Towards a Threat Model for Fog Computing

Yasser Karim
Department of Computer Science
University of Alabama at Birmingham
Birmingham, AL
Email: yasser@uab.edu

Ragib Hasan
Department of Computer Science
University of Alabama at Birmingham
Birmingham, AL
Email: ragib@uab.edu

***Abstract*—In recent years, the addition of billions of Internet of Thing (IoT) device spawned a massive demand for computing service near the edge of the network. Due to latency, limited mobility, and location awareness, cloud computing is not capable enough to serve these devices. As a result, the focus is shifting more towards distributed platform service to put ample computing power near the edge of the networks. Thus, paradigms such as Fog and Edge computing are gaining attention from researchers as well as business stakeholders. Fog computing is a new computing paradigm, which places computing nodes in between the Cloud and the end user to reduce latency and increase availability. As an emerging technology, Fog computing also brings newer security challenges for the stakeholders to solve. Before designing the security models for Fog computing, it is better to understand the existing threats to Fog computing. In this regard, a thorough threat model can significantly help to identify these threats. Threat modeling is a sophisticated engineering process by which a computer-based system is analyzed to discover security flaws. In this paper, we applied two popular security threat modeling processes – CIAA and STRIDE – to identify and analyze attackers, their capabilities and motivations, and a list of potential threats in the context of Fog computing. We posit that such a systematic and thorough discussion of a threat model for Fog computing will help security researchers and professionals to design secure and reliable Fog computing systems.**

***Index Terms*—Computer Networks, Internet, Network Security, Edge computing, Middleware**

I. Introduction

The rapid emergence of the Internet of Things (IoT) is bringing upfront some new challenges. The billions of connected devices are producing an enormous amount of data every second. All of these devices are also in need of computing resource such as computation power, memory, storage, etc. as they are resource constrained. With the assistance of Cloud infrastructure, these issues can be resolved up to a certain point. It is estimated that by the year 2024, the number of the total connected device will be more than 75 billion [1], which is almost double the current total. Therefore, providing services for these many devices using only the Cloud will be very difficult. Besides, latency sensitive application such as a smart vehicle, gaming as a service, instant face recognition, etc. are already suffering because of the distance issue between the Cloud data center and end-user device. To tackle this issue, researchers and industry stakeholders are bringing the concept of Fog/Edge computing, which brings the computation power much closer to the edge network. As the Fog/Edge shares some core characteristic with the Cloud, malicious entities will also target the Fog/Edge infrastructures. New security threats are rising as the Fog/Edge is more distributed than the Cloud.

Fog/Edge computing inherits similar types of threats like Cloud computing. Because of virtualization technology, the Fog/Edge also has to face the threats due to co-tenancy. Also, connection over network brings other communication threats such as eavesdropping, sniffing, jamming, etc. Along with these, the Fog/Edge has to confront new threats such as resource exhaustion attack because a Fog/Edge node or server is not as resourceful as Cloud data centers. The Fog/Edge brings another layer between the Cloud and the Client, which opens up a few more attack surfaces for the adversaries. Therefore, Fog/Edge computing requires an extended security threat model which will contain all the attributes from the Cloud computing threat model as well as the newer threats that challenges the system.

One of the core objectives of Fog/Edge computing is to mitigate the latency issue by putting the infrastructure much closer to the end user. Because of this, a Fog/Edge server is situated in a much higher risky position. A Cloud data center usually centered in a single location with high-security surveillance. Also, a Cloud data center usually equipped and capable with enough resource to face security threats. Therefore, security in a Fog/Edge node is much more challenging. A Fog/Edge server also works as a cache between the Cloud and the end user. Therefore, cache attacks are highly possible, targeting a node with security flaws. Fog services are mainly designed to serve the nearest user. As a result, user privacy, especially related location is highly susceptible to malicious attack. It is quite apparent that Fog computing has to address more security threats than Cloud computing, which are more challenging with respect to Cloud. On this regard, a proper and complete security threat model is essential for designing a security framework in a Fog/Edge environment. A threat model can provide insight to the developer while designing such applications.

