Towards a Threat Model for Vehicular Fog Computing

Mohammad Aminul Hoque
Department of Computer Science
University of Alabama at Birmingham
Birmingham, USA
mahoque@uab.edu

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

***Abstract*—Security is a huge challenge in vehicular networks due to the large size of the network, high mobility of nodes, and continuous change of network topology. These challenges are also applicable to the vehicular fog, which is a new computing paradigm in the context of vehicular networks. In vehicular fog computing, the vehicles serve as fog nodes. This is a promising model for latency-sensitive and location-aware services, which also incurs some unique security and privacy issues. However, there is a lack of a systematic approach to design security solutions of the vehicular fog using a comprehensive threat model. Threat modeling is a step-by-step process to analyze, identify, and prioritize all the potential threats and vulnerabilities of a system and solve them with known security solutions. A well-designed threat model can help to understand the security and privacy threats, vulnerabilities, requirements, and challenges along with the attacker model, the attack motives, and attacker capabilities. Threat model analysis in vehicular fog computing is critical because only brainstorming and threat models of other vehicular network paradigms will not provide a complete scenario of potential threats and vulnerabilities. In this paper, we have explored the threat model of vehicular fog computing and identified the threats and vulnerabilities using STRIDE and CIAA threat modeling processes. We posit that this initiative will help to improve the security and privacy system design of vehicular fog computing.**

***Index Terms*—vehicular fog, threat model, threat, attack, adversary, security**

I. Introduction

Over the past few years, various vehicular network paradigms have been proposed to enhance road safety, driving assistance, and situational awareness on the road such as Vehicular Ad-hoc Networks (VANET) [1], Internet of Vehicles (IoV) [2], and Vehicular Cloud (VC) [3]. Vehicles are becoming smart with the ability to communicate with other entities through the Internet and wireless networks. Business Insider has predicted in a report that there will be 380 million connected cars on the road by 2021 [4]. Tech giant Google has launched their self-driving car project [5]. All of these demonstrate the improvements in vehicle intelligence. With the anticipated improvement of vehicle capabilities in the near future, these resources can be organized into pervasive networks for numerous applications related to road safety and driving assistance while on the move. Vehicular fog [6] is the latest vehicular networking paradigm which provides location-aware and latency-sensitive services to the vehicles in close proximity. Security and privacy of this paradigm are important because security breaches and attacks on this architecture may cause adverse incidents such as road accidents. To design a better security system, we must understand the threats and vulnerabilities of vehicular fog architecture. A complete threat model provides details about the security of this paradigm.

Threat modeling refers to a proactive and systematic approach to analyze all the aspects of security, threats, and vulnerabilities of a system regardless of their severity and chance of occurrence [7]. This helps to understand the attack vector, profile of the attacker, valuable assets of the system, and the potential mitigation strategies based on the known security solutions. Understanding the threat model is important before designing a security solution because there can be some trade-offs in performance and security requirements in vehicular fog computing. Hence, the security solution must consider the design and architecture of the system and meet the security requirements to avoid random usage of security technologies [8]. To design the threat model, we need to think from the perspective of an attacker to figure out what are the valuable assets and potentially vulnerable points of the system [9]. Moreover, the motives behind the attack make the threat modeling problem more interesting. Security and privacy issues of vehicular fog architecture have not been explored widely yet. Hence, the security definition and requirements are not clear in this context. Most often, the solution to a security problem is designed based on intuition, brainstorming, or recent attack incidents which are not systematic approaches to address the security flaws. The security solution must be compatible with system architecture and requirements after proper identification of security requirements of that particular system. The threat model will help to validate the assumptions from brainstorming and justify the countermeasures implemented in the security solution. Hence, the vehicular fog architecture requires a complete threat model for designing security solutions.

In this paper, we have analyzed all the components of a complete threat model of vehicular fogs. We have also examined the threat models of other vehicular network paradigms and designed the threat model for vehicular fog, considering its unique security issues. We expect that this threat model will help researchers to design better security solutions in the future.

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

Contribution: The contributions of this paper are as follows:

1) We have analyzed the challenges and requirements for protecting vehicular fogs.
2) We have provided a complete threat model for vehicular fog computing.
3) We have identified the potential threats and vulnerabilities based on two popular threat modeling processes.

Organization: The rest of the paper is organized as follows: Section II provides the background of threat modeling and vehicular fog computing. Sections III and IV identify the assets and entry points respectively. Section V defines the attacker model. Section VI presents the threats and vulnerabilities of vehicular fog using two threat modeling processes. Section VII identifies the mitigation strategies. Section VIII contains the related works and we finish with conclusions in Section IX.

II. Background

In this section, we provide background information on threat modeling and vehicular fogs. Before starting threat modeling, it is crucial to explore the system thoroughly. This will help to understand the component details, identify related dependencies among them, and make necessary assumptions.

