Informatics Bulletin, Faculty of Computers and Artificial Intelligence, Helwan University
Published Online ***Vol 3 Issue 2, July 2021***
(https://fcihib.journals.ekb.eg)

A Review of Intrusion Detection and Prevention Systems in Fog Computing Environment

Ibrahim Mohsen Selim
Tech.Assis. of Information Technology Department
Faculty of Computers and Artificial Intelligence
,Helwan University
Cairo , Egypt
ibrahimselim229@gmail.com

Rowayda Abdel-Hamid Sadek
Assoc.Prof. of Information Technology Department
Faculty of Computers and Artificial Intelligence
,Helwan University
Cairo , Egypt
rowayda_sadek@fci.helwan.edu.eg

***Abstract*—The development of the Internet of Things (IoT) has increased the interconnectivity of many IoT devices. Cloud computing is an ingenious way to process and store massive amounts of data in a simpler way, but using cloud computing seems to have some annoying problems, such as lack of location awareness, lack of geographic location distribution, lack of support for mobility, in addition to high latency and delay in response time. Developed another computing platform called Fog Computing as a supplement to the cloud solution, because it extends the computing range of the fog part and cloud services to the edge of the system, thereby making the processing, connection, retention, and storage functions more Proximity to this device solves the deficiencies faced by cloud computing. In addition, many issues related to protection, privacy, and security have appeared in the fog computing platform. Network defenses must be developed in a high-performance manner, detecting abnormal activity, monitoring all input and output communications in real-time, and developing new models for appropriate fog network portals to identify new attack families from the edge.**

***Index Terms*—Fog Computing, Cloud Computing, Edge Computing, Internet of Things.**

I. INTRODUCTION

With the popularity of the Internet of Things (IoT), the network architecture includes three layers: edge, cloud and fog, as shown in Figure 1, to provide dynamic analysis of network monitors and large-scale data analysis [1]. The edge layer contains IoT devices, computing devices and tools close to the organization. Fog is a decentralized computing architecture with the same services similar to the cloud, including software as a service (SAAS) , platform as a service (PAAS), and infrastructure as a service (IAAS) [2].

Fog computing is designed to solve cloud deficiencies such as lack of location awareness, lack of geographical location distribution, lack of support for mobility, in addition to high latency and delay in response time. The fog layer includes the same services as the cloud, but they are distributed to handle big-scale models and data services. Compared with cloud systems, as shown in Table I , fog systems have less resource computing power, such as memory, processing and storage, but they can be increased as needed.

A. Cloud Computing

Cloud computing is one of the most important services available on-demand that benefit users and organizations in general, as it provides a lot of resources over internet, whether it is computing power or storing huge amounts of data for them with high efficiency and lowest costs [3].

B. Fog Computing

The fog model aims to improve some of the deficiencies of cloud systems and analyze big data at network edge [4]. It brings the computing and data storage closer to were required to shorten the response time. Due to its instant response functionality, it can support many industrial applications, providing flexible and inexpensive in terms of hardware and software. In modern Edge-Fog-Cloud architecture, the network system is connected to many devices and computing

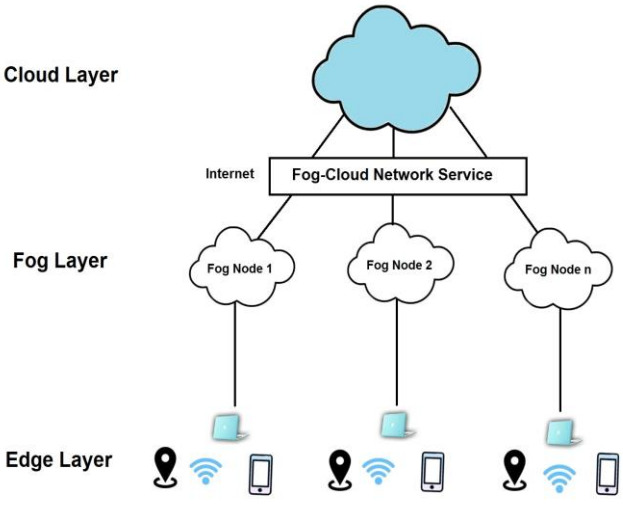

Figure 1.Hirarchical Architecture of Fog Computing

applications. A single device may generate small data, but when multiple device data are combined, the amount of data generated will become very large and difficult to process and verify in real time. Hardware and network elements are vulnerable to cyber-attacks because they use devices or network services.