Towards building a threat model for Fog computing, several aspects have to be adopted from Cloud computing. The attack surface of a Fog/Edge is similar to a Cloud. Fog also uses virtualization techniques to provide services such as compute, storage, and memory. The experts proposed several threat model [2]–[4] for Cloud computing. Also, a threat model for virtualization techniques can provide what kind of security threats come into play because of this. Also, a Fog/Edge node can also work as a gateway for IoT devices. These devices are often in different communication protocols as well as mediums. Therefore, a multi-protocol environment brings a different kind of threats towards a node or server. NIST [5] provides a conceptual model for Fog computing but lacks in

978-1-7281-3885-5/19/$31.00 ©2019 IEEE

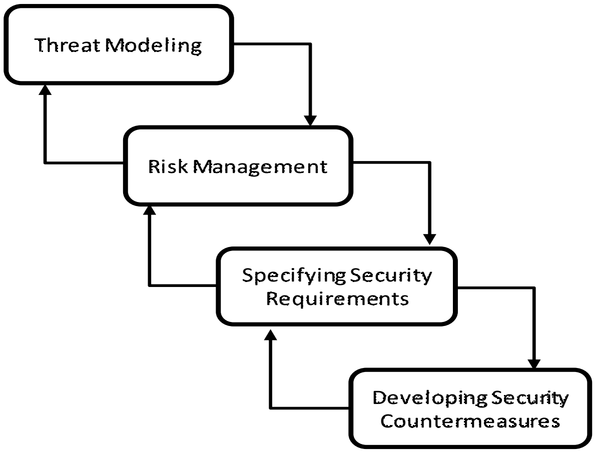
Threat Modeling
Risk Management
Specifying Security Requirements
Developing Security Countermeasures

Fig. 1: Threat Modeling

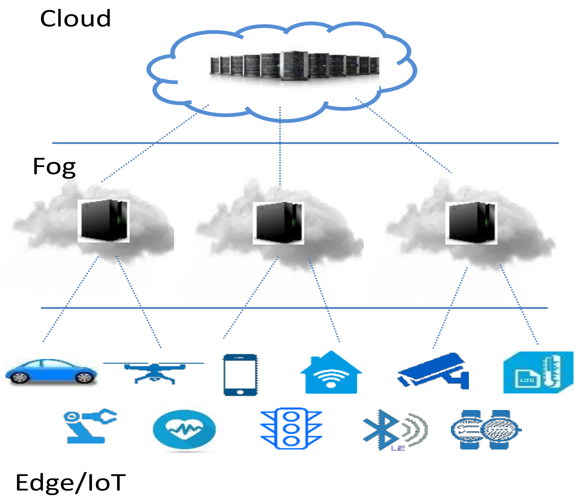

Fig. 2: Fog Overview

outlining a security model for it. Besides, the trade-offs of implementing such security measure need to be addressed also. For example, for better network security, all Fog node can be equipped with hardware level intrusion detection system but it will reduce the portability of each node as well as increase the power consumption. With better security threat model, hardware level intrusion detection may not be required in every node of a Fog network.

Thus, it is very important to comprehend all the threats and vulnerabilities in Fog computing. Before designing any protection or security system, one must understand all kinds of threats to determine security countermeasures. With this respect, Threat modeling is a structured engineering technique to recognize all possible threats and security issues in a complex system. In literature, several works have discussed security and privacy issues of Fog computing [6]–[10]. To our best of knowledge, neither of existing works discuss these issues with respect to a threat modeling approach.

In this paper, we thoroughly study the security threats of Fog computing through the lens of threat modeling process. The contribution are as follows:

1) We discuss the two threat model process - CIAA (Confidentiality, Integrity, Availability, and Authentication) and STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privileges), from Fog computing perspective.
2) We provide a comprehensive threat modeling process using both model.
3) We present the threats that are identified by these processes in a organized way.

The rest of the paper is organized as follows: Section II describes the background and architecture of Fog platform. We describe both threat modeling process in Section III. Section IV presents the related work. We conclude in Section V.

II. Background

In this section, we briefly describe the similarities of Fog computing with other similar paradigms. It has been already established that the main goal of the Fog (Figure 2) is to bring Cloud-like service at the edge of the network, closer to the end devices. Therefore, it is evident that the Fog reuses many concepts from Cloud, Edge, IoT, and Mobile Computing. We provide a concise definition and characteristics of these concepts to give a better understanding of the Fog. We also provide a brief architecture of the Fog.

A. Cloud

The term Cloud [11] refers to the core of Cloud computing– the large data centers which are responsible for providing different facets of this paradigm. These data centers contain thousands of physical machines. With the Internet connection, three primary services: a) Infrastructure b) Platform and c) Software are provided to the user. Usually, these data centers are located in safe and secure locations, far from the end user. Cloud frees the enterprises and their end users from the specification of many details, such as storage resources, computation limitation and network communication cost. In recent years, with the rise of real-time applications such as smart vehicular network, distributed artificial intelligence service, ultra-high definition video, the distance between the Cloud and the end user is causing disruptions in providing quality services.

