**A Review of Threats, Attacks and Security Countermeasures in Fog Computing**

Raphael KAIBIRU

*Machakos University, P.O Box 136-90100, Machakos, Kenya*

Mercy WAIRIMU

*Machakos University, P.O Box 136-90100, Machakos, Kenya*

**Abstract:** The world currently is experiencing an upsurge growth in the number of devices that are connected to the internet. This development is being referred to as Internet of Things (IoT). This phenomenon has presented new challenges to the already existing cloud infrastructure and in turn led to development of an intermediating paradigm called Fog Computing. Fog computing as a subset of Cloud Computing is being used to improve on the challenges faced by the cloud computing infrastructure especially when it comes to latency and real-time feedback of processed data. Several research have been done addressing the issue of privacy in Fog Computing but few have tackled the specific threats, attacks and security countermeasures facing Fog Computing. Therefore, this paper addresses the threats, attacks and security measures related with Fog Computing. The methodology opted for this paper is a review of papers with keywords IoT, Fog Computing Security, Threats, attacks and solutions or countermeasures. In this paper we presented threats, attacks and countermeasures in fog computing.

**Keywords**: IoT, Cloud Computing, Fog Computing, Fog Computing Security

# **Introduction**

The exponential growth of connected smart devices has shaped the current computing technology. The emergent of non-computer devices (things) being integrated in the internet has come to be referred to as Internet of Thing (IoT). IoT has been made popular by the current development in wearable devices, smart homes and cities, smart meters, connected vehicles, smart traffic lights among other development (Rauf, Shaikh, and Shah 2018; Yi, Qin, and Li 2015). Internet of Things devices are primarily used to collect and transmit data for processing in the cloud and receive feedback or results for decision making. According to (Liu et al. 2018), IoT technology has become an indispensable part of our daily life with billions of IoT devices joining the internet infrastructure.

Despite the increased use of IoT devices, these devices are faced with challenges ranging from low computation power, battery, storage and bandwidth which has a negative result of low quality of Service (QoS) and user experience (Atlam, Walters, and Wills 2018; Ni et al. 2017; Rauf et al. 2018; Yi et al. 2015). To alleviate on the challenges faced by IoT devices, cloud computing is considered as an ideal platform that can deliver services to the users. Cloud computing however is not a one-fit solution to problems inherent in IoTs functioning (Stojmenovic et al. 2015; Yi et al. 2015).

To address this problems Fog Computing (FC) was proposed by Cisco in 2012. Cisco predicted that 50 billion devices will be joining the internet by the year 2020 and that these numbers would reach 500 billion by the year 2025 (Cahmi, 2015). This can be interpreted to mean that more data will be produced and users will need results and feedbacks quickly. Therefore, Fog computing will bring services closer to the end user of these devices (Aljumah and Tariq 2018; Mukherjee et al. 2017; Ni et al. 2017; Razouk, Sgandurra, and Sakurai 2017).

In an abstract manner Fog computing is a subset of Cloud Computing which is an intermediating infrastructure to offer services in an efficient manner to the end user. Despite the security advantages attributed to cloud computing, that cannot be said of Fog Computing. This is to mean that Fog computing cannot entirely inherit similar advantages or disadvantages from cloud computing (Ni et al. 2017). There are specific security problems facing Fog computing that are unique to this emerging paradigm.

1. **Problem Statement**

This review paper is domiciled on the hard research fact that there is a lack of literature review regarding threats, attacks and sound solutions to security issues facing Fog Computing. An in-depth review shows that many researchers have focused more on privacy of Fog Computing and not addressing the real threats that would compromise the security in this infrastructure (Alrawais et al. 2017; Lee et al. 2015; Liu et al. 2018; Rauf et al. 2018; Yi et al. 2015). From an Information Systems Security perspective, privacy is just one of the goals of computer security. Therefore, it is worth noting that there is need to look at Fog Computing in holistic manner hence encompassing all the three security goals of Confidentiality, Integrity and Availability. In this paper threats, attacks and countermeasures central to the security of Fog Computing were discussed.

1. **Objectives**

The main objective of this paper is to provide a review of threats, attacks and countermeasures in Fog Computing. In order to achieve this objective, the following specific objectives were addressed.

1. To discuss the concept of Fog Computing.
2. To review related work in Fog Computing
3. To identify and analyze threats and attacks in Fog Computing.
4. To provide countermeasures of threats and attacks in Fog Computing.