A. Threat Modeling

A proper threat model refers to a systematic process of identifying and prioritizing the potential threats and vulnerabilities of a system from the attacker's point of view [9]. It is a continuous process to enhance the system security according to the threat model analyzed by both the security experts and developers. Threat modeling helps to assess the risk of an attack and decide whether to solve it immediately or ignore safely. Threat modeling consists of five steps or components where each of them are important and complement each other to provide a complete security assessment of the system [7]. The components of threat modeling are as follows:

Assets: The attacker always targets some assets of a system to gain which she is interested in. Before designing a security solution, it is important to understand what are the valuable assets of the system, which may attract the attacker.

Entry points: Entry points refer to the vulnerable or untrusted points through which the attackers can enter into the system.

Attacker model: The attacker model explains the characteristics of the attackers. It defines who the attackers are, their attack motives, and capabilities.

Threats and vulnerabilities: The most important part of threat modeling is to identify the threats and vulnerabilities of the system. There are several popular threat modeling processes which make the analysis structured by categorizing the threats and vulnerabilities.

Mitigation strategies: Mitigation strategies refer to techniques to prevent potential attacks and solve the vulnerabilities with known security solutions to enhance the security of the system.

B. Vehicular Fog Conceptual Overview

In vehicular fog architecture, interested vehicles can serve as fog nodes to share their resources with other vehicles in close proximity. Both parked and moving vehicles can serve as vehicular fog nodes. The whole architecture is controlled by one or more Road Side Units (RSUs) who are responsible for managing and allocating the available resources among the users. Fog nodes are required to communicate with the RSUs and other vehicles in that vehicular fog network through the wireless communication channel. The vehicles communicate with each other by vehicle-to-vehicle (V2V) communication through Dedicated Short Range Communication (DSRC) which is based on IEEE 802.11p standard [10]. Vehicles communicate with RSUs by vehicle-to-infrastructure (V2I) communication. Figure 1 gives an overview of vehicular fog architecture.

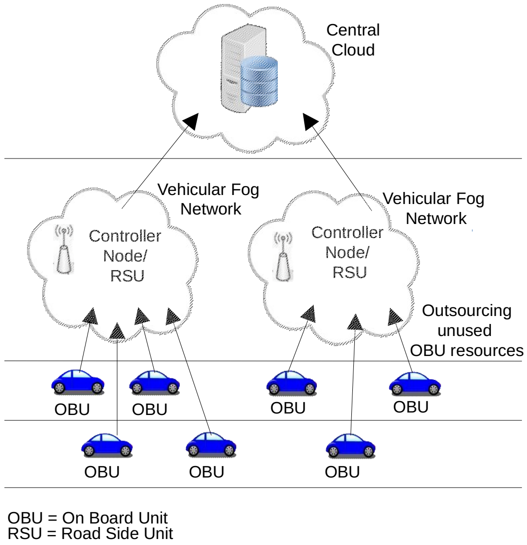

Fig. 1: Vehicular Fog Architecture

III. Assets of Vehicular Fog Architecture

Assets are closely related to threats because the attackers always target to gain unauthorized access of some assets while launching an attack. Hence, determination of valuable and important assets of the system is the first step of threat modeling. The assets of vehicular fog computing architecture can be tangible (e.g., roadside units) or abstract (e.g., system availability). Potential valuable assets of vehicular fog are:

- Messages
- Vehicle information
- Driver information
- Vehicle health information
- Sensor and GPS data
- Low latency services
- Road side units
- Log files
- Outsourced data for storage or computation
- Storage and memory of RSU
- Vehicular fog node storage and memory

Different security properties are important for different assets. Table I provides the important security properties based on confidentiality, integrity, availability, and authentication.

IV. Entry Points of attackers in Vehicular Fog

To perform an attack, the attacker needs to get inside the system. Entry points are the vulnerable points where an attacker can enter the system and gain access to the valuable assets.

TABLE I: Important security properties of assets based on Confidentiality, Integrity, Availability, and Authentication

Asset	C	I	A	A
Messages	✓	✓	×	×
Vehicle information	✓	✓	×	✓
User information	✓	✓	×	✓
Vehicle health information	✓	✓	×	×
Location information	✓	✓	×	✓
Sensor and GPS data	✓	✓	×	✓
Low latency services	×	×	✓	✓
Road side units	×	×	✓	✓
Log files	✓	✓	✓	×
Outsourced data for storage or computation	✓	✓	✓	✓
Storage and memory of RSU	✓	✓	✓	✓
Storage and memory of vehicular fog nodes	✓	✓	✓	✓