B. Multi Access Edge Computing

Mobile or Multi Access Edge Computing [12] is very similar to Cloudlet except that it is primarily located in mobile base stations. It is a framework for providing business oriented, Cloud computing platform within the radio access network at the proximity of mobile subscribers to serve to delay sensitive, context-aware applications.

C. Internet of Things (IoT)

The Internet of Things (IoT) [13] has emerged as a popular paradigm in recent years. At a conceptual level, IoT represents a global information network of our everyday devices (e.g., home appliances, automotive), and provides an intelligent framework with the property of sensing capability, contextual awareness, and device autonomy. The connectivity among these devices enables them to communicate smartly to each other or to us. Connected devices embedded with sensors or actuators perceive their surroundings and are smart enough to understand the observed data (what is going on around them) and perform accordingly. To achieve this, the sensed data is processed by the smart device itself, or at a device hub (e.g., gateway), or in a Cloud. Devices might take a decision autonomously based on the processed data, or might propagate the information to the users to receive the best decision from them.

D. Fog Architecture

A Fog computing platform can be composed of the following components. We briefly explain several components [14].

*1) **Authentication and Authorization**:* One of the core components of a Fog node is authentication and authorization. This module maintains the accessibility of Fog computing services and resources. All of the requests for services and resources should be authenticated and authorized. This module is the gateway of all types of security because all kinds of communication have to pass through it. Fog computing introduces different types of security issues which require new types of authentication and authorization techniques. [15].

*2) **Management for Offloading**:* This component is very vital because it handles the offloading task from both client devices and the cloud. The primary purpose of Fog computing is to provide computing service with very less latency. Thus, this component is responsible for maintaining low latency. In [15], various techniques of offloading management are discussed. There are three main issues are need to resolve: i) what type of information are necessary for offloading decision, ii) how to divide the applications and resources, and 3) how to find an optimal or sub-optimal solution within a specified period.

*3) **Location Services**:* One of the main advantages of Fog computing is it can provide highly targeted service based on location information. In most cases, fog nodes are designed to serve users who are proximal to their location. Thus, the location service module keeps track of neighboring nodes as well as the end users with proper credentials.

*4) **System Monitor**:* System monitor is an essential part of cloud setup. It is responsible for keeping track of workload, resource usage, consumption of power, etc. for better management. In a Fog node, system monitor also requires to do similar work with higher efficiency because Fog nodes are equipped with limited resource. Without a better monitoring system, a fog node will fail to serve appropriate users.

*5) **Resource Management**:* The resource management module will be responsible for allocation of resources and distribution of idle resources. It will maintain the list of other Fog nodes which are willing to share their resources. If there are unused resources, this module can share with other nodes.

*6) **VM Scheduling**:* A fog node provides its services via Virtual Machines (VM). This module is responsible for scheduling the launch of VMs. Based on system usage, workloads, locations, mobility, etc. it generates a plan for VM launch. Performance of this module directly affects the performance of a fog node.

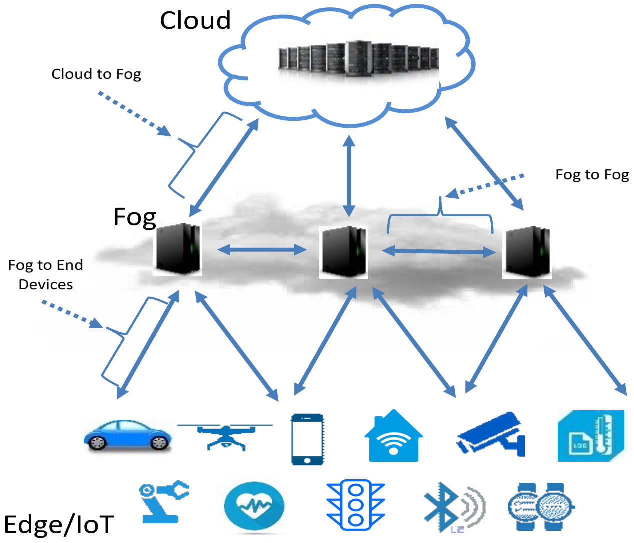

Fig. 3: Attack Surfaces

III. Threat Modeling Process for Fog

Threat modeling requires systematic well engineered process which can be followed multiple times. All threats can not be discovered in one pass. An attacker has to simple find one security gap to comprise the system. Thus a well designed systematic process is required which consider several things while building a model. In this section, We will discuss important steps in threat modeling process and describe each of them to understand the work-flow.

