IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 2 December 2022, accepted 17 December 2022, date of publication 20 December 2022,
date of current version 28 December 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3231189

RESEARCH ARTICLE

A Threat Model for Vehicular Fog Computing

TIMO KLEIN, TANJA FENN, ANETT KATZENBACH, HEINER TEIGELER, SEBASTIAN LINS, AND ALI SUNYAEV

Institute of Applied Informatics and Formal Description Methods, Karlsruhe Institute of Technology, Karlsruhe, 76049 Baden-Württemberg, Germany

Corresponding author: Heiner Teigeler (teigeler@kit.edu)

This work was supported by the Karlsruhe Institute of Technology (KIT).

ABSTRACT Vehicular Fog Computing (VFC) facilitates the deployment of distributed, latency-aware services, residing between smart vehicles and cloud services. However, VFC systems are exposed to manifold security threats, putting human life at risk. Knowledge on such threats is scattered and lacks empirical validation. We performed an extensive threat assessment by reviewing literature and conducting expert interviews, leading to a comprehensive threat model with 33 attacks and example security mitigation strategies, among others. We thereby synthesize and extend prior research; provide rich descriptions for threats; and raise awareness of physical attacks that underline importance of the cyber-physical manifestation of VFC.

INDEX TERMS Vehicular fog computing, fog computing, threat model, STRIDE, security.

I. INTRODUCTION

By 2025, the Automotive Edge Computing Consortium estimates that 100 million connected vehicles worldwide may generate up to 10 exabytes of data per month [1]. With the start of 2016, there were already more new cars added to cellular networks than phones [2]. This development is projected to even accelerate as the number of connected vehicles will rise by 295% from 2018 to 2023, when connected vehicles will make up 24% of all vehicles [3]. One of the biggest challenges of connected vehicles is the management, storage, and real-time processing of huge amounts of data. Whereas cloud computing has been a success story over the past decade [4], current infrastructures and conventional cloud computing architectures are unable to handle these large streams of generated data while ensuring low latency and enabling real-time processing that is needed by connected cars [1], [5].

A potential remedy to these challenges is fog computing and its application to road traffic, so called Vehicular Fog Computing (VFC), which has increasingly gained attention in both practice and research over the last years. In general, fog computing adds an intermediate layer consisting of so-called fog nodes between edge devices (e.g., sensors, actuators, or smart end-devices) and central cloud servers with the goal of lowering latency [6] and more efficient usage of computational resources (e.g., due to less time spent on data upload [7]) compared to traditional cloud architectures [8], [9]. Fog nodes are the core component of a fog computing system and refer to either physical components (e.g., gateways, routers, servers, etc.) or virtual components (e.g., virtualized switches, virtual machines, cloudlets, etc.). They are tightly coupled with edge devices or access networks, and provide services to these devices, including applications, operating platforms, or bare computing infrastructure [8].

By building on these technological premises and advancements of fog computing, VFC transforms conventional road infrastructures by adding an intermediate layer of (physical or virtual) fog nodes, enabling ubiquitous access to computing resources. The VFC architecture facilitates the deployment of distributed, latency-aware services, residing between smart vehicles and end-devices embedded in the road infrastructure (e.g., smart traffic lights), and centralized (cloud) services. As such, VFC fog nodes enable smart vehicles to perceive and interact with their environment through sensory input as well as exchange data with low-level roadside infrastructures, among others. VFC provides benefits for both individuals and the society as a whole by reducing the amount of road traffic congestion and number of car accidents [10]. Apart from optimization, the provision of local, scalable computing power might also enable more innovative use cases. For instance, Fleck et al. [11] enable traffic data collection complying with privacy regulations by using specific fog nodes for local data preprocessing, so-called Roadside Units (RSUs).

The associate editor coordinating the review of this manuscript and approving it for publication was Huan Zhou.

Besides VFC's many opportunities, there are still challenges of such systems which are not well understood, in particular with respect to security threats [12]. VFC not only inherits common service computing security threats like Denial of Services (DoSs) or eavesdropping (i.e., secretly listening to private communication of vehicles) but also introduces further challenges, such as preventing physical attacks, including physical destruction of nodes or theft of components. The importance of such security threats is exacerbated by the road traffic context, where failure of components could result in human life being at risk. Examining the security threats and identifying possible mitigation strategies for VFC helps to build trust in VFC, which is needed to further diffuse VFC and achieve promised advantages within society.