TABLE I

SIMPLE COMPARISON OF CLOUD AND FOG COMPUTING [5]

	Cloud Computing	**Fog Computing**
Support for Mobility	limited	included
Location awareness	Partially	included
Latency	High	Low
Geographic distribution	Centralized	Decentralized
Distance to devices	Far	Near
Energy consumption	High	Low
Computation power and storage capabilities	High	Low
Service location	Through the internet	At network edge
Real-time interactions	supported	supported

C. Edge Computing

Edge computing offers additional advantages over fog computing because it increases the independence of each device and reduces points of failure, but this makes it difficult to manage data and also makes it difficult to collect data on large networks such as the Internet of Things [6].

II. FOG SECURITY

Since the Fog device is connected to the Cloud and IoT system, it allows the use of various cyber threats to exploit the IoT network. This is due to the proliferation of many unsecured devices and the inability to monitor and protect sites with high efficiency, the open structure of fog is a major cause of weaknesses as well. Attackers can use these weaknesses to work in fog devices and services, in addition to threats to their big data privacy [7].

A. Fog Attacks

There are also many different types of attacks facing Fog-IoT-Cloud architecture, such as intruders, Zero-day attacks and of course flood attacks in addition to abuse of service, advanced persistent threats and other attacks such as port scanning, back-door attacks, and user attacks to the root [1].

- **Intruders:** Users who access Fog as authorized users and are trying to obtain some resources without rights.
- **Zero-day attacks:** There is vulnerability in the software that is being exploited by the hacker and it is usually on virtual machines.
- **Flood attacks:** The attacker floods the victim by sending him an enormous number of packets such as Distributed Denial of Service (DDoS).
- **Service Abuse:** Allowing unauthorized hackers to access and exploit services.
- **Advanced Persistent Threats:** Attackers break into the system by using some sophisticated software to steal data from the system
- **Port scanning:** The hacker sends a message to find out a list of ports which are active, which are not, and then are being exploited**.**
- **Back-door attacks:** They are attacks that the hacker accesses authentication anonymously to control it remotely**.**
- **User attacks to Root:** An attacker try to access to the root from a legitimate user.

B. Fog Security Solutions

Access Control and Authentication as well as Encryption, Intrusion Detection, Firewall and Defense Systems. These security solutions seek to solve some of the various security problems and privacy challenges of the IoT-Fog-Cloud architecture [1]. There is also a set of suggested solutions that have been presented through the research [8], which are to secure every part in the layers of cloud and fog, as shown in Figure 2.

The Fog platform must have a high-quality mechanism to monitor the use of network resources, and it must be one of the basics of any fog platform where harmful activities are detected and attempted to avoid them or reduce their damages as much as possible before they occur [8]. It involves scanning dynamic networks to identify harmful packets based on a set of specific network controls and policies.

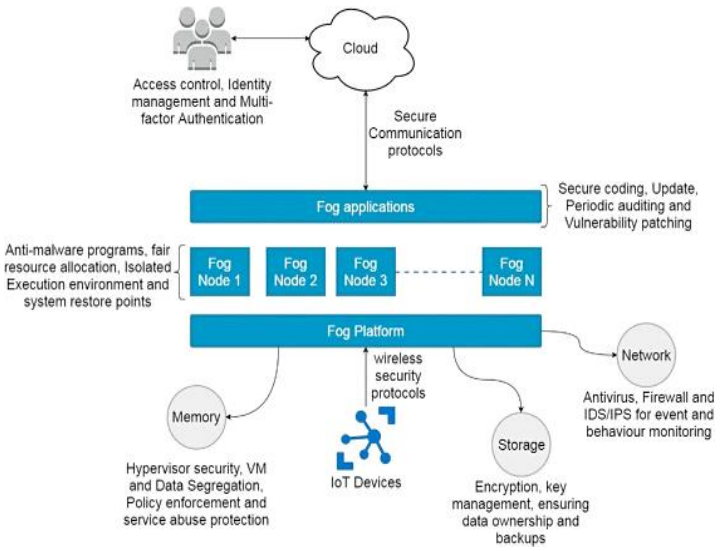

Figure 2.Some Security Solutions for each Component of the Fog System [8].