The remainder of this paper is organized as follows. In section 2 we present an overview of fog computing. In section 3 we present an overview of related works. In Section 4, we provide a discussion on threats, attacks and countermeasures in fog computing. Finally we conclude with a summary of a discussion on our contribution and future work in section 5.

# **Overview of Fog Computing**

Before delving into the main focus of this paper, it is worth providing an overview of Fog computing. This enables the reader to gain foundational knowledge in this emerging paradigm.

##  **Evolution from Cloud to Fog**

IoT enables connected devices to collect data and communicate with each other. IoT devices are small, low storage, low processing speed in nature. While these challenges pose an imminent functional downsides, Cloud computing comes in to leverage on these weaknesses. Cloud is deemed the ideal solution to these inherent challenges in IoT (Alrawais et al. 2017; Liu et al. 2018; Ni et al. 2017).

The integration of IoT with Cloud provides practical solutions ranging from powerful data processing, centralized data storage, scalable resource allocation and low cost. This integration gave rise to Cloud-based IoT architecture that is made up of two layers-the top layer and bottom layer. The top layer consists of the cloud storage and control layer in which the cloud operates. The bottom layer consists of all IoT devices interconnected to gather data. These two layers are connected through communication medium and equipment such as gateways, routers, bridges, and exchange data via standard protocols (Ni et al. 2017).

Despite the benefits provided by cloud computing in cloud based IoT architecture, (Ni et al. 2017, 2017; Razouk et al. 2017; Saraju et al. 2019) noted that cloud computing is not a panacea that can address all the problems in IoT. The distance between cloud and IoT devices creates a problem of latency and jitters which needs a quick fix, as IoT devices continue to increase in their thousands. The solution to this problem has come to be referred to as Fog Computing.

## **What is Fog Computing?**

The concept of Fog Computing was introduced by Cisco in the year 2012 and it is defined as an extension of cloud computing paradigm that provides computation, storage, and networking services between end devices and the traditional cloud servers (Bonomi et al, 2012). A closer look at this definition, it can be noted that fog computing is leveraging on issues experienced with cloud based IoT architecture. However, it is still worth noting that Fog Computing is not a replacement of cloud computing but complement it (Alrawais et al. 2017; Ni et al. 2017; Rauf et al. 2018).

Fog nodes are deployed next to the edge of the network closer to the devices. To deal with the increasing number of IoT devices Fog Computing manages storage, networking and computation services provided at the edge of a network (Ni et al. 2017; Zaheer and Shah 2017).

## **Fog Computing Architecture**

Fog computing architecture can be divided into two categories; Cloud-Fog-Device framework and Fog-Device Framework. Figure 1 show the Cloud-Fog-Device framework made up of three layers.



Figure 1: Cloud-fog-device framework

In Cloud-Fog-Device framework, Layers are arranged in an increasing order of processing power and storage capabilities.

**Device Layer**

The device layer has two types of devices that include mobile IoT devices and fixed IoT devices. As the name suggests, mobile IoT devices are carried around by their owners such as wearable devices (fitness trackers, wearable cameras, sport bracelets) and mobile smart devices (smart phones, smart watches, smart glasses) (Zaheer and Shah 2017). People owning these devices can or devices belonging to one person can form a groups and communicate with each other using wireless and ad hoc networks (Mukherjee et al. 2017; Ni et al. 2017). The fixed IoT devices are pre-deployed in specific areas or products to fulfill a certain task.

**Fog Layer**

The fog layer consists of network equipment such as routers, gateways, switches, base stations with installed servers. These devices form what is referred to as fog nodes that can be deployed anywhere with network connection such as roadside, inventory rooms, buildings etc. Fog nodes are equipped with certain storage capabilities to store data temporarily. This transient storage of data in the fog nodes significantly reduce communication overheads between fog nodes and cloud, which in turn shortens the response time of access data and updates (Ni et al. 2017).

**Cloud Layer**

This is a consolidated computing and storage platform that provides IoT services in global perspective. The cloud receive summarized data from fog nodes and the data from other sources to improve on business insights in IoT application such as health status monitoring, weather forecasting among others.

1. **Related Work**

This section is a review of related work on security in Fog Computing. Seventeen papers with key words fog computing security were reviewed. This was arrived at through purposive sampling from the high number of papers with key words fog computing. Owing to the high number of papers from journals, Google scholar and other online sources papers were selected based on relevance of the topic under discussion.