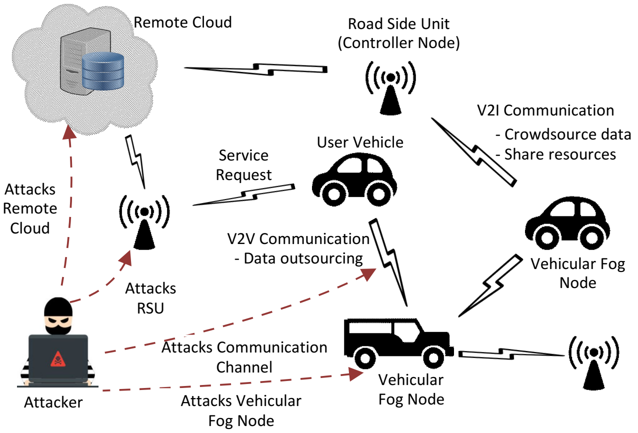

Fig. 2: Attacker Entry Points in Vehicular Fog Architecture

Entry points are also important to define the trust boundary [8] because anything outside the trust boundary is not trusted and the attackers attempt to exploit the entry points situated there. Implementation of a proper security mechanism is required for the outside of the trusted zone to prevent security attacks. Figure 2 shows the potential entry points.

Vehicular fog node: One of the most common ways to enter the vehicular fog network is as the vehicular fog nodes. The attacker pretends to be a legitimate fog node or user node and gets inside the system to acess the desired assets.

Road side unit: Road side units work as the controller nodes of a vehicular fog architecture which can also serve as fog nodes. Attackers can use RSUs to get inside the system.

Cloud data center: The vehicular fog networks send periodic update or summary to the remote cloud server. The attacker can get inside the cloud data center to launch attacks.

Communication channel: The vehicular fog nodes communicates with other fog nodes by V2V communication and road side units by V2I communication. The attacker can use these communication channels as the potential entry points for launching attacks.

V. Attacker Model

Characterizing the attacker model is important to think from the attacker's point of view. The attacker model identifies attacker entities, attack motives, and their capabilities.

A. Attackers

Attackers are the person or entities who directly launch attacks on the system to achieve any goal. There can be different classification of attacker such as insiders vs outsiders, malicious vs rational, and active vs passive attackers. Potential attackers of vehicular fog architecture are identified and listed as follows:

Road side unit attacker : Road side unit attacker attempts to access the storage and memory of the road side units. She can attack using a laptop by exploiting the communication protocol and read the unprotected texts and data of RSUs.

Vehicle driver: Vehicle drivers usually gets inside the network as vehicular fog node or user. A malicious user can let his vehicle join the network as a legitimate fog node and later exploit this to lauch different attacks. Similarly, an adversary can join the network to exploit the facilities as an user.

Remote cloud attacker: The controller nodes communicate with remote cloud to send periodic updates or summary. An adversary can attack the remote cloud to exploit the system.

B. Attack Motives

All the attacks performed on a system have some motives behind them which are closely related to the assets of the system. The potential attack motives can be:

Financial and personal gain: An attacker can perform the attack on behalf of any other person in exchange of money to achieve financial gain. Again, the attacker may want to increase the usage of her resources by manipulating the scheduling mechanism to gain more incentives. Moreover, the attacker can perform attacks in order to achieve personal gain such as sending forged cword-sourced message to make the other vehicles to take alternate routes who have the same destination.

Retrieve sensitive information: Vehicular fog architecture exploits the storage sharing with other vehicles in close proximity. An attacker may target the storage of nearby vehicular fog nodes and RSUs to retrieve any sensitive information about the storage users.

C. Capabilities

Capabilities are the actions an attacker is able to perform from inside or outside of the architecture. Attacker capabilities depend on many factors such as access and privilege of the attacker, known inside information, resource availability to launch the attacks, etc. Potential attacker capabilities are:

Access into the network: Attacker has the capability to get into the vehicular fog network in different ways such as user, vehicular fog node, or system admin. She also has the ability to send and receive data inside the vehicular fog network. Thus, she can steal valuable information from the users.

Eavesdropping the network: An attacker has the ability to eavesdrop on any ongoing communication in a vehicular fog network. If the message is unprotected, then she can easily learn the messages. However, if the messages are encrypted, the attacker still can perform different cryptographic attacks such as known plain-text attack, known cipher-text attack, etc.

Sniffing data: The attacker may have the ability to sniff the messages of an ongoing communication.

Collusion: Several vehicular fog nodes can collude with any malicious entity inside the vehicular fog network such as rouge fog nodes or RSUs. They can also collude with entities related to integrity analysis framework such as dishonest trusted third party or investigator.

VI. Threats and Vulnerabilities

We will identify the threats and vulnerabilities of vehicular fog architecture from the perspective of two popular threat modeling processes. One of them is the Confidentiality, Integrity, Availability, and Authentication model which is known as the CIAA model [7]. The other one is the STRIDE security model which means Spoofing, Tempering, Repudiation, Information disclosure, Denial of service, and Elevation of privilege [11].

A. The CIAA Threat Modeling Process

A secure system must ensure four properties to make it secure which are confidentiality, integrity, availability, and authentication (CIAA) [7]. In this section, we have identified and categorized the attacks based on these four security properties. Figure 3 provides an overview of the attack taxonomy according to the CIAA threat modeling process.