Over the past years, fog computing and VFC in particular have gained substantial research traction [13]. Extant research, for example, specifies VFC architectures (e.g., [10]), discusses potential use cases (e.g., [14]), applies VFC to achieve smart cities (e.g., [15]), or defines communication protocols to enable data exchange (e.g., [16]). Concerning security threats, researchers have started to discuss possible risks of VFC systems, developed early threat models to assess possible risks for VFC, and developed security measures against them [17]. However, the knowledge is scattered across different research articles and disciplines, and lacks empirical validation. For example, Hoque and Hasan [18] discuss important security risks in the context of VFC. However, physical attacks have been neglected so far, mostly because physical attacks are not explicitly emphasized as relevant threats in popular threat models like STRIDE [19], [20]. Still, threat models like STRIDE allow capturing physical attacks although they are not highlighted as a category of their own. To enhance security of VFC systems, we are aiming to consolidate the currently scattered knowledge on VFC's threats and extend the existing knowledge in key areas like physical attacks. The main goal of this work is thus to provide an extensive threat assessment of an application of fog computing to road traffic by answering the following question:

What are security threats of VFC systems?

To answer this research question, we followed a two-step approach. First, we conducted a literature review to assess the current state of research in the VFC field and synthesize the knowledge currently scattered across the community. Second, we carried out 12 expert interviews to empirically validate previous findings. More importantly, interviews additionally served to extend the literature and add information from a practitioner's point of view on further issues such as information on physical attacks that have been neglected so far. We consolidated the findings into a comprehensive threat model based on Khan et al. [12]'s STRIDE threat modeling for cyber-physical systems.

Our combined research yields 33 attacks, which we grouped along 6 STRIDE attack categories. Threats thereby relate to spoofing (e.g., sybil attacks), tampering (e.g., bogus information), repudiation (e.g., liability avoidance), information disclosure (e.g., eavesdropping), DoS (e.g., black holes), and elevation of privilege (e.g., improper resource allocation and sharing). All categories are consistently mentioned across both literature and experts. We also shed light on three relevant physical attacks that have been neglected so far: physical data breach, physical denial of service (PDoS) and physical compromising. Finally, our research provides an outlook on potential security mitigation strategies to overcome identified threats.

Our work contributes to the further development and deployment of VFC systems by providing a unified threat model. With this study, we synthesize and harmonize extant research and provide a structured threat model aligned with the STRIDE attack categories, helping to identify common security mitigation strategies that are associated with these categories. We also extend our current understanding of threats by providing rich descriptions and empirical validation, thereby providing support to define requirements and boundary conditions of VFC systems and security measures. Finally, we fill an important gap in extant research by raising awareness of physical attacks that underline importance of the cyber-physical manifestation of VFC. With this work, practitioners can obtain manifold insights into possible attack vectors in VFC along with example guidelines on how to mitigate those threats. These findings may then be used in defining requirements for a VFC system from a security perspective, ultimately helping to make future systems more secure and safe.

This paper is structured as follows. First, we briefly introduce the background of our work and define fog computing and VFC as theoretical basis of our research. The following section outlines our applied research methodology, both in regards to the literature review as well as the expert interviews. Afterwards, we provide a detailed threat model of VFC that summarizes the findings of our literature review and the expert interviews. The following section provides an overview on related works by contrasting the limitations of the existing literature and indicating where our study fills the gaps. We conclude our work with a discussion about our principal findings and potential threat mitigation strategies, highlighting implications and limitations of our research. We close this paper with a brief conclusion.

II. THEORETICAL BACKGROUND

A. FOG COMPUTING

Extant research still lacks an established definition of fog computing. Literature (e.g., [21]), tutorials (e.g., [22]) and company white papers (e.g., [23]) use various definitions of fog computing, and there is no consistent understanding of the term. Other terms like edge computing, mist computing, fogging, cyber foraging, and cloudlets are also often mentioned as synonyms, competing models, or supplementary models [24], [25]. In this work, the National Institute of Standards and Technology (NIST)'s[1] definition for fog computing provides the basis for defining the term [8].

[1]Mell and Grance [26] of NIST have also provided the de facto definition of cloud computing with over 19900 citations.