A. Attack Surfaces

Attack interface increases in many folds in Fog environment. Three tier architecture (Figure 3) is the core framework in Fog computing. We can classify attack surfaces in three categories. They are - *1) Cloud to Fog 2) Fog to Fog 3) Fog to End Device*

*1) **Cloud to Fog**:* In Fog computing architecture, the Cloud is the top layer. A Fog node communicates with Cloud for offloading preprocessed data and more heavy computation which can not be done in a Fog node. This Cloud to Fog communication interface is one of the attack surfaces that can be targeted by the adversaries. An attacker can compromise both the services.

*2) **Fog to Fog**:* In Fog environment, the nodes also communicate in between them. From resource sharing to access delegation, Fog nodes constantly interact with each other for better services. An adversary can launch Man-in-the-Middle attack to eavesdrop between two Fog nodes.

*3) **Fog to End Device**:* The bottom layer in Fog computing architecture is the Fog to End Device. In Fog network, each Fog node provides services to end or client device. It can act as a smart gateway for the devices in the edge network. Therefore, this communication fold also very lucrative towards the adversaries. Attackers can act as deceiving end device and launch denial of service attack against the Fog nodes. On the other hand, a Fog node can be compromised and can host malicious services which can steal client devices' information.

B. Attacker Targets

The next step in the threat modeling process is to identify the attacker's goals. By doing this, we will be able to understand what part of the system needs to be guarded. Usually, the attacker's goals are the system asset especially system resources from which they can be benefited. These assets are the prime reason for launching an attack. Some of these assets are as follows: *1) Computation Power*, *2) Virtual Memory*, *3) Physical Memory*, *4) Data Storage*, *5) Data Blocks*, *6) Virtual Storage*, *7) Log Files 8) Metadata*

C. Access Entry Point

In the next step, entry points should be considered in the discussion. These are used by the attackers to gain access to the system. For examples, an open socket on any Fog node server can be used to gain entry in the system. Identifying access entry point is very important. The main security policies will be implemented around these points. With a thorough study, we can find the following list of access entry points that can be exploited by adversaries:

- Access a Fog node from a compromised end devices.
- Open sockets and ports in a Fog node.
- Compromise a Fog node via trusted access.
- Coordinated and sophisticated process from a Cloud.
- Physical access to a Fog node.

D. CIAA Threat Model Process

Any computer-based system must consider the following four criteria: confidentiality, integrity, availability, and authentication (CIAA) [16]. This process is called CIAA process for threat modeling. In this section, we present and categorize different types of attack on Fog-based system into different groups so that we can address them by CIAA protection method. At first, the application of each CIAA features concerning Fog-based system was described, followed by a list of specific attack instances. We have tried to put a thorough list of possible scenarios but in future new types of attacks are possible on Fog-based system. Although they are new types of attacks, they can be fallen into the four categories of CIAA process.

For better understanding, we considered physical attacks as a separate group from CIAA. Physical attacks are not part of computer security. This attacks cannot be defended using regular computer security policies. These should be dealt with by organizational structure for physical security. We are considering them in our discussion each physical attack also violates multiple CIAA aspects.

1) ***Confidentiality Attacks:*** This type of attacks attempt to gain information or to access certain resource from the system without proper authorization. An attacker can achieve higher authorization by snooping onto legit user information or exploiting very weak security schemes via open and unguarded ports and sockets. With theses privileged access, and an adversary can steal valuable information or use the resources for other purposes which will impact the service. On the side, an attacker can steal information without this kind of accessibility. They can snoop into communication and look for sensitive information. We identify the following confidentiality attacks on Fog-based systems:

- *Sniffing Network Traffic:* Fog-based system highly rely on network communication. Therefore, an attacker can sniff network channels for revealed and exposed data.
- *Snooping on Buffered Information:* One of the core objectives of Fog node is to act as an intermediate buffer between the end devices and the cloud. It stores lots of information in volatile memory as non volatile memory such as hard disk for short period of time. These buffered information could hold sensitive information of a client device. Adversaries can look into these buffer systems.
- *Memory Accusation:* A Fog node provides computing service such computation, memory, and storage for an client device. Client devices can run important workload using these services. After finishing a particular process, the Fog system unallocated the memory from particular client device. Until this unallocated memory assigned to some other client, this memory portion holds the previous data. An attacker can take advantage of this window and can steal information from this deallocated memory by using any kind of memory accusation tools.
- *System Profiling:* Fog nodes are mini server with lots of ports and sockets. It is highly possible that some of these ports or sockets can be unprotected. An attacker can exploit these unguarded and launch an system profiling attack. She can monitor specific ports such as http ports or database access ports for particular pattern. Using these pattern, the attacker can identify sensitive information.