1) Confidentiality Attacks: Confidentiality is ensuring that the data is secret to everyone except the user. Confidentiality attacks are trying to retrieve explicit and implicit information from the vehicular fog architecture. We have identified the following confidentiality attacks on vehicular fog:

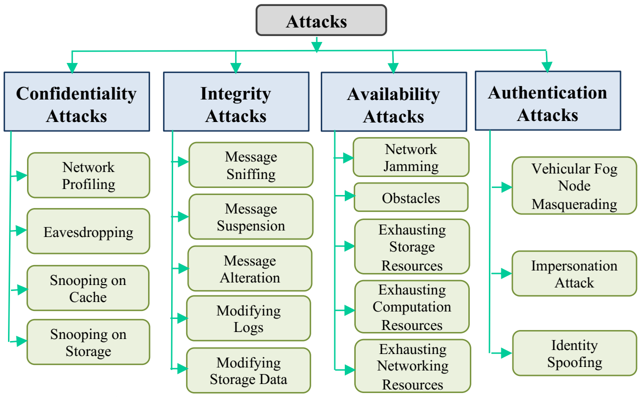

Fig. 3: Attack Taxonomy Based on CIAA

Network Profiling: An attacker can profile the vehicular fog network to get idea about the current network topology, movement of the vehicles, size of the network, capability of the network, current occupancy of available resources, etc.

Eavesdropping: Eavesdropping is unauthorized listening to the ongoing messages between two parties. This type of attack does not directly harm the system, but the attacker can learn the ongoing communication if the messages are not encrypted.

Snooping on cache and storage: Vehicular fog nodes have virtual machines in their OBUs to perform the offloaded computation tasks. They can also share the on-board storage to serve as ad-hoc storage for the users. If an attacker can gain the unauthorized access to the OBU of a fog node, then she can snoop on the cache and storage to learn the computation tasks and the data that has been outsourced to that node. Additionally, the attacker can also snoop on the cache and storage of other entities such as RSU, remote cloud, and trusted third party.

2) Integrity Attacks: Integrity ensures that nobody can tamper or modify the data which is inside the vehicular fog network. Potential integrity on vehicular fog can be:

Message Sniffing: Message sniffing refers to capturing and tampering the ongoing communication messages between two entities. The attacker can use unprotected communication channel to sniff the message in vehicular fog environment.

Message suspension: Message suspension is an integrity attack where the malicious fog node drops some packets or hold them before forwarding it. Intention behind message suspension is to prevent other entities from learning about any incidents or sensitive information about the user herself [12].

Message alteration attack: In message alteration attack, an entity provides wrong information or modifies the information when the message is passed through the entity.

Modifying logs and storage data: RSUs can store the event logs of the vehicular fog network. If the attacker can access the logs, she can modify or delete it to provoke wrong decisions in any future investigations performed by law enforcement agency. She can also perform integrity attacks on the storage by intentionally inserting, modifying, or replicating data.

3) Availability Attacks: A system must be available all the time to provide service seamlessly. Availability attacks make the system unavailable for a period of time. Potential availability attacks on vehicular fog networks are as follows:

Network jamming: The attacker may intend to jam the vehicular fog network by overloading the communication channels so that the messages cannot pass among the entities.

Obstacles: Attacker can put some obstacles between two vehicular fog entities which are communicating with each other for trust establishment by observing the behavior. Such obstacles may create a No Line of Sight situation which may hamper the usual workflow [13].

Exhausting storage, computation, and networking resources: Vehicular fog nodes can share their unused storage, computation, and networking resources to the resource constraint vehicles for performing different tasks using these resources. The RSUs also may have these resources to share with the users. A malicious greedy user may request and occupy all the available resources for her own usage by letting the legitimate users strive for resources.

4) Authentication Attacks: In authentication attack, the attacker masquarades with a legitimate user identity or vehicular fog identity to gain unauthorized access to the system. Potential authentication attacks can be:

Impersonation attacks: In impersonation attack, the malicious user pretends to be authenticated and performs action according to this. A malicious vehicular fog node can bypass the authentication protocol to gain unauthorized access to the system and perform malicious activity.

Identity spoofing: Identity spoofing is pretending to be another user by spoofing the identity and getting authenticated to enter the system. Wahiduzzaman et al. [14] have analyzed identity spoofing attacks in the context of vehicular networks .

Vehicular fog node masquarading: An attacker may masquarade the identity of a legitimate vehicular fog node to share its resources to the user vehicles. Later, the attacker may snoop on the data outsourced from the user to learn sensitive information.

B. The STRIDE Threat Modeling Process

The STRIDE threat modeling process was first proposed by Microsoft to identify the security threats of a system [11].

