrusion prevention system. The experiment tested detection applications for both normal and malicious packets using the SDN in the fog. The work concludes with extensions that consider machine learning techniques in the future.

Diro et al. (2017) [8] explored deep learning-based distributed attack detection in the Internet of Things. Their work compared distributed deep learning and traditional machine learning approaches and infers that the deep learning model outclasses the rest of ineffective attack detection. Their work used a distributed and parallel-based intrusion detection scheme in fog computing. The NSL-KDD dataset was used for validation and evaluation, and the experimental process considered both normal and attack datasets. The parameters used were accuracy, false alarm rate, and detection rate between the deep and shallow approaches.

Krishnan et al. (2018) [16] dealt with a secure IoT environment with an SDN framework and explored the security aspects of IoT devices with an SDN/NFV-based implementation process. The process works in heterogeneous networks with IoT devices and evaluates key SDN and IoT network features such as security, latency, load balancing, and programmability in huge IoT networks.

Three design criteria are applied: loosely-coupled, tightly-coupled, and global cloud configurations. It handles DDoS HTTP Botnet attacks on an SDN-based IoT and analyzes its performance against attack traffic and normal traffic flowing through the SDN switch per second. The improved performance of DDoS mitigation via the SDN–IoT network using the OpenFlow protocol has been recorded and proved.

The sample articles above explored a range of SDN-DDoS issues in the fog computing environment. However, much more research is needed on the topic of security, especially as it pertains to fog computing. The literature has highlighted certain aspects for a better understanding of the DDoS attack detection scheme using the fog between the IoT and the cloud.

ISSN: 2233-7857 IJFGCN

6 Challenges, Reviews, and Research Opportunities

Based on a scrutiny of the review papers above, this work has identified certain limitations and challenges in the research on fog-related IoT, SDN, and DDoS environments, which are presented below in Tables 1, 2, and 3.

Table Error! No sequence specified.. A Summary of Future Research direction and their Challenges in SDN based Fog attack detection

S.No	Challenges	Description	Focus/ Objectives	Contributions of the articles reviewed	Future opportunities
1	A practical implementation of fog-based SDN DDoS attack mitigation	Mitigation of distributed denial-of-service attacks, via SDN-based fog computing to the cloud, from edge users to protect cloud access	• To implement distributed local servers and centralized coordination • To use real-time traffic filtering via firewalls • To cut the distance between cloud users • To strengthen edge-oriented detection and mitigation • To use the network function virtualization technique for traffic filtering	A DDoS mitigation process using a fog-based approach in IIoT systems with SDN controllers [1], [2], [3], [4], [5], [23], [25], [27], [28], [29], [30]	• To offer improvements with more real-time application data • To concentrate further on accurate security • To focus on load balancing and real-time decision making • To reduce the number of control messages between the switches and the controller • To develop a new screening mechanism and resource allocation algorithm for DDoS attack detection

S. No	Challenges	Description	Focus/ Objectives	Contributions of the articles reviewed	Future opportunities
1	Security implementation, only in fog computing	A discussion and provision of security in the fog Cloud of Things (CoT) without the concept of SDNs	• To implement distributed fog nodes for effective local preprocessing • To implement ML-based intrusion detection using the fog for IoT data • To identify malicious attacks using a 2-stage hidden Markov model	Dealing with security issues in fog computing and IoT systems [6], [9], [8], [10], [13], [14], [18], [24], [26]	• To apply new and different techniques for effective fog processing • To reconsider fog node placements, latency, delay, and power consumption • To enhance performance using different datasets and neural networks
2	Security and QoS	Complexity and failure at the controller node, stemming from an increasing number of nodes and controllers	To reduce traffic by distributing controllers among the primary, secondary, and local levels. The resultant connected dominant set evaluates node density and range to minimize link failures	Programmable architecture based on the SDN for an IoT-CDS approach [21]	To concentrate on additional parameters for improved QoS

Table Error! No sequence specified.. A Summary of Future Research direction and their Challenges in Fog based security and QoS

S. No	Challenges	Description	Focus/ Objectives	Contributions of the articles reviewed	Future opportunities
1	Energy and power consumption	Increased energy in all layers, stemming from a large number of computing devices shifting from the edge to the cloud	To design a system with the most nano distributed centres (nDCs) connected to a centralized data enter (DC) to consume the least energy, based on the proportional value of idle and active time	Fog computing energy savings in the cloud [14], [16], [21]	To improve energy efficiency in IoT devices, and for home end users. with nano server implementation