2) ***Integrity Attacks:***

- *Network Communication Jamming:* A Fog-based system use different types of communication medium for providing and receiving services. It uses wired network for connecting with the cloud on the other hand it might use both wired and wireless medium for providing services to the client devices. An attacker can launch jamming attack in these mediums to damage the integrity of the packets. She can flood the wired network or broadcast in same wireless frequency. She can capture particular packets and modify those on the fly.
- *Modifying Metadata* Fog is a highly virtualized platform. For better performance, these platforms has to keep a lot of logs. Therefore, a targeted attack on these metadata saved on these log can be devastating. An adversary can snoop into the system and tamper a log file which could easily disrupt the system. For example, by modifying database log file, the main database can get corrupted which will not able to provide any service.
- *Memory Tampering* As mentioned in confidentiality attacks, an attacker can acquire memory and read information from it using any kind of memory accusation tool. With proper security privilege they can access storage memory blocks and tamper the stored data.

*3) **Availability Attacks**:*

- *Exhausting Log Space:* Virtualized systems such as Fog have to use log files for maintenance activity. These log files also need to be backed up time to time for better recovery. A Fog node could fail if does not have enoug space for creating log files. An attacker can attempt to write garbage values on these files and consume the log space. If the space is overrun before the backup the services will be interrupted.
- *Exhausting Buffer Space:* Buffer space are used for short period of time. It stored most wanted information to reduce the latency. An attacker can create a large number of unnecessary files and request them continuously to keep them in the buffer. Also, attacker can request buffer space with unresponsive connection similar to syn flood attack in TCP/IP communication.
- *Network Communication Disruptor:* Any service based platform depends on network communication. Adversaries can jam these communication medium using different techniques. They can flood the Ethernet network with dummy packets which will create network congestion. They can jam the wifi channel by broadcasting in the same frequency. All of these, will hamper the service provided by the Fog nodes.
- *Virtual Resource Disruption* A Fog node has limited resource in comparison with a Cloud. It provide similar service like a Cloud with less physical resources. Therefore, an adversary can request multiple resource and keep them idle. As a result, those resource will be utilized by an actual user. It will create an disruption in providing virtual resources.

*4) **Authentication Attacks**:*

- *User Impersonation:* Fog provides its services to a client device by authenticating that client. An attacker can impersonate an user by retrieving her credentials or exploiting niches in authentication scheme. Once authenticated, the attacker gains access in the system and use services for ill activity.
- *Device Impersonation:* Some of the services of a Fog-based system are provided for specific devices. An attacker can use different device to impersonate as certain device to authenticate itself. It will allow the attacker to use those device specific services for malicious activity.

*5) **Physical Attacks**:*

- *Power Disruption:* One of the challenges of physically securing a Fog node is that a Fog node can often be located at public space where security is minimum. Besides, Fog node like this often powered from general public power supply. Therefore, adversaries can disrupt the power supply which will make the Fog node unavailable for service. In most cases, a Fog node will have battery backup but long term power disruption can drain the whole battery backup.
- *Communication Disruption:* Fog nodes are usually connected to a wired network or a wireless network. As these nodes are situated near the edge network, an attacker simply hamper the communication by physically damaging the network communication. She can cut off the network line or break the communication antenna.
- *Device Theft:* As most of the Fog nodes are with minimum security, it is highly possible that components of a Fog node can be stolen by the adversaries. Specially, storage units will be the prime target. An attacker can open the server and simply detach the storage unit. As a result, the Fog node will not able to provide service as well as device information can also be retrieved from that storage medium. Also, an attacker can simply attach a USB memory stick and steal information or install malware on the Fog node.
- *Physical Destruction:* Along device theft, a Fog node can be physically damaged by the adversaries. One can simply damaged a Fog node by hitting it with heavy object or putting it in fire or pouring liquid like water. These act can easily cripple a Fog node permanently.
- *Hardware Based Attack:* As mentioned earlier, an attacker can easily attach a USB stick and install malicious software. Also, an attacker can connect to Fog node directly connecting it via its own terminal at the location. Even if the Fog node does not have any terminal, attackers can attach its own device to it and launch attack.