The term STRIDE refers to **S**poofing, **T**ampering, **R**epudiation, **I**nformation disclosure, **D**enial of service, and **E**levation of previlege. Each section of STRIDE model corresponds to a desirable security property which are authenticity, integrity, non-repudiability, confidentiality, availability, and authorization. Figure 4 provides an overview of the attack taxonomy according to this threat modeling process.

1) Spoofing Attacks: Spoofing means falsifying data to make a system fool to gain any kind of unauthorized access. It ruins authenticity which is one of the most important security properties. Some possible spoofing attacks are:

Bogus information attack: The vehicular fog nodes share their sensor, video, and location information to gain situational awareness. However, an attacker can send bogus information to mar the whole crowd-sourcing application which may lead to erroneous conclusions.

False resource requests: An attacker can send a lot of false resource requests to the vehicular fog network which will not eventually be used by the attacker. These false requests can eventually make the system run out of resources.

Sybil attack: In Sybil attack, the attacker broadcasts messages from multiple node identities which pretends to be from multiple vehicles [14]. The controller node and other vehicles think that all the messages are coming from different vehicles.

2) Tampering Attacks: Tampering attacks are performing unauthorized updates or alteration to any contents in the vehicular fog network. These are the attacks on integrity of the system. Example of tampering attacks are:

Tampering storage data: Storage constrained vehicles can outsource their data to nearest vehicular fog nodes. An attacker can get access to the data and erase or insert data blocks.

Tampering messages: The most important asset of vehicular for architecture is the messages passed among the entities. A malicious entity may catch and tamper the message before it reaches to the destination.

Tampering logs: The RSUs or remote central cloud server may store the logs of everything that happened in the vehicular fog architecture. The attacker can gain unauthorized access to the logs and modify those for various purposes such as trying to fool the investigator after performing malicious activities.

3) Repudiation Attacks: Repudiation attacks occur when an attacker repudiates performing an action intentionally.

Liability avoidance: From the perspective of vehicular fog nodes, the attacker may deny after performing an incident such as road accident, providing wrong information, deleting outsourced storage data, etc. User fog nodes can also perform these type of attacks, such as denying after taking services.

False presence: The attacker may claim to be present in a place in a particular time without actually being present there. These attacks are very severe in vehicular fog architecture because the applications are mostly highly location sensitive.

Activity hiding: While performing an attack, the attacker may try to hide the activity by not letting those event to be logged so that she cannot be convicted in future investigation.

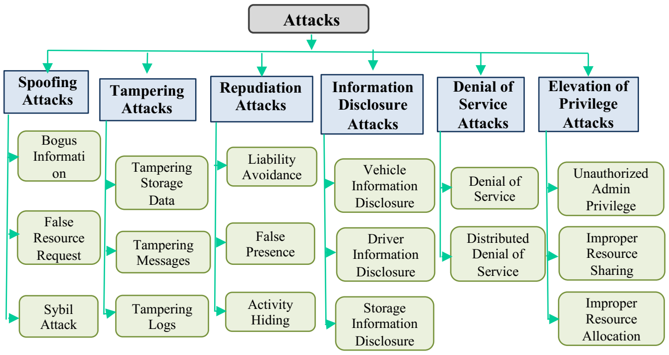
Attacks
Spoofing Attacks
Tampering Attacks
Repudiation Attacks
Information Disclosure Attacks
Denial of Service Attacks
Elevation of Privilege Attacks
Bogus Informati on
False Resource Request
Sybil Attack
Tampering Storage Data
Tampering Messages
Tampering Logs
Liability Avoidance
False Presence
Activity Hiding
Vehicle Information Disclosure
Driver Information Disclosure
Storage Information Disclosure
Denial of Service
Distributed Denial of Service
Unauthorized Admin Privilege
Improper Resource Sharing
Improper Resource Allocation

Fig. 4: Attack Taxonomy Based on STRIDE

4) Information Disclosure Attacks: In the information disclosure attacks, the attacker can hide the identity to acquire specific sensitive information about an user or vehicle and later use or disclose those information outside. For example:

Vehicle and driver information disclosure: The attacker may capture and disclose confidential information about vehicle and driver such as sensor data, location, registration information, mileage, driving license, driving history, insurance, etc.

Storage information disclosure: The user vehicles may outsource their data to the storage of nearest vehicular fog nodes. However, these data may contain sensitive information about the users. An attacker or a dishonest vehicular fog node may reveal this information to outside entities.

5) Denial of Service Attacks: The denial of service attacks can be performed to disrupt the service availability, performance, and efficiency of the system.

Denial of service: In the denial of service attack, the attacker consumes available resources through spoofing or greedy usage, which makes the legitimate users strive for the resources. As this attack is usually performed by one attacker, too many messages or resource requests can be turned down to prevent the attack and ensure logical resource sharing among the users.