ISSN: 2233-7857 IJFGCN

			To calculate the downtime after each iteration to determine whether to proceed, or stop to minimize the downtime		To promote green computing
2	Optimal workload allocation in the fog-cloud	The need for mobile users to be able to find a service providing equal distribution with minimal power and delays	To allocate work between the fog and the cloud by decomposing problems into subproblems for reduced power consumption, delay, and bandwidth use	An optimal fog-cloud workload allocation with balanced delays and minimal power consumption [15], [19]	To improve optimization from a centralized controller in a distributed manner
3	The multicast routing complexity problem	Problems with routing, brought on by the prevalence of large numbers of vehicles, resulting in time complexity and overhead	To use priority-based and classification-based scheduling algorithms to minimize multicast routing problems	Energy efficiency for vehicle routing, based on SDN and fog networks [21]	To improve routing efficiency with routing algorithms and scheduling for the reduced delay, power, and time complexity

Table Error! No sequence specified.**.** A Summary of Future Research direction and their Challenges in Fog based Energy and optimization issue

7. Conclusion

Fog computing is an emerging, powerful virtualized framework model, and not merely a substitute for cloud computing. This paper has presented a comprehensive background to fog computing, fog with the IoT, SDN with fog, and, finally, SDN with security against malicious attacks, especially DDoS attacks. Fog computing provides intermediate storage and maximizes efficiency between edge components and cloud services. With its distributed methodology, fog computing improves security and trust between edge devices and the cloud. It motivates researchers to identify new methods and offer fresh solutions to problems. Fog computing presents quick solutions in sensor- oriented industrial applications and managing health care data in a highly secure environment. The fog provides better-distributed detection results than other existing methods, given the huge mass of IoT- oriented data to be handled. Further, it efficiently resolves big data-oriented problems from IoT and sensor devices. This survey has focused on fog computing with SDNs and security in cloud services and presents efficient solutions to thwart DDoS attacks in the cloud in fog-based SDNs. The SDN controller is placed in the fog layer, which may be centralized or distributed, based on the network framework. Thus, though the fog-based SDN provides an array of secure solutions, based on the survey above, it needs more work on intrusions of all sorts and malicious attacks. Given today's huge data growth from all IoT edge devices to the cloud, the fog provides the best solutions of all. Further, SDNs adequately support the fog layer, or nodes, through detecting and providing security against all edge-related malicious inputs. This survey has examined, from the existing literature, the security-related aspects of fog computing as well as several multifarious techniques that offer promising solutions, both of which have applications in future research.

REFERENCES

1. Aazam, M. et al.: Offloading in fog computing for IoT: Review, enabling technologies, and research opportunities. Future Generation Computer Systems. 87, 278–289 (2018). https://doi.org/10.1016/j.future.2018.04.057.
1. Abeshu, A., Chilamkurti, N.: Deep learning: the frontier for distributed attack detection in fog-to-things computing. IEEE Communications Magazine. 56, 2, 169–175 (2018).
2. Alharbi, T. et al.: Holistic DDoS mitigation using NFV. In: 2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC). pp. 1–4 IEEE, Las Vegas, NV, USA (2017). https://doi.org/10.1109/CCWC.2017.7868480.
3. Bendouda, D. et al.: Programmable architecture based on Software Defined Network for Internet of Things: Connected Dominated Sets approach. Future Generation Computer Systems. 80, 188–197 (2018). https://doi.org/10.1016/j.future.2017.09.070.