III. Important Aspects of Fog Security Techniques

A. Network Monitoring

The process of monitoring the network for network attacks can be divided into dynamic, static, or mixed of the two. Protection systems, firewalls, anti-virus , and intrusion have been used extensively to monitor and prevent harmful events. However, each method has its own advantages and disadvantages. Due to new variants in attack signatures, no one can detect and stop advanced persistent threats. The purpose of network monitoring is to collect useful information from different parts of the network so that the information collected can be used to administer and control the network [9]. Virtual Private Networks (VPNs) are also a line of protection that can protect networks from specific attacks, but they can also be compromised through using cryptographic attacks like man in the middle attacks.

B. Intrusion Detection System

Intrusion Detection Systems are widely used in network, cloud, fog and edge systems to reduce malicious attacks such as denial of service attacks and port scanning attacks in addition to attacks on virtual machines, especially hypervisors [10]. IDS is also considered a very important tool for networks in general to defend against attacks and predict them in the future before they happen [11]. In Fog Computing, IDS can be used in the fog node to detect malicious intrusions and activities by monitoring persistent user login information, following access control policies, as well as carefully analyzing log files [12]. It can also be used on the network side and also helps to clarify some of the features of advanced systems and how it can detect both client-side and cloud-based intrusion. There are also some challenges that these systems face, such as implementing large intrusion detection in a fog computing environment with high mobility and geographic dispersion, taking into account the low latency. IDS can also be used in computing fog on the fog node system side to detect any unsuspecting behavior by monitoring and analyzing files, especially log files, tracking the implementation of access control policies, as well as monitoring user login information. Also, intrusion detection techniques can be classified into two categories, namely detection, signature based intrusion detection systems, and anomaly-based intrusion detection systems [13].

C. Intrusion Prevention System

Intrusion prevention system is one of the tools that exist on the network, which is used to discover malicious activities and prevent any malicious activity trying to access the network. IPS is mainly used to detect attacks in addition to recording them, as well as prevent malware or other types of special exploits [14].

D. Privacy and Encryption

The protection of user information is one of the biggest problems we face in many systems such as the Internet of Things, fog, and edge in addition to cloud systems. There are also many different methods and many mechanisms for preserving privacy that have been proposed and implemented in both the cloud and networks. It can complete between layers of cloud and fog to prevent infiltration and protect big data between them. Encryption techniques must be used during data exchange between internal network nodes and other networks [15]. Distributions of network nodes, security and privacy technologies need a lot of research to secure sensitive information.

E. Access Control

Access control is one of the most important tools to ensure system security in addition to protecting privacy, and due to the nature of the outsourcing of the fog layer, it must be encrypted for the external data. Several public key-based solutions have been used in an effort to achieve access control. Yu et al. [16] made a scheme that illustrates and uses Attribute-Based Encryption.

We will present some cyber defense plans, discover anomalies, monitor all input and output network connections in real-time with high performance, and develop models on network portals that are fog/edge fit, such as IDS that can identify new attack families from the edge. IDS detects malicious intrusions and activities by monitoring persistent user login information, following access control policies, as well as carefully analyzing log files.

IV. Challenges of Fog Security

Since the fog network is connected and deals with a huge number of devices, the data that any device generates may be small, but when a number of devices are combined, it becomes

difficult to process the total amount of data, so filtering each network packet will insist on increasing processing power and memory. Fog computing systems contain many and many nodes because of their nature that they are decentralized and this leads to high energy consumption. Therefore, a lot of work is required in developing and improving protocols that help to save and start new structures that are suitable for fog models such as improving the efficiency of communication protocols and increasing Efficiency of network resources and optimization of computing protocols [17].

The network resource monitoring mechanism must be implemented within each fog platform because it is one of the basics of the fog system as it is used to identify and reduce harmful activities before any damage to the system occurs. The process includes examining large and dynamic networks to identify harmful and unwanted packets according to predefined basics and network rules. Scanning is usually done by classification of firewalls, antivirus, intrusion detection, and protection systems.