Distributed denial of service: Distributed denial of service attack is performed by multiple malicious fog nodes to jam the communication channel by flooding meaningless messages or resource requests to exhaust the resources. These are harder to detect because multiple vehicular fog nodes perform the attack from different vehicles.

6) Elevation of privilege attacks: Elevation of privilege refers to gaining unauthorized privileges after getting inside the system which the attacker does not suppose to have. These attacks ruin authorization, which is a critical security property.

Unauthorized admin privilege: The attacker can elevate her privilege to gain the admin level access of vehicular fog system to control different components of the architecture, such as RSUs and remote cloud data centers.

Improper resource sharing: The vehicular fog nodes share their resources for financial gain. These resources are required to be distributed among users optimally to ensure fairness. However, the attacker may elevate the privilege to increase the usage of her resources more than other vehicular fog nodes.

Improper resource allocation: The available heterogeneous resources are allocated optimally according to the requirements. All the user vehicles expect to get a fair share of available resources. However, the attacker can elevate her privilege to gain more storage, computation, or networking resources.

C. Physical Attacks

Both the CIAA and STRIDE model do not consider the physical attacks in threat model processing. In the physical attacks, the attacker has physical access to the components of vehicular fog and has the capability to harm those physically. Possible physical attacks on vehicular fog architecture include power incision, hardware tampering, RSU component theft, network disruption, storage theft, etc.

VII. Mitigation strategies

Defining the mitigation strategies is the final step of threat modeling. Table II provides overview of the complete threat model. Based on all the previous sections, mitigation strategies are defined to prevent the attacks and mitigate the threats and vulnerabilities as they provide a relation between identified threats and possible standard solutions to them. Potential mitigation strategies are:

Secure authentication and authorization: Vehicular fog nodes need to provide identification information for joining the network. Several research works have proposed anonymous identity-based authentication such as public key infrastructure [15], symmetric key, group signature [16], and identity-based signature [17]. Along the journey to the destination, a vehicle may be required to be authenticated for multiple times. There should be proper protocols for entering and leaving each vehicular fog networks which will ensure secure cross data center authentication. To make the process faster, the cryptographic solutions should not be too computation-heavy. The key size used in signature or encryption should not be too long, and it also needs to provide enough security so that an adversary cannot figure out the key. Blockchain can be a possible solution to reduce communication and computation overhead because it eliminates the security issues related to the central authority and reduces the communication overhead with multiple entities. Researchers have proposed several blockchain-based authentication mechanisms for vehicular fog architecture. Yao et al. [18] and Kaur et al. [19] proposed blockchain-based authentication mechanism for vehicular fog architecture.

Secure and optimized resource allocation: In vehicular fog architecture, the fog node coordinator allocates the available heterogeneous resources among the users based on the requirements. The attacker may try to occupy more resources than it should have been granted. Several research works have proposed solutions for secure and optimized resource allocation in vehicular fog computing such as latency and quality optimized task allocation [20], optimized bandwidth allocation [21], contract-based resource allocation [22], and latency and quality balanced task allocation [23].

Encryption for confidentiality and integrity: All communication among vehicular fog entities should be encrypted using symmetric or asymmetric key encryption to ensure confidentiality and integrity. The data dissemination is important for several crowdsourcing applications of vehicular fog. These crowdsourcing and data dissemination process should be protected by encryption. Ensuring the security of outsourced data through encryption is also important because those may contain sensitive information.

Integrity analysis mechanism: The vehicular fog architecture should contain the mechanism for auditability of data and logs. No entity of the architecture should be able to repudiate after performing an action. For any future investigation, the investigator should be able to perform proper integrity analysis of an incident from the logs.

VIII. Related Works

Though this is the first attempt of domain-specific threat modeling in vehicular fog computing, there are several security enhancement research works which analyzed specific security issues in this context. Researchers have also explored the attack spaces for other vehicular networking paradigms. Engoulou et al. [24] provided a security survey of VANET, which consists of all the components of threat modeling analysis. Leinmuller et al. [25] modeled the roadside attacker behaviors in vehicular ad-hoc networks. There are several other research works on exploring the threats and vulnerabilities of VANETs. Al-kahtani et al. [26] identified and categorized potential attacks on VANETs. Zeadally et al. [27] explored the security challenges, attacks, and mitigation strategies of vehicular ad hoc networks. Besides the VANETs, there are some other research works in the context of threat modeling of vehicular clouds. Yan et al. [28] analyzed the security challenges in vehicular cloud computing. Wahiduzzaman et al. [14] explored the potential threats and vulnerabilities of vehicular cloud along with the architectural designs and security requirements. Huang et al. [29] analyzed the architecture, use case, security, and forensic challenges in vehicular fog computing.

In this paper, we have analyzed the threat model of vehicular fog based on CIAA and STRIDE threat modeling processes. Several research works have proposed different approaches for threat modeling. Oladimeji et al. [30] proposed a goal-oriented approach for security threat modeling and analysis. Saini et al. [31] explored attack tree based threat modeling approach, which was first introduced by Schneier [32]. Steffan et al. [33] introduced collaborative attack modeling process.