In his paper (Saraju et al. 2019) provided a discussion on fog computing security challenges and future direction. Security issues discussed were based on architectural aspect of fog computing and this contributed to the body of knowledge in fog computing security. The paper also provided the solutions to the current security issue affecting fog computing.

 (Aljumah and Tariq 2018) wrote a review paper on fog computing and security issues. In this paper the overview of security issues was addressed and the paper focused more privacy aspect of fog computing to ensure there was security. Therefore, the main focus of that paper was to provide a summary of security and privacy issues in fog computing.

On the part of Fog Computing application (Khan, Parkinson, and Qin 2017) wrote a review paper on Fog computing security with a focus on application and security solutions. The paper provided information on security issues surrounding various areas of Fog Computing application. The researcher proposes a holistic approach to fog security by not only looking at one element in the big architecture of fog computing.

 (Stojmenovic et al. 2015) conducted a research on issues affecting Fog Computing. The paper was based on the man-in-the-middle attack simulation. This paper was biased to only one form of attack in fog computing.

The introduction of Fog Computing in the Cloud-IoT infrastructure has posed many security challenges. To address this issue (Alrawais et al. 2017) conducted a research on how to provide security to the IoT through Fog Computing. In their paper, security of IoT was implemented by providing a Certificate verification between communicating IoT devices.

In (Liu et al. 2018; Yi et al. 2015) security and privacy issues of fog computing was discussed. The paper focused on challenges and solutions affecting fog computing.

System reliability is one of the key factor to consider when implementing an information security. To address this topic (Zaheer and Shah 2017) did a review on fog security issues and the main focus was on the architectural vulnerabilities that can be exploited by attackers. The paper proposed a security feature that can be applied to ensure the reliability of the system.

Traditional security solutions cannot be used to provide security to the current and new paradigm in IoT infrastructure. Based on this fact (Razouk et al. 2017) wrote a paper on how Fog Computing can applied to provide security to IoT infrastructure. The contribution of this paper was development of a middleware mediating security solution in Fog Computing.

Other researchers (Lee et al. 2015; Ni et al. 2017; Rauf et al. 2018) wrote papers on securing IoT through Fog Computing. Collectively these papers indicated that for IoT to be secure, there is need to first think of the intervening security measures in the fog layer of Fog computing.

1. **Security Threats in Fog computing**

Earlier in this paper it was noted that Fog computing is not a replacement of cloud computing but a complement. Despite that Fog Computing is a new paradigm in the cloud infrastructure, this extension of Cloud Computing is faced with the same security threats. In this section we discuss threats facing Fog Computing. The following are the security threats facing Fog Computing:

**Insider User Threat**

System users within the organization pose the greatest threat to any information system. In Fog computing environment, user tasked with the responsibility of accessing, maintaining, using and monitoring IoT devices can turn to be malicious attackers. Since Fog nodes are deployed next to the IoT network closer to the users, they are prone to insider threat. It is worth noting that an insider attacker can cause serious problems to the entire cloud supported network. The attacker can cause a Distributed Denial of Service among other attacks.

**External Threat**

Fog Computing is also susceptible to external threats from outside the organization. At the edge network there are IoT devices facing the public network. An external attacker can conduct an attack to several aspects of Cloud-Fog-IoT architecture by compromising the hardware and software. Some attacks such as jamming can be performed remotely hence having a security implication to the IoT system.

**Data Leakage**

Since Fog Computing operate on the Cloud Platform, it is prone the data leakage. Cloud infrastructures are a shared resource where several customers can be given similar platform and this scenario can lead to data leakage. Human errors or faulty hardware can cause data to leak to competitor companies sharing the same cloud service provider.

**Physical Disruption**

The threat of disruption caused by physical access, natural disaster such as earthquake, floods and human vandalism can affect fog computing infrastructure. Companies and institutions that implement fog computing in their IoT infrastructure need to ensure that these devices are safe from physical threats that can cause a disruption in case of an attack.

**Denial of Service Threat**

The threat of denial of service against fog computing can be both from external or internal source. In the event there is a DoS attack to a Fog computing infrastructure the impact of this attack can affect the entire IoT device ecosystem.

1. **Attacks in Fog Computing**

Since this paper was focusing on Threats, attacks and countermeasures, this section provides a discussion on threats, attacks and countermeasures in the Fog layer. The Fog layer is further categorized into three sections namely Fog Server, Middleware (Communication Medium) and Sensing Layer (IoT Plane). Figure 2 shows the hierarchy of the Fog layer.