Applications can be used in a distributed manner, suitable for network distribution, and in an intuitive and intelligent manner that will help improve network monitoring. As there are a huge number of different heterogeneous devices that transfer, exchange and process data at different levels such as operating systems, system management programs and also applications. Spending a lot of time discovering and monitoring normal network activity may not correspond to the real-time nature of sending packets of data. Encryption methods are very accurate and effective ways to provide privacy, but these systems usually affect performance because they require a lot of accounts and communication. With the emergence of new attack families, over time, the old attacks gradually developed and a new group of attack families appeared, so it was necessary to keep pace with and deal with those attacks.

V. STATE OF THE ART

A total of six research works have been identified in which a range of different technologies have been used to secure and monitor fog computing [18], [19], [20], [21], [22], [23].

- *Related Work*

  In [18], Sohal, A. S., Sandhu, R., Sood, S.K, & Chang made a network security framework using three different technologies, Markov Model, IDS, and Honeypot Virtual Device (VHD), as shown in Figure 3, used to identify harmful devices in a fog computing environment.

  1. Markov Model: The hidden two-stage Markov model is used to effectively classify peripheral devices into different levels :
     - Legitimate Devices (LD)
     - Sensitive Devices (SD)
     - Under Attacked Devices (UD)
     - Hacked Devices (HD)
  2. Intrusion Detection System (IDS): It analyzes the network traffic of Fog Computing as when certain end devices try to slow down the network speed, for example when sending data at a rate slower than its available capacity, alerts of attack are generated.
  3. Virtual Honeypot Device (VHD): used to record logs of all hacked devices to help the system discard future unknown attacks.

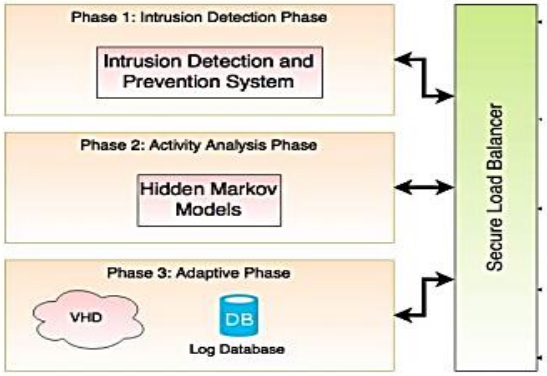

Figure 3.Three Phase of Cyber-Security Framework [18].

It was clarified in the outputs that this model is successful in detecting the harmful devices in addition to that it reduces the false IDS alarm rate, but there is a problem as when the legitimate edge device is returned from the VHD, some errors can occur.

In [19], Wang, Y., Meng, W., Li, W., Li, J., Liu, WX, & Xiang, Y made a framework for privacy protection for signature-based fog detectors in distributing networks based on some characteristics where results in all environments show that similar methods used in the framework can also have. They used a way to protect IDS privacy by implementing Non Trusted Third Party (TTP) encryption methods. The Privacy Protection Framework is used for distributed intrusion detection and collaboration, including the approved threat model and Rabin's fingerprint algorithm, for signature matching for intrusion detection based on the collaborative signature.

This framework can help maintain shared data privacy, reduce cloud-side workload, and provide less detection delay.

In [20], the author proposes to discover different DDoS vulnerability attack cases on Fog network where DDoS attacks are malicious attempts to destroy normal traffic of the target network by flooding the target or the infrastructure around internet traffic. In this case, the IDS for DDoS attacks is detected based on:

- Nave Bayesian: The author uses Bayesian Networks for measurement conditional probabilities to

determine if a packet is normal or it is an intrusion packet.

- Markov model and virtual honeypot device can provide high protection and increase security against DDoS attackers.

With a dataset containing multiple features, it is necessary to choose some of the attributes appropriate for this attack and to remove redundant features because it helps improve detection accuracy for the rapid detection of DDoS attacks, but it is only suitable for the need to detect DDoS. Found to get good results and reduce the false positive rate of attack.

In addition, Yassin et al. in [21], the intrusion detection system is developed using certain functions of fog computing to identify network attacks in wireless sensor networks. Especially in selective forwarding attacks (SFA), attackers who participate in routing as normal nodes selectively ignore data packets from neighboring nodes. The IDS system uses static monitoring sensors to alleviate the selective redirection problem in mobile wireless sensor networks. The log also maintains a table of input data packets, and forwards data packets to or from the monitored node's data packet. This information is used to determine the node's neglect rate at a given time to determine whether the node is a malicious node or a safe one.