IX. Conclusion

Vehicular fog computing architecture presents unique security challenges. In this paper, we have presented a complete threat model of vehicular fog computing by analyzing the threats and vulnerabilities with two popular threat modeling processes which are CIAA and STRIDE. Along with the identification of potential attacks, we have also presented the mitigation strategies and illustrated the attacker model of vehicular fog. However, new attacks will be introduced in future days and they will be required to be classified using threat modeling processes. We posit that this initial domain-specific threat model will help the researchers to design better security solutions for vehicular fog computing.

Acknowledgement

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.

TABLE II: Overview of Vehicular Fog Threat Model

Assets	Entry Points	Attacker Model	Threats and Vulnerabilities		Mitigation Strategies
			CIAA	STRIDE	
• Messages • Vehicle information • Driver information • Vehicle health information • Location information • Sensor and GPS data • Low latency services • Road side units • Log files • Outsourced data for storage or computation • Storage and memory of RSU • Storage and memory of vehicular fog nodes	• Vehicular fog node • Road side unit • Cloud data center • Communication channel	**Attackers** • Road side unit attacker • Vehicle driver • Remote cloud attacker **Attack motives** • Financial gain • Personal gain • Greedy usage of resources • Retrieve sensitive information **Attacker capabilities** • Access into the network • Eavesdropping the network • Physical Access • Sniffing data • Affiliation	**Confidentiality attacks** • Network profiling • Eavesdropping • Snooping on cache • Snooping on storage **Integrity attacks** • Message sniffing • Message suspension • Message alteration • Modifying logs • Modifying storage data **Availability attacks** • Network jamming • Obstacles • Exhausting storage resources • Exhausting computation resources • Exhausting networking resources **Authentication attacks** • Vehicular fog node masquerading • Impersonation attack • Identity spoofing	**Spoofing attacks** • Bogus information • False resource request • Sybil attack • Impersonation attack **Tampering attacks** • Tampering storage data • Tampering messages • Tampering logs **Repudiation attacks** • Liability avoidance • False evidance • False presence • Activity hiding **Information disclosure attacks** • Vehicle information • Driver information • Storage information **Denial of service attacks** • Denial of service • Distributed denial of service **Elevation of privilege attacks** • Unauthorized admin privilege • Improper resource sharing • Impropar resource allocation	• Secure authentication and authorization • Secure and optimized resource allocation • Encryption for confidentiality and integrity • Integrity analysis mechanism • Using virtualization

REFERENCES

[1] S. Zeadally, R. Hunt, Y.-S. Chen, A. Irwin, and A. Hassan, "Vehicular ad hoc networks (vanets): status, results, and challenges," *Telecommunication Systems*, vol. 50, no. 4, pp. 217–241, 2012.

[2] J. Contreras-Castillo, S. Zeadally, and J. A. Guerrero-Ibañez, "Internet of vehicles: Architecture, protocols, and security," *IEEE internet of things Journal*, vol. 5, no. 5, pp. 3701–3709, 2017.

[3] M. Eltoweissy, S. Olariu, and M. Younis, "Towards autonomous vehicular clouds," in *International Conference on Ad Hoc Networks*. Springer, 2010, pp. 1–16.

[4] B. Insider, "The connected car report: Forecasts, competing technologies, and leading manufacturers," 2016, last accessed date: 03-October-2019. [Online]. Available: https://www.businessinsider.com/connected-car-forecasts-top-manufacturers-leading-car-makers-2015-3

[5] Waymo, "We are building the worlds most experienced driver," 2009, last accessed date: 03-October-2019. [Online]. Available: https://waymo.com/

[6] X. Hou, Y. Li, M. Chen, D. Wu, D. Jin, and S. Chen, "Vehicular fog computing: A viewpoint of vehicles as the infrastructures," *IEEE Transactions on Vehicular Tech*, vol. 65, no. 6, pp. 3860–3873, 2016.

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

[8] S. Myagmar, A. J. Lee, and W. Yurcik, "Threat modeling as a basis for security requirements," in *Proc. of the Symposium on Requirements Engineering for Information Security*. IEEE, 2005, pp. 94–102.

[9] F. Swiderski and W. Snyder, *Threat Modeling*. Microsoft Press Redmond, WA, USA, 2004.

[10] U. D. o. T. National highway traffic safety administration, "Vehicle safetycommunications project - final rep." Apr. 2006, last accessed date: 03-October-2019. [Online]. Available: https://www.nhtsa.gov/DOT/NHTSA/NRD/Multimedia/PDFs/CrashAvoidance/2006/VehicleSafetyCommunicationsProject-FinalReport.pdf

[11] Microsoft, "The stride threat model," 2009, last accessed date: 03-October-2019. [Online]. Available: https://docs.microsoft.com/en-us/previous-versions/commerce-server/ee823878(v=cs.20)

[12] F. Qu, Z. Wu, F.-Y. Wang, and W. Cho, "A security and privacy review of vanets," *IEEE Transactions on Intelligent Transportation Systems*, vol. 16, pp. 2985–2996, 2015.