E. STRIDE Threat Model Process

STRIDE threat model is a popular threat model which is mainly developed from the perspective of a developer [17]. Every computer based system is driven by software. While designing security for application, developers and software engineers must consider security threats as early in Software Development Life Cycle. STRIDE threat model can provide assistance in this regard. STRIDE stands for as follows: *1) **S**poofing, 2) **T**ampering, 3) **R**epudiation, 4) **I**nformation Disclosure, 5) **D**enial of Service, 6) **E**levation of Privileges*

In this section, we will follow the STRIDE threat model and will analyze the threats of Fog computing using this model. We will also show similarities between the CIAA and STRIDE threat model.

*1) **Spoofing**:* It refers to a situation in which an attacker impersonate as a legitimate user to gain an illegitimate advantage. An attacker can use phishing techniques to acquire a valid credentials. Also, adversaries can advantages of security flaws such as SQL injection to authenticate himself. A Fog system also is susceptible for spoofing attack. Attackers can use compromised end user device to authenticate itself correctly. They can also use brute force method to find legitimate credentials for gaining access. Spoofing attacks are similar to authentication attacks of the CIAA. In spoofing, for Fog-based system, another issue is the location. Fog services are highly targeted for a certain location. Adversaries can spoof their location to authenticate from a different location. As a result, they can exploit this for other malicious activity.

*2) **Tampering**:* In this type of attack, the main objective is to modify data or processes. Attackers snoop in communication channels or listen to unguarded ports and sockets. Once they identify certain packets, they modify the main contents or the header and disrupt the communication. This type of attack align with integrity attack of the CIAA, A Fog node is in the line for tampering attack. It uses different types of communication medium in which adversaries can steal sensitive information.

*3) **Repudiation**:* It refers to the situation where action is denied by its perpetrators. This type of attack occur when system lacks proper logging system. Without keeping important activity in check can open a path for the adversaries to conduct devastating act such as deleting all records from the database. Also, attacker can consume the log space so that the system can not keep track of some incidents. Repudiation makes harder for identifying the main culprits or how things actually happened.

*4) **Information Disclosure**:* It occurs when data is leaked or breached. It can happen when the data is transferring or stored in a storage medium or from a process. An attacker sniff network communication to read data which are not encrypted. They can listen a unprotected port such as SQL database port when SQL call is occurring. If the data is not encrypted properly, adversaries can easily find the information they are looking for. This type of attack is similar to confidentiality attacks of the CIAA.

*5) **Denial of Service**:* It is one of most popular and dangerous type of attack. Main objective of this attack is to disrupt the service. It is an availability attack. An attacker can launch SYN flood attacks against a particular Fog node to consume its buffer space. It can make the node unresponsive. As the Fog node provide computation, memory, and network service, adversaries can request chunk of resources and do nothing with those. As a result, the node will not able to serve appropriate user. The storage medium, specially the metadata and log space can also be consumed with coordinated techniques which will also hamper the service. This type of attack concerned with availability attack.

*6) **Elevation of Privileges**:* This type of attack focuses on gaining access to some resource without proper authorization. In this kind of scenario, the attacker might have legitimate credential for authentication but she does not have proper authorization. An user can take advantage of a buffer overflow to acquire higher level privilege. Also, with co-tenancy, an attacker can snoop into others resources and access them by exploiting weak authorization system.

F. Fog vs Cloud

Fog computing bears a lot of similarities with cloud computing. Both are highly virtualized platform for providing computing service as computation capability, memory, storage, network support etc. Therefore, the question arises - “What is the difference between the threat models of the Fog and the Cloud?”. In Table I, we provided differences between the threat model of Fog and Cloud.

IV. Related Work

Threat modeling is an important task in securing a computer based system. Without proper threat modeling, one can not properly secure a system. In literature, several works have done with regard to threat modeling. Prior research works showed significant amount of works have been conducted with security and privacy issues in fog computing. To best of our knowledge, we could not find any work that follows a proper threat modeling process like CIAA or STRIDE for building a complete threat model. In this section we discuss similar works with regard to this paper.