Figure 2: Fog Hierarchy according to network communication

The following section we provide a discussion of security attacks in Fog Computing based on the three hierarchy. Several researchers (Aljumah and Tariq 2018; Atlam et al. 2018; Lee et al. 2015; Ni et al. 2017; Rauf et al. 2018; Saraju et al. 2019) have provided literature on security attacks in Fog computing and in this paper we provide a discussion of these attacks.

**Sensing Layer**

The sensing layer of fog architecture is responsible for collecting data directly from the environment and is also referred to as object layer. Devices and the technologies used in this layer include Radio Frequency Identity (RFID) tags, Wireless Sensor Networks (WSN) and Near Field Communication (NFC) (Saraju et al. 2019). In the following section we provided a discussion of threats affecting sensing layer.

* 1. **Security Attacks in Sensing Layer**

Potential threats and attacks associated with sensing layer includes: Node capture/device tampering, Spoofing attacks, signal jamming, Sybil attack, replay attack, node outage, Denial of Service and malicious data.

1. **Node Capture-** IoT Nodes are susceptible to node capture or device tampering. Things at the IoT gateways are weakened and important data are leaked. Such threats can have detrimental effects to the correct functioning of the network.
2. **Spoofing Attack-** In cyber security spoofing is when a person or something pretends to be something else and with an attempt to gain our confidence and trust, and get access to the system, data, steal money or spread malware. Spoofing attacks in fog computing, attackers conceal data and send fake data to the network. In this attack, things take identity of the original source and this gives the attacker full access of the system.
3. **Signal Jamming-** Jamming generates interference in the communication between network devices using radio frequency. This attack is deployed by flooding the network with large amount of data packets to jam or consume the transmission channels or its resources in order to restrict the genuine users from having an efficient and reliable network access.
4. **Denial of Service Attack-** This attack floods sensor nodes by injecting replayed and false packets. These intrusion attacks consume network resources like bandwidth, battery, time thus degrading the performance of fog as the fog resources are limited.
5. **Sybil Attack-** The network criminals use fake name and identities to control the fog computing effectiveness and convert the genuine nodes into compromised nodes. The ruthless effect is that it generates fake crowd sensing reports as the results prepared by these reports are not worth trusting. In addition to this, these attackers can expose the personal information of a legitimate user.
	1. **Security Attacks in Middleware Layer**

Secure transmission of sensed data and storage is the main concern in the middleware layer. This layer deals with Confidentiality, Integrity and Availability issues. Threats and attacks in this layer include: selective forwarding, black hole attack, wormhole, hello flood attack, acknowledge flooding.

1. **Selective Forwarding-** In selective forwarding some data packets are blocked and selectively dropped by a malicious node. There are two types of selective forwarding-the dropping of data packets and infected nodes randomly skipping the routing of data packets.
2. **Black hole attack-** In this attack unfaithful routing information is created and all the data packets are diverted to the sink hole. This attack may cause network congestion and packet drop.
3. **Wormhole attack-**The bits of data are relocated in the network by tunneling to a different storage location.
4. **Hello flood attack-** The attacker floods the channel with false data packets to create network congestion. They also persuade every node that their neighbor is a malicious node when participating in packet transmission.
	1. **Security Attacks in Fog Server**

The fog server is the front end in fog hierarchy and it requires different levels of security based on applications running on it. The security threats vary as per the protocols. The protocols involved include Message Queuing Telemetry Transport, Advanced Message Queuing Protocol, Constrained Application Protocol and the Extensible Messaging and Presence Protocol. These protocols face the following threats and attacks:

1. **Sniffer/Loggers:** The attackers use sniffing to extract important data such as password, email and FTP files. Many protocols in the network are vulnerable to sniffing.
2. **Phishing attack:** the email address of the main authority is used to gain credentials and damage data.
3. **Injection:** it is when infected codes are injected into the application that is executed on the server. This attack can be result in loss of data especially if it performed on database.
4. **Session hijacking:** this attack basically hijacks the session of someone else identity. This gives the attacker access to the persons system.
5. **Social Engineering:** Attackers gain vital application information by befriending them and later misusing their information.
6. **Security Countermeasures of Attacks in Fog Computing**

In this section we discussed some of the sound solutions to security threats faced in each layer of fog layer.

* 1. **Security Solutions in Sensing Layer**

Existing solutions to overcome security threats in the sensing layer of fog computing include, authorization, cryptography, steganography, image processing, spread spectrum communication, jamming report, error correcting codes and collision detection.