[13] O. Abumansoor and A. Boukerche, "Towards a secure trust model for vehicular ad hoc networks services," *IEEE Global Telecommunications Conference - GLOBECOM*, pp. 1–5, 2011.

[14] M. Whaiduzzaman, M. Sookhak, A. Gani, and R. Buyya, "A survey on vehicular cloud computing," *Journal of Network and Computer Applications*, vol. 40, pp. 325–344, 2014.

[16] X. Lin, X. Sun, P.-H. Ho, and X. Shen, "Gsis: A secure and privacy-preserving protocol for vehicular communications," in *IEEE Transactions on Vehicular Technology*, vol. 56. IEEE, 2007, pp. 3442 – 3456.

[15] A. Studer, E. Shi, and F. Bai, "Tacking together efficient authentication, revocation, and privacy in vanets," in *6th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks*. IEEE, 2009, pp. 1–9.

[17] P. Kamat, A. Baliga, and W. Trappe, "An identity-based security framework for vanets," in *Proceedings of the 3rd international workshop on vehicular ad hoc networks*. ACM, 2006, pp. 94 – 95.

[18] Y. Yao, X. Chang, and J. Mi, "Bla:blockchain-assisted lightweight anonymous authentication for distributed vehicular fog services," *IEEE Internet of Things Journal*, vol. 6, pp. 3775 – 3784, 2019.

[19] K. Kaur, S. Garg, and G. Kaddoum, "Blockchain-based lightweight authentication mechanism for vehicular fog infrastructure," in *IEEE ICC Workshop on Wireless Physical Layer Security*. IEEE, 2019.

[20] C. Zhu, J. Tao, G. Pastor, Y. Xiao, Y. Ji, Q. Zhou, Y. Li, and A. Yia-Jaaski, "Folo: Latency and quality optimized task allocation in vehicular fog computing," in *IEEE Internet of Things Journal*. IEEE, 2018.

[21] F. Lin, Y. Zhou, G. Pau, and M. Collotta, "Optimization-oriented resource allocation management for vehicular fog computing," in *IEEE Access*, vol. 6. IEEE, 2018, pp. 69 294 – 69 303.

[22] Y. Wang, C. Xu, and Z. Zhou, "Contract-based resource allocation for low-latency vehicular fog computing," in *PIMRC*. IEEE, 2018.

[23] C. Zhu, G. Paster, Y. Xiao, and A. Yale-Jaeaeski, "Fog following me: Latency and quality balanced task allocation in vehicular fog computing," in *15th Annual IEEE Internation Conference on Sensing, Communication, and Networking (SECON)*. IEEE, 2018, pp. 1–9.

[24] R. G. Engoulou, M. Bellache, and S. Pierre, "Vanet security surveys," *Journal of Network and Computer Applications*, vol. 44, pp. 1–13, 2014.

[25] T. Leinmuller and R. K. Schmidt, "Modeling roadside attacker behavior in vanets," in *IEEE Globecom Workshops*. IEEE, 2008, pp. 1–8.

[26] M. S. Al-kahtani, "Survey on security attacks in vehicular ad hoc networks (vanets)," in *6th International Conference on Signal Processing and Communication Systems*. IEEE, 2012, pp. 1–9.

[27] S. Zeadally, R. Hunt, Y.-S. Chen, A. Irwin, and A. Hassan, "Vehicular ad hoc networks (vanets): status, results, and challenges," *Computer Communications*, vol. 50, pp. 217–241, 2012.

[28] G. Yan, D. Wen, and S. Olariu, "Security challenges in vehicular cloud computing," *IEEE Transactions on Intelligent Transportation Systems*, vol. 14, pp. 284–294, 2013.

[29] C. Huang, R. Lu, and R. Choo, "Vehicular fog computing: Architecture, use case, and security and forensic challenges," in *IEEE Communications Magazine*, vol. 55. IEEE, 2017, pp. 105–111.

[30] E. A. Oladimeji, S. Supakkul, and L. Chung, "Security threat modeling and analysis: A goal-oriented approach," in *SEA '06*. ACTA Press, 2006, pp. 178 – 185.

[31] V. Saini, Q. Duan, and V. Paruchuri, "Threat modeling using attack trees," *Journal of Computing Sciences in Colleges*, vol. 23, pp. 124–131, 2008.

[32] B. Schneier, "Attack trees," *Dr. Dobb's journal*, 1999.

[33] J. Steffan and M. Schumacher, "Collaborative attack modeling," in *Proceedings of the ACM symposium on Applied computing*. ACM, 2002, pp. 253 – 259.