In addition, Aliyu, F., Sheltami, T. and Shakshuki, EM in [22] made intrusion detection systems and intrusion prevention systems in a fog environment to eliminate MitM attacks as IDS nodes inquire about the nodes connected to them with one hop away and IPS uses simple encryption to prevent MitM attacks.

In addition, Shi, Y., Abhilash, S., Hwang, and K. in [23] made a security framework that based on the Cloudlet network architecture. It can detect intruders in a cloud and ensure that mobile devices, Cloudlet and communications between clouds are secure. The security framework also creates a protective shield to combat cloud intrusion and prevent spam or virus attacks.

VI. FOG SIMUATION PLATFORMS

In addition to real solutions, we also need simulations to study and try the inner and outer workings of different IoT-Fog-Cloud system, also to develop effective new algorithms for managing and protecting data. There are several simulators available to specifically check distributed cloud systems and IoT systems [24]. Simulations are easier to set up, cheaper, and usually faster and more convenient, so there are some tools that are some of the best simulation tools for edge, fog and cloud computing, and the Internet of Things such as:

- OMNet ++: A library and framework for building standard network emulators [25].
- IFogSim: A framework for simulating fog computing services used to provide a global simulation framework in which to develop and pilot a fog computing infrastructure [26].
- Cloudsim: a framework for simulating the infrastructure of cloud computing where one can focus on designing a system to verify some problems without worrying, in addition to providing accurate information related to the cloud infrastructure and services [27].

VII. FUTURE WORK

A new mechanism must be developed on network portals suited to a fog/edge environment that can identify new attack families from the edge in an effort to reduce some of the limitations of previous network monitoring techniques, develop network defenses, detect anomalous activity, and monitor all input and output communications using high-performance manners.

VIII.CONCLUSION

The research provides research works on fog/edge, which is a decentralized computing architecture with the same services as similar to cloud services. Utilizing fog by addressing tasks at the network edge eliminates major cloud layer challenges such as supporting mobility, location awareness, low latency, and geographic location. Fog technology continues to be used to address security and privacy challenges that stem from connectivity to IoT architecture and cloud systems. The goal is to enhance the security of fog computing and develop a network defense that can identify new attack families from the edge.

REFERENCES

[1] Moustafa, N. (2019). A Systemic IoT-Fog-Cloud Architecture for Big-Data Analytics and Cyber Security Systems: A Review of Fog Computing. *arXiv preprint arXiv:1906.01055*.

[2] Dastjerdi AV, Gupta H, Calheiros RN, Ghosh SK, Buyya R (2016) Fog computing: Principals, architectures, and applications. *arXiv preprintarXiv:1601.02752*

[3] Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J., & Ghalsasi, A. (2011). Cloud computing—The business perspective. *Decision support systems*, *51*(1), 176-189.

[4] Stojmenovic, I., & Wen, S. (2014, September). The fog computing paradigm: Scenarios and security issues. In *2014 federated conference on computer science and information systems* (pp. 1-8). IEEE.

[5] Hu, P., Dhelim, S., Ning, H., & Qiu, T. (2017). Survey on fog computing: architecture, key technologies, applications and open issues. *Journal of network and computer applications*, *98*, 27-42.

[6] Neware, R. (2019). Fog Computing Architecture, Applications and Security Issues: A Survey.

[7] Pierson, R. M. (2017). How Does Fog Computing Differ from Edge Computing. *Online: https://readwrite. com/2016/08/05/fogcomputing-different-edge-computing-pl1/. Accessed*, *12*.

[8] Khan, S., Parkinson, S., & Qin, Y. (2017). Fog computing security: a review of current applications and security solutions. *Journal of Cloud Computing*, *6*(1), 1-22.

[9] Shin, S., & Gu, G. (2012, October). CloudWatcher: Network security monitoring using OpenFlow in dynamic cloud networks (or: How to provide security monitoring as a service in clouds?). In *2012 20th IEEE international conference on network protocols (ICNP)* (pp. 1-6). IEEE.