* 1. **Security Solutions in Middleware Layer**

The existing and some of the proposed solutions to overcome the security threats of fog computing middleware includes: Transport Layer security (TLS), Secure Socket Layer (SSL), Internet Protocols Security (IPSec), Intrusion Prevention System (IPS), firewalls.

Other solutions include link layer encryption, authenticated broadcasting, multipath routing, identity verification and packet authentication as well as password management and policies and periodic password change.

* 1. **Security Solutions in Fog Server**

Existing solutions to overcome the security of the fog server layer include the following.

* Safe programming testing, antivirus software, cache development and data verification.
* Access control lists, selective disclosure, IPS, Firewall, Intrusion detection system and session inspection.
* Boundary inspection and data encryption to avoid the risk of primary leakage.
* Risk assessment to identify threats in the involved network.
1. **Conclusion and Future Work**

In this paper we have provided a review of threats, attacks and countermeasures to security issues related to fog computing. We have provided threat and attacks affecting various layers of fog architecture and their countermeasures. In order to provide security in fog computing Fog as a Service (FaaS) providers need to offer solutions to security threats and attacks that are specific to fog computing and not the general security solutions applied in the traditional computing architectures. In addition we have provided a brief but concise overview regarding fog computing and how it links between the IoT devices and the traditional cloud architecture.

This paper has contributed to the body of research by providing threats, attacks and countermeasures to security issues affecting fog computing. In future research we propose that more research in the field of fog computing the address the issue of specific threats. This intervention will give rise to more knowledge in this ever growing paradigm in Cloud and IoT Computing.

**Reference**

Aljumah, Abdullah, and Ahamed Tariq. 2018. “Fog Computing and Security Issues: A Review.” in *2018 7th International Conference on Computers Communication and Control (ICCCC)*.

Alrawais, Arwa, Abdulrahman Alhothaily, Chunqiang Hu, and Xiuzhen Cheng. 2017. “Fog Computing for the Internet of Things: Security and Privacy Issues.” *IEEE Computer Society*.

Atlam, Hany, Robert Walters, and Gary Wills. 2018. “Fog Computing and the Internet of Things: A Review.” *MDPI Journals* 1(10):1–18.

Khan, Saad, Simon Parkinson, and Yongrui Qin. 2017. “Fog Computing Security: A Review of Current Applications and Security Solutions.” *Journalof Cloud Computing: Advances, Systems and Applications* 6(19).

Lee, Kanghyo, Donghyun Kim, Dongsoo Ha, Ubaidullah Raput, and Heekuck Oh. 2015. “On Security and Privacy Issues of FOg Computing Supported Internet of Things Environment.”

Liu, Ximeng, Yang Yang, Raymond Choo, and Huaqun Wang. 2018. “Security and Privacy Challenges for Internet of Things and Fog Computing.”

Mukherjee, Mithun, Rakesh Matam, Lei Shu, Leandros Maglaras, Amine Ferrag, Nikumani Choudhury, and Vikas Kumar. 2017. “Security and Privacy in Fog Computing: Challenges.” *IEEE Access* 5:19293–304.

Ni, Jianbing, Kuan Zhang, Xiaodong Lin, and Xuemin Shen. 2017. “Securing Fog Computing for Internet of Things Applications: Challenges and Solutions.”

Rauf, Abdul, Riaz Shaikh, and Asadullah Shah. 2018. “Security and Privacy for IoT and Fog Computing Paradigm.”

Razouk, Wissam, Daniele Sgandurra, and Kouichi Sakurai. 2017. “A Security Middleware Architecture Bases on Fog Computing and Cloud to Support IoT Constrained Devices.” Liverpool, United Kingdom: Association of Computing Machinery.

Saraju, Mohanty, Deepak Puthal, Bhavake Ashok, Graham Morgan, and Rajiv Ranjan. 2019. “Fog Computing Security Challenges and Future Directions.” *IEEE Consumer Electronic Magazine*, 92–96.

Stojmenovic, Ivan, Sheng Wen, Xinyi Huang, and Hao Luan. 2015. “An Overview of Fog Computing and Its Security Issues.”

Yi, Shanhe, Zhengrui Qin, and Qun Li. 2015. “Security and Privacy Issues of Fog Computing: A Survey.” *Springer International* 685–95.

Zaheer, Bushara, and Ali Munam Shah. 2017. “Fog Computing: Security Issues, Solutions and Robust Practices.” in *Proceedings of the 23rd International Conference on Automation & Computing*. Hudders Field, UK: University of Hudders Field.