ISSN: 2233-7857 IJFGCN

4. da Costa, K.A.P. et al.: Internet of Things: A survey on machine learning-based intrusion detection approaches. Computer Networks. 151, 147–157 (2019). https://doi.org/10.1016/j.comnet.2019.01.023.
5. Deepali, Bhushan, K.: DDoS attack defense framework for cloud using fog computing. In: 2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT). pp. 534–538 IEEE, Bangalore (2017). https://doi.org/10.1109/RTEICT.2017.8256654.
6. Deng, R. et al.: Optimal Workload Allocation in Fog-Cloud Computing Towards Balanced Delay and Power Consumption. IEEE Internet Things J. 1–1 (2016). https://doi.org/10.1109/JIOT.2016.2565516.
7. Diro, A.A., Chilamkurti, N.: Distributed attack detection scheme using deep learning approach for Internet of Things. Future Generation Computer Systems. 82, 761–768 (2018). https://doi.org/10.1016/j.future.2017.08.043.
8. Firdhous, M. et al.: Fog Computing: Will it be the Future of Cloud Computing? 8 (2014).
9. Gupta, H. et al.: iFogSim: A toolkit for modeling and simulation of resource management techniques in the Internet of Things, Edge and Fog computing environments: iFogSim: A toolkit for modeling and simulation of internet of things. Softw. Pract. Exper. 47, 9, 1275–1296 (2017). https://doi.org/10.1002/spe.2509.
10. Imran, M. et al.: Toward an optimal solution against Denial of Service attacks in Software Defined Networks. Future Generation Computer Systems. 92, 444–453 (2019). https://doi.org/10.1016/j.future.2018.09.022.
11. Jalali, F. et al.: Fog Computing May Help to Save Energy in Cloud Computing. IEEE J. Select. Areas Commun. 34, 5, 1728–1739 (2016). https://doi.org/10.1109/JSAC.2016.2545559.
12. Kadhim, A.J., Seno, S.A.H.: Energy-efficient multicast routing protocol based on SDN and fog computing for vehicular networks. Ad Hoc Networks. 84, 68–81 (2019). https://doi.org/10.1016/j.adhoc.2018.09.018.
13. Kahvazadeh, S. et al.: Securing combined fog-to-cloud system through SDN approach. In: Proceedings of the 4th Workshop on CrossCloud Infrastructures & Platforms. p. 2 ACM (2017).
14. Khan, S. et al.: Fog computing security: a review of current applications and security solutions. J Cloud Comp. 6, 1, 19 (2017). https://doi.org/10.1186/s13677-017-0090-3.
15. Krishnan, P. et al.: SDN Framework for Securing IoT Networks. In: Kumar, N. and Thakre, A. (eds.) Ubiquitous Communications and Network Computing. pp. 116–129 Springer International Publishing, Cham (2018). https://doi.org/10.1007/978-3-319-73423-1_11.
16. Modarresi, A. et al.: A framework for improving network resilience using SDN and fog nodes. In: 2017 9th International Workshop on Resilient Networks Design and Modeling (RNDM). pp. 1–7 IEEE, Alghero (2017). https://doi.org/10.1109/RNDM.2017.8093036.
17. Mukherjee, M. et al.: Security and Privacy in Fog Computing: Challenges. IEEE Access. 5, 19293–19304 (2017). https://doi.org/10.1109/ACCESS.2017.2749422.
18. Mukherjee, M. et al.: Survey of Fog Computing: Fundamental, Network Applications, and Research Challenges. IEEE Commun. Surv. Tutorials. 20, 3, 1826–1857 (2018). https://doi.org/10.1109/COMST.2018.2814571.
19. Osanaiye, O. et al.: From Cloud to Fog Computing: A Review and a Conceptual Live VM Migration Framework. IEEE Access. 5, 8284–8300 (2017). https://doi.org/10.1109/ACCESS.2017.2692960.
20. Özçelik, M. et al.: Software-defined edge defense against IoT-based DDoS. In: 2017 IEEE International Conference on Computer and Information Technology (CIT). pp. 308–313 IEEE (2017).
21. Prabakaran, S., Ramar, R.: Stateful firewall-enabled software-defined network with distributed controllers: A network performance study. Int J Commun Syst. 32, 17, e4237 (2019). https://doi.org/10.1002/dac.4237.
22. Priyadarshini, R., Barik, R.K.: A deep learning based intelligent framework to mitigate DDoS attack in fog environment. Journal of King Saud University - Computer and Information Sciences. S1319157818310140 (2019). https://doi.org/10.1016/j.jksuci.2019.04.010.

ISSN: 2233-7857 IJFGCN

23. Sohal, A.S. et al.: A cybersecurity framework to identify malicious edge device in fog computing and cloud-of-things environments. Computers & Security. 74, 340–354 (2018). https://doi.org/10.1016/j.cose.2017.08.016.
24. Somani, G. et al.: DDoS attacks in cloud computing: Issues, taxonomy, and future directions. Computer Communications. 107, 30–48 (2017). https://doi.org/10.1016/j.comcom.2017.03.010.
25. Yousefpour, A. et al.: All one needs to know about fog computing and related edge computing paradigms: A complete survey. Journal of Systems Architecture. S1383762118306349 (2019). https://doi.org/10.1016/j.sysarc.2019.02.009.
26. Zhang, P. et al.: Security and trust issues in Fog computing: A survey. Future Generation Computer Systems. 88, 16–27 (2018). https://doi.org/10.1016/j.future.2018.05.008.
27. Zhou, L. et al.: A fog computing based approach to DDoS mitigation in IIoT systems. Computers & Security. 85, 51–62 (2019). https://doi.org/10.1016/j.cose.2019.04.017.
28. Internet of Things (IoT), mobile cloud, cloudlet, mobile IoT, IoT cloud, fog, mobile edge, and edge emerging computing paradigms_ Disambiguation and research directions.

ISSN: 2233-7857 IJFGCN