[10] Modi, C., Patel, D., Borisaniya, B., Patel, H., Patel, A., & Rajarajan, M. (2013). A survey of intrusion detection techniques in cloud. *Journal of network and computer applications*, *36*(1), 42-57.

[11] Sadek, R. A., Soliman, M. S., & Elsayed, H. S. (2013). Effective anomaly intrusion detection system based on neural network with indicator variable and rough set reduction. *International Journal of Computer Science Issues (IJCSI)*, *10*(6), 227.

[12] Raponi, S., Caprolu, M., & Di Pietro, R. (2019, June). Intrusion detection at the network edge: Solutions, limitations, and future directions. In *International Conference on Edge Computing* (pp. 59-75). Springer, Cham.

[13] Sadaf, K., & Sultana, J. (2020). Intrusion detection based on autoencoder and isolation Forest in fog computing. *IEEE Access*, *8*, 167059-167068.

[14] Tabrizchi, H., & Rafsanjani, M. K. (2020). A survey on security challenges in cloud computing: issues, threats, and solutions. *The Journal of Supercomputing*, 1-40.

[15] Lee, K., Kim, D., Ha, D., Rajput, U., & Oh, H. (2015, September). On security and privacy issues of fog computing supported Internet of Things environment. In *2015 6th International Conference on the Network of the Future (NOF)* (pp. 1-3). IEEE.

[16] Yu, S., Wang, C., Ren, K., & Lou, W. (2010, March). Achieving secure, scalable, and fine-grained data access control in cloud computing. In *2010 Proceedings IEEE INFOCOM* (pp. 1-9). Ieee.

[17] Sadek, R. A. (2018). Hybrid energy aware clustered protocol for IoT heterogeneous network. *Future Computing and Informatics Journal*, *3*(2), 166-177.

[18] Sohal, A. S., Sandhu, R., Sood, S. K., & Chang, V. (2018). A cybersecurity framework to identify malicious edge device in fog computing and cloud-of-things environments. *Computers & Security*, *74*, 340-354.

[19] Wang, Y., Meng, W., Li, W., Li, J., Liu, W. X., & Xiang, Y. (2018). A fog-based privacy-preserving approach for distributed signature-based intrusion detection. *Journal of Parallel and Distributed Computing*, *122*, 26-35.

[20] Singh, S., Kumari, K., Gupta, S., Dua, A., & Kumar, N. (2020, June). Detecting Different Attack Instances of DDoS Vulnerabilities on Edge Network of Fog Computing using Gaussian Naive Bayesian Classifier. In *2020 IEEE International Conference on Communications Workshops (ICC Workshops)* (pp. 1-6). IEEE.

[21] Yaseen, Q., AlBalas, F., Jararweh, Y., & Al-Ayyoub, M. (2016, September). A fog computing based system for selective forwarding detection in mobile wireless sensor networks. In *2016 IEEE 1st International Workshops on Foundations and Applications of Self* Systems (FAS* W)* (pp. 256-262). IEEE.

[22] Aliyu, F., Sheltami, T., & Shakshuki, E. M. (2018). A detection and prevention technique for man in the middle attack in fog computing. *Procedia Computer Science*, *141*, 24-31.

[23] Shi, Y., Abhilash, S., & Hwang, K. (2015, March). Cloudlet mesh for securing mobile clouds from intrusions and network attacks. In *2015 3rd IEEE International Conference on Mobile Cloud Computing, Services, and Engineering* (pp. 109-118). IEEE.

[24] Markus, A., & Kertesz, A. (2020). A survey and taxonomy of simulation environments modelling fog computing. *Simulation Modelling Practice and Theory*, *101*, 102042.

[25] Varga, A., & Hornig, R. (2008, March). An overview of the OMNeT++ simulation environment. In *Proceedings of the 1st international conference on Simulation tools and techniques for communications, networks and systems & workshops* (pp. 1-10).

[26] Mahmud, R., & Buyya, R. (2019). Modelling and simulation of fog and edge computing environments using iFogSim toolkit. *Fog and edge computing: Principles and paradigms*, 1-35.

[27] Beloglazov, A. (2016). Cloudsim: A framework for modeling and simulation of cloud computing infrastructures and services. Cloud Computing and Distributed Systems (CLOUDS) Laboratory, Department of Computer Science and Software Engineering, the University of Melbourne, Australia.