Martin et al. [6] provided an overview of the security landscape of OpenFog architecture. In this paper, OpenFog Security Workgroup offered an overview of the security landscape of OpenFog architecture as well as a survey of the functional requirements and the technical approaches. Bonomi et al. [7] presented the characteristics of Fog computing and put a discussion why this paradigm is ideal for critical Internet of Things services and applications. Yi et al. [8] surveyed security and privacy challenges besides those inherited from Cloud computing. Madsen et al. [9] discussed about the reliability issues in existing paradigm and put a comparison with Fog computing to demonstrate usefulness and resilience of Fog paradigm. Lee et al. [10] presented a discussion about the security and privacy issues of Fog based IoT environments.

Roman et al. [18] analyzed the security threats, challenges, and mechanisms in mobile edge computing with respect to Fog. Sun et al. [19] proposed a hierarchical Fog computing architecture in each Fog node to provide flexible IoT services while maintaining user privacy. The proposed framework brought the computing resources close to IoT devices so that the traffic in the core network can be alleviated and the end to end delay between computing resources and IoT devices is minimized. The author envisioned mobile network base station as a wireless gateway to all the IoT devices. The core of EdgeIoT is implemented using SDN structure. The core network is controlled by open flow controller which is responsible for network management operation. Shi et al. [20] introduced the definition of edge computing followed by several case studies.

Threat modeling process is a well established method. Several prior works described this processes thoroughly. Hasan et al. [16] presented a threat modeling for a storage system using CIAA threat model. Fog has similarities with cloud. In [2], described the threat modeling techniques for the cloud computing and identified the threats via this process. Alhebaishi et al. [3] conducted a comprehensive threat modeling for cloud data center infrastructure. Kamongi et al. [4] proposed a architecture named Nemesis for threat modeling automatically for cloud system.

From our understanding, our work is first attempt to generate threat model for Fog computing using sophisticated and organized threat modeling process. Our work is novel in nature and it uses multiple threat modeling process (CIAA and STRIDE).

V. Conclusion

Fog-based system brings unique security challenges in the table for security researchers. With a systematic and thorough threat model, security issues with regards to these challenges can be identified. Threat modeling process provides a systematic way to discover security problems of a computer

TABLE I: Differences between the threat model of Fog and Cloud

Topic	Cloud	Fog
Communication surfaces	In cloud platform, it has only one communication surface. The cloud only has to communicate with user or users' devices. All devices or users outside the data center are at the same level. Therefore, attack surfaces of all are at the same level.	A typical fog node has to maintain communication with both end user and the cloud. Besides, fog nodes themselves keep communication between them. It is obvious that there are at three different communication surfaces to consider in threat model process
Communication medium	A cloud infrastructure maintain its communication with outside via wired network. An user can connected via wifi to a cloud service but eventually the packets will be transfered over either ethernet or fiber optic network to cloud.	In fog network, fog node is typically equipped with both wired network as well as wireless network. Fog nodes maintain communication with cloud mainly using wired connection. On the other side, fog nodes use both wired and wireless medium for communicating with other nodes and end users
Physical threats	A cloud infrastructure is usually heavily guarded with top notch security. Most of these data centers keep their computing hardware under one roof. This data centers have multiple back up power sources. Thus physical threat is very non existence	Fog nodes are highly distributed and they are located in various location. Some nodes can be located inside a hospital, some other can be found near road side. Because of this, guarding every fog node with heavy security is quite impossible. That is why physical threat is a concern for fog threat model.
Severity of DoS attack	The cloud is a high value target for DoS attack. Usually, the cloud is well equipped with resources. Therefore, a cloud infrastructure could have its own mechanism against DoS attack.	A fog node is not capable enough to defend against a sophisticated DoS attack. This node will require outside assistant to defend a DoS attack. Usually, multiple Fog nodes coordinate with each to defend a DoS attack. Also, in Fog networks some Fog nodes work as controller which monitor the traffics to detect DoS attacks early.
Location awareness	A cloud data center static in nature. It is not mobile in nature. The cloud services, in most cases, are available at any location and do not have to consider proximity of the end user device.	A fog node is designed and deployed at the edge of the network to serve the users who are proximal to the node. Also, some fog nodes can be mobile in nature (f.g. nodes in trains and aircrafts)

based system. In this paper, we focused on building a threat model for Fog computing paradigm. We used two widely popular methods. The CIAA methods are the traditional threat model process and cover the core concepts of security. On the other hand, STRIDE is designed from developers point of view. We presented both of these threat models thoroughly and discussed each instances elaborately. This study will help us to picture the security threats in Fog computing and point direction towards the places where we should put high security concerns. For future work, we focus on building a prototype of a Fog testbed addressing all the security concerns mentioned in this work.