Fog computing is described as a "*layered model for enabling ubiquitous access to a shared continuum of scalable computing resources*" [8, p. 2]. The fog model facilitates the deployment of distributed, latency-aware applications and services, and consists of fog nodes (physical or virtual), residing between smart end-devices and centralized (cloud) services [8]. One of fog computing's key characteristic is thereby the introduction of an intermediate layer of computational resources between cloud servers and edge devices, which is shown in Figure 1. In fog computing, end-devices communicate with fog nodes in this intermediate computing layer and receive data that are processed, analyzed, or stored in the layer's fog nodes. These nodes can be either physical or virtual and possess five defining attributes [8]:

Autonomy: Fog nodes are able to make independent, local decisions. This may for instance be a device regulating traffic at a smart intersection autonomously.

Heterogeneity: Fog nodes can exist in various forms and shapes. If, for example, the fog node is placed on a traffic light it needs to be more robust to outside conditions compared to a node located inside a building.

Hierarchical Clustering: Fog nodes support hierarchical structures, where each level of the hierarchy provides different services while working together in a large system. As an example, one fog node may emit warnings based on road conditions whereas another may use these warnings to reroute traffic. Hierarchical clustering also is a key distinction between fog computing and edge computing. Compared to the focus on computationally enhanced end devices in edge computing, fog nodes provide a wider array of services like data storage and decision-making [8].

Manageability: Fog nodes are managed by a complex system. It can perform routine operations automatically. In a VFC context this means that there is no need for low level human interaction to manage a city's traffic.

Programmability: Programmability refers to an object being able to modify its behavior without needing to change its representation [27]. In fog computing, this is achieved through specialized software. Fog nodes in particular are designed to be programmable by different stakeholders such as equipment manufacturers [8]. For example, a fog node providing infotainment to nearby vehicles may be programmed by a network operator to analyze traffic volume. This does not change its representation within the VFC system: It is still a fog node.

Fog computing is conceptually related to edge computing. Both aim to solve similar challenges like latency and band-width constraints [28]. While it can be argued that the terms are interchangeable, there are important differences between both models. Fog computing is an inherently hierarchical model with a focus on infrastructure while edge computing is concerned with providing computation directly at the edge layer [28]. Another difference lies in the data processing, storage and decision-making capabilities of fog nodes compared to the networking and computation focus of devices in edge computing [8].

B. FROM FOG COMPUTING TO VEHICULAR FOG COMPUTING

VFC is one of the most promising and often discussed application of fog computing. In this work, we focus on this specific application. As of today, there exist a variety of definitions of VFC and its components, leading to multiple theoretical foundations as basis. For this study, we build on Huang et al. [10] and Ning et al. [15] who introduced a three-layered VFC system, in which vehicles represent edge devices, fog nodes are stationed near the road and so-called Roadside Units (RSUs), and central cloud services are used to perform sophisticated data analyses. This system may be further extended to include additional layers, such as a cloudlet layer [29] or smartphones and other smart roadside devices as edge devices [30]. In our view, the architecture introduced by Huang et al. [10] presents the most natural extension of the conceptual model of fog computing outlined above while still being general enough to encompass more specialized architectures or additional layers. Note that by using the term VFC system we also take a more abstract, system-theoretic perspective referring to a socio-technical set of relationships consisting of individuals and technologies that interact to perform certain tasks, such as driving, using infotainment fog services, or exchanging data [31].

One commonly related model are so called Vehicular ad hoc Networks (VANETs) that enable car-to-car ad hoc mobile communication and networking. VANETs became particular important to enable autonomous driving and for the dissemination of messages over short or long distances. While the vehicles themselves may then be regarded as fog nodes [14], [32], VANETs do not necessarily rely on fog computing as evidenced by their inception years before the emergence of fog computing [23], [33].

Figure 1 shows a schematic visualization of the selected VFC system and provides links between key terms. VFC commonly comprises smart vehicles perceiving their environment through sensory input as well as low-level roadside infrastructure like traffic lights as edge devices. While these edge devices possess data pre-processing capabilities, they lack the computational resources to optimize traffic on an area-wide level. Thus, they are connected to a fog network with RSUs collecting their data [10] via multiple possible interfaces like WiFi or radio frequency bands (e.g., LTE or 5G) [30]. These connections must link the RSU with cars on one hand and the cloud server on the other hand while balancing reliability and bandwidth constraints. The RSUs process the input from devices on the edge layer and use it for local decision making. Concrete examples of decisions on this level include sending warnings to other driving vehicles about bad road conditions and accidents [10], or scheduling traffic lights to enable an ambulance to reach its destination as fast as possible [34]. Computational abilities of RSUs are however not enough to optimize traffic on a city-wide level. Therefore, they forward key information towards centralized cloud servers that are tasked with large scale decision making and data analysis.

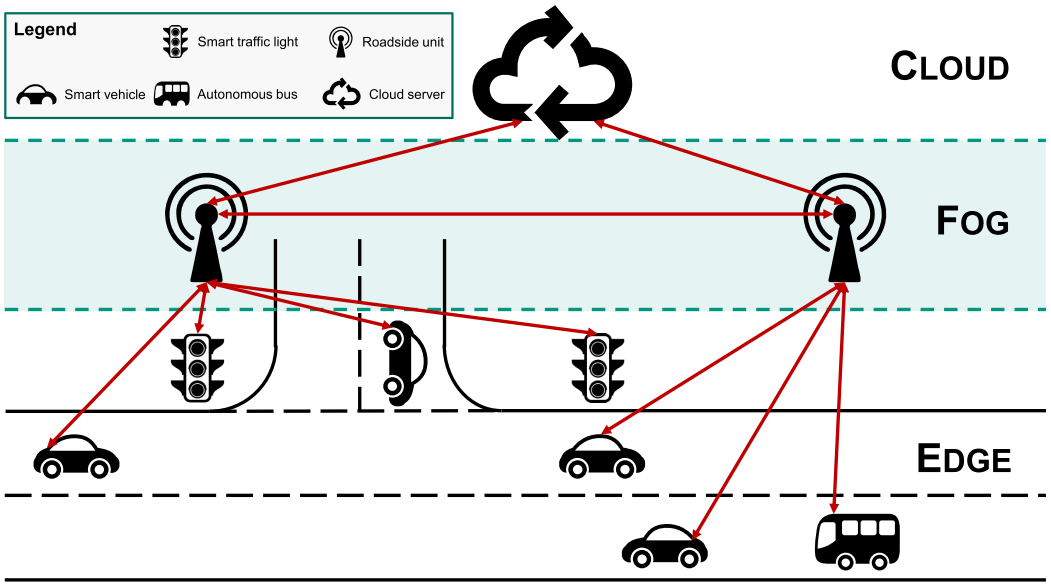


FIGURE 1. Schematic illustration of a vehicular fog computing architecture.

VFC is a technology with huge potential benefits and various use cases have been proposed and implemented in practice. For example, fog nodes can be used to distribute content in VANETs, offer entertainment services in inter-state buses, enable traffic scheduling, or monitor the condition of vehicles in real-time to decentralize maintenance and increase road safety [35], [36]. Moving the management of critical road infrastructures into a complex and interwoven ecosystem of information systems (e.g., edge devices, fog nodes, and cloud services), however, introduces new risks, particularly cyber threats that require mitigation measures and strategies.

III. RESEARCH METHOD

To answer our research question, we applied threat modeling as a common tool from cyber security for the structured assessment of a system's threats as well for developing suitable countermeasures, thereby also achieving a better understanding of such threats. To gather relevant data for developing a comprehensive threat model for VFC systems and particularly identifying threats and vulnerabilities of VFC, we conducted two complementary iterations of data gathering and analyzing. First, we conducted a scientific database search to identify relevant literature, and extract existing data on threats and threat models. Second, we conducted 12 one-to-one interviews to get in-depth knowledge about security challenges and opportunities in the area of VFC, thereby aiming to validate and extend prior research findings and better understand peculiarities of VFC threats (e.g., physical attacks).

A. STRIDE-BASED THREAT MODELING

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 [37]. 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.

While there is a multitude of threat modeling techniques to choose from, threat modeling typically consists of five components where each of them are important and complement each other to provide a comprehensive security assessment of the system [38]: (1) assets (valuable systems or components which attackers are interested in); (2) entry points (vulnerable points through which the attackers can enter into the system); (3) attacker model (the characteristics of the attackers); (4) threats and vulnerabilities; and (5) mitigation strategies (techniques to prevent potential attacks and solve the vulnerabilities). To derive these components for VFC systems, this work adopts the STRIDE threat modeling methodology [19] because it has already been applied to VFC (e.g., [37]) and related areas like cyber-physical systems (e.g., [20]). Additionally, it is mature and popular compared to other techniques [39]. We particularly rely on the threat modeling approach of Khan et al. [20], who have extended STRIDE-based threat modeling to consider peculiarities of cyber-physical systems, which also apply to VFC.

Khan et al. [20]'s STRIDE-based threat modeling approach involves five major steps, which we applied throughout our study. In a first step, we decomposed the VFC system into a component graph with the goal of identifying all internal and external entities in contact with the system (i.e., identifying entry points). Second, we established connections and data flows between different entities and plotted them in a Data Flow Diagram (DFD). The DFD aims to visualize all relevant entities and functionality within the system. In the third step, we aimed to identify possible threats based on the DFD. The STRIDE model provides common attack categories that we

considered when performing threat assessments. Note that certain STRIDE threats may apply only to specific parts of the system. In general, STRIDE is a mnemonic and stands for six cyber-attacks that we considered during our data gathering and analysis iterations:

- *Spoofing* refers to an attack in which an individual or piece of software disguises its identity within the system, usually for their own gain.
- *Tampering*. In a tampering attack an adversary manipulates or alters data in any part of the system. This includes both data stored within a system as well as data being transmitted between components.
- *Repudiation*. When an attacker manages to deny actions which have already been implemented within the system, it is called repudiation.
- *Information disclosure* refers to the leakage or revelation of sensitive information to actors which otherwise would not have access to it.
- *Denial of Service (DoS)*. DoS attacks aim to disrupt a system and make it (temporarily) unavailable. DoS can either target a specific component or the system as a whole.
- *Elevation of privilege*. Here attackers try to gain unauthorized access to system resources which are beyond the scope of their privilege.

In the fourth threat modeling step, we identified vulnerabilities causing some of these security threats, giving insights into how the discovered threats arise. Such a vulnerability could be, for instance, a car manufacturer producing vehicles with an easily accessible vehicle bus that eases compromising attacks. In the last step, we briefly elaborated on high-level mitigation strategies based on appropriate security features as counters to the identified threats, such as secure authentication and authorization, or encryption for confidentiality and integrity. Table 1 summarizes the STRIDE attack categories and matches them with mitigation strategies proposed by STRIDE [19], [40].

B. LITERATURE REVIEW

To gather data for our threat model, we performed a scientific database search in the following databases that cover a wide range of journals and conferences (i.e., they cover the top computer science and information systems journals and conferences): ACM Digital Library, EBSCOhost, IEEE Xplore, and ScienceDirect. Each database was searched with the following search string in title, abstract and keywords: ''(security OR privacy) AND (fog OR edge) AND vehicular''. We filtered for peer-reviewed articles and excluded grey literature, such as books and doctoral theses. We identified 203 articles as potentially relevant for our research (as of May 2020). To make sure that these articles are relevant for our research, we analysed title, abstract, and keywords. In total, we excluded 185 articles: 49 articles that are off-topic, 32 articles that do not refer to an system with a fog layer, 8 articles without relation to the vehicular context, 16 articles that do not focus on security and 80 articles which describe only a technical implementation, leading to a final set of 18 articles that were analyzed in detail.

After the literature review was completed, we employed the coding method of Lacity et al. [41] to identify potential threats. In particular, we recorded for each extracted threat a name, a description, and the affected VFC system component. In addition, we noted security mitigation strategies, attacker types, motives and consequences of threats, in case prior research mentioned these. Gathering this additional data helped us to better understand the threats, their origins, interdependencies and potential consequences. We created a list of master variables to aggregate the identified threats. A master variable is an aggregation of similar threats consisting of a master variable name and a master variable description. If an identified threat fitted into an existing master variable, we assigned it accordingly; otherwise, a new master variable was created. For example, we aggregated the threats ''IP spoofing'' and ''fake identities'' to the master variable ''impersonation attack''. Since different people often put the same labels on different things, and vice versa, we considered semantic ambiguities (e.g., different terms for the same threat) during our data analysis [42]. The resulting coding scheme consisted of 115 variables that were aggregated to 33 master variables posing a threat for VFC.

C. EXPERT INTERVIEWS

We complemented our literature review findings with expert interviews to deepen our knowledge of threats for VFC and extend our threat model by VFC specifics, such as physical attacks that have been neglected by prior research. In total, we conducted 12 semi-structured one-to-one expert interviews. To acquire potential interviewees, we applied a purposeful sampling strategy that focused on selecting individuals who are especially knowledgeable about our phenomenon of interest (i.e., security in VFC) [43]. Consequently, we included only experts who were engaged in fog computing and security. Especially due to the early stage of VFC, it was difficult to find interviewees who are well versed in both subject areas. However, we deem that the composition of our interviewees covers both areas well, as summarized in Table 2. We interviewed experts both from industry and research to examine current state of the art and gain knowledge from current research. Eleven out of 12 interviewees are based in Germany while one interviewee is from Sweden.

We applied a semi-structured interview method for different reasons. A certain basic structure was necessary for our research because we aim to gather further information on identified threats from prior research. While providing such a basic structure, semi-structured interviews also leave interviewed experts with a sufficient degree of freedom to talk about aspects that might not have come to our attention during the literature review or preparation of the interview.

The interview guide was derived and discussed by the authors before conducting the interviews. In addition, we made constant improvements to the interview guide in terms of clarity and comprehensibility of the questions. The

TABLE 1. Overview on STRIDE categories and the corresponding high-level mitigation strategies. Adopted from Howard and Lipner [40].

Attack category	Description	Mitigation strategy	Description
Spoofing	Assuming a wrong identity	Authentication	Verification of identities
Tampering	Manipulation of data	Integrity	Monitoring of data flows
Repudiation	Denial of actions	Non-repudiation	Recording of system actions
Information Disclosure	Revelation of data	Confidentiality	Prevention of illegal data access
Denial of Service	System disruption	Availability	Ensuring system availability
Elevation of Privilege	Unauthorized access to resources	Authorization	Access right verification

TABLE 2. Brief overview of experts interviewed.

Expert	Position	Field of Expertise	Experience in VFC
E-1	Researcher	Automotive	1-3 years
E-2	IT-Security Consultant	IT-Security	< 1 year
E-3	Researcher	Academic	< 1 year
E-4	Researcher	Automotive	> 5 years
E-5	IT-Security Manager	Automotive	> 5 years
E-6	Technology Expert for V2X	Automotive	> 5 years
E-7	Software Developer	Automotive	3-5 years
E-8	CTO	IT	3-5 years
E-9	Researcher	Academic	> 5 years
E-10	IT Project Manager	Automotive	> 5 years
E-11	Other	Automotive	< 1 year
E-12	Researcher	Academic	1-3 years

interview guide was structured as follows. First, we asked experts about their background and experience in the area of VFC and security. We anticipated different comprehensions of terms like edge computing and fog computing. Thus, to ensure a common understanding for the interview, we discussed and introduced a VFC scenario before starting with content-related questions. In the main part of the interview, we asked our interview partners about security aspects of the VFC system, as well as relevant security threats and potential security concepts, guided by the STRIDE model (i.e., attack categories and mitigation strategies). We applied a non-judgmental form of listening, maintained distance, and strived to sustain an open and non-directive style of conversation during the interviews to ensure impartiality and avoid bias. We recorded and transcribed each interview. Interviews typically lasted between 30 to 50 minutes.

To analyze the interview data, we applied scientific coding techniques, including selective, open, and theoretical coding [44] using the tool 'f4analyse' to facilitate this process. Coding refers to a process in which one annotates and labels interview transcripts with a piece of text [45]. To determine the code labels, we used words that the interviewees suggested [46]. We first started with deductive coding by assigning master variables identified in the literature review to textual segments of the interviews to validate findings from prior research as well as gather additional information. We thus inserted the master variables into our codebook and selectively assigned these codes to textual segments that relate to the specific master variable. For example, we coded the master variable "data breach" to the interview statement "*If an attacker can intercept concrete location data, it is possible to say that a car registered to person X can be found here or there in the city*" [E-3]. Deductive coding enabled us to dive deeper into the threats proposed by prior research and derive rich descriptions. Afterwards, we performed open coding to identify further threats, such as physical attacks, that have been neglected in prior research so far. Open coding entails fracturing the data by describing concepts in it that may define a significant occurrence or incident about a phenomenon [44], [47]. During open coding, all available data were labeled for direct visibility of the structure and information of the interview. With open coding, we have deepened our knowledge on physical attacks in particular. For example, we coded the phrase "There would be the possibility [with fog nodes] that someone could physically go there, open the box, and put its USB stick with a virus on it in. That is simply a possibility that does not exist with cloud computing" [E-1] to the novel threat code "Physical compromising". The coding approach resulted in a consolidated number of 33 threats, comprising literature review and interview findings. We also aimed to move beyond a mere description of threats to a more abstract level of conceptualization by performing axial and selective coding [48]. We therefore synthesized our findings with the STRIDE model to group similar codes to more abstract categories according to common themes, thereby creating hierarchical classifications. Particularly, we used the STRIDE threat model to cluster our findings into the six attack categories of STRIDE: Spoofing, Tampering, Repudiation, Information disclosure, DoS, and Elevation of privilege [19]. Tables 4 - 9 summarize our coding results.

IV. A THREAT MODEL FOR VEHICULAR FOG COMPUTING

A. ASSETS AND ENTRY POINTS

Extant research and interviewees reported various valuable assets in the context of VFC that require protection [37]. These may be:

- *messages*, e.g., an RSU warning message about bad road conditions to succeeding vehicles,

TABLE 3. Comparison of typical entities in each layer for fog computing and vehicular fog computing.

Layer	Typical entities in fog computing	Typical entities in vehicular fog computing
Edge	Smartphone	Connected vehicles, smart roadside devices
Fog	Server, switch, router	Roadside Unit (RSU)
Cloud	Commercial data center	Government data center

- *vehicle information*, e.g., a vehicle identification number,
- *driver information*, e.g., driver ID number,
- *vehicle health information*, e.g., current motor oil level,
- *sensor or GPS data*, e.g., current vehicle location,
- *(low latency) services*, e.g., driver infotainment,
- *log files*, e.g., daily traffic volume data.

In this work we focus on three entities offering vulnerable points where an attacker can enter the system and gain access to the valuable assets: fog nodes, edge devices, and cloud services, while considering the network and communication channels that link these entities. Table 3 contrasts typical entities for each computing level (fog, edge and cloud) in fog computing with those used in the VFC definition outlined above.

Building on these entities, we developed a DFD that serves as basis for our threat model and is depicted in Figure 2. In order to keep this article as broadly applicable as possible, we opt for a high-level DFD that fits with the conceptual nature of our work. The DFD shows the components of our architecture - edge devices, fog nodes and cloud services – as concrete *system entities* within the VFC system as ellipses. *External entities* are actors who are not part of the VFC system but interact with it. They include stakeholders like car manufacturers or users like a vehicle owner. Abstract boundaries within the system are represented as *trust boundaries*. Data exchange within a trust boundary can be assumed to be verified, whereas exchange between boundaries needs to be validated (e.g., through the use of authentication mechanisms). The last component of the DFD are data flows, which model the interactions between components and are depicted as arrows. The tips of the arrow indicate the direction of the exchanged data. The broader category of data flows is further divided and contains three distinguished subgroups:

- **Edge-Fog data flows** contain all data exchange between smart vehicles or other edge devices and fog nodes, particularly RSUs.
- **Fog-Cloud data flows** comprise transferred data between the fog and cloud layers of the system.
- **Data flows outside system** represent an exchange with an entity not within the VFC system.

We found it reasonable to assume that data transfer between two types of entities within the system relies on similar technology, therefore exhibiting comparable vulnerabilities. This grouping allows for a more concise analysis in the following sections. While we acknowledge that attacks on entities outside of the VFC system may compromise the system as well, they are not the focus of our article. Consequently, attacks on these entities or data transferred to them are not considered. Compliance of outside entities with security standards of the VFC system can be achieved, for example, via certification and audits (e.g., ISO/IEC 27001 information security management systems standard).

B. ATTACKER MODEL

In order to further characterize the attacks identified throughout the modeling stages, we specify the following attacker model, comprising three orthogonal dimensions on how the attackers behind different threats to the VFC system may be categorized:

ATTACKER ACTIVITY (ACTIVE VS. PASSIVE)

Active attackers seek to deliberately disrupt or destroy the functionality of the system, for instance by transmitting fake data to network components [10], [17]. Passive attacks are not aimed at a disruption of the system. Instead, their goal is to monitor the system and collect private information [10], [49].

ATTACKER CAPABILITIES (INTERNAL VS. EXTERNAL)

Internal attackers run their attacks from compromised parts of the system, like RSUs or the cloud, whereas external attackers are "*not equipped with key materials in a [VFC] system*" [10