Acknowledgment

This research was supported by the National Science Foundation through awards DGE-1723768, ACI-1642078, and CNS-1351038, and by the National Institute of Health grant 1R21HD095270-01.

References

[1] statista, "Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions)," https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/, 2019.

[2] J. A. Ingalsbe, D. Shoemaker, and N. R. Mead, "Threat modeling the cloud computing, mobile device toting, consumerized enterprise-an overview of considerations." in *AMCIS*, 2011.

[3] N. Alhebaishi, L. Wang, S. Jajodia, and A. Singhal, "Threat modeling for cloud data center infrastructures," in *International Symposium on Foundations and Practice of Security*. Springer, 2016, pp. 302–319.

[4] P. Kamongi, M. Gomathisankaran, and K. Kavi, "Nemesis: Automated architecture for threat modeling and risk assessment for cloud computing," in *Proc. 6th ASE International Conference on Privacy, Security, Risk and Trust (PASSAT)*, 2014.

[5] M. Iorga, L. Feldman, R. Barton, M. Martin, N. Goren, and C. Mahmoudi, "The nist definition of fog computing," National Institute of Standards and Technology, Tech. Rep., 2017.

[6] B. A. Martin, F. Michaud, D. Banks, A. Mosenia, R. Zolfonoon, S. Irwan, S. Schrecker, and J. K. Zao, "Openfog security requirements and approaches," in *Fog World Congress (FWC), 2017 IEEE*. IEEE, 2017, pp. 1–6.

[7] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, "Fog computing and its role in the internet of things," in *Proceedings of the first edition of the MCC workshop on Mobile cloud computing*. ACM, 2012, pp. 13–16.

[8] S. Yi, Z. Qin, and Q. Li, "Security and privacy issues of fog computing: A survey," in *International conference on wireless algorithms, systems, and applications*. Springer, 2015, pp. 685–695.

[9] H. Madsen, B. Burtschy, G. Albeanu, and F. Popentiu-Vladicescu, "Reliability in the utility computing era: Towards reliable fog computing," in *Systems, Signals and Image Processing (IWSSIP), 2013 20th International Conference on*. IEEE, 2013, pp. 43–46.

[10] C. Yoon, T. Park, S. Lee, H. Kang, S. Shin, and Z. Zhang, "Enabling security functions with sdn: A feasibility study," *Computer Networks*, vol. 85, pp. 19–35, 2015.

[11] P. Mell, T. Grance *et al.*, "The nist definition of cloud computing," 2011.

[12] T. Taleb, K. Samdanis, B. Mada, H. Flinck, S. Dutta, and D. Sabella, "On multi-access edge computing: A survey of the emerging 5g network edge cloud architecture and orchestration," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 3, pp. 1657–1681, 2017.

[13] F. Xia, L. T. Yang, L. Wang, and A. Vinel, "Internet of things," *International Journal of Communication Systems*, vol. 25, no. 9, pp. 1101–1102, 2012.

[14] S. Yi, Z. Hao, Z. Qin, and Q. Li, "Fog computing: Platform and applications," in *2015 Third IEEE Workshop on Hot Topics in Web Systems and Technologies (HotWeb)*. IEEE, 2015, pp. 73–78.

[15] C. Dsouza, G.-J. Ahn, and M. Taguinod, "Policy-driven security management for fog computing: Preliminary framework and a case study," in *Information Reuse and Integration (IRI), 2014 IEEE 15th International Conference on*. IEEE, 2014, pp. 16–23.

[16] R. Hasan, S. Myagmar, A. J. Lee, and W. Yurcik, "Toward a threat model for storage systems," in *Proceedings of the 2005 ACM workshop on Storage security and survivability*. ACM, 2005, pp. 94–102.

[17] I. Lütkebohle, "BWorld Robot Control Software," http://aiweb.techfak.uni-bielefeld.de/content/bworld-robot-control-software/, 2008, [Online; accessed 19-July-2008].

[18] R. Roman, J. Lopez, and M. Mambo, "Mobile edge computing, fog et al.: A survey and analysis of security threats and challenges," *Future Generation Computer Systems*, vol. 78, pp. 680–698, 2018.

[19] X. Sun and N. Ansari, "Edgeiot: Mobile edge computing for the internet of things," *IEEE Communications Magazine*, vol. 54, no. 12, pp. 22–29, 2016.

[20] W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu, "Edge computing: Vision and challenges," *IEEE Internet of Things Journal*, vol. 3, no. 5, pp. 637–646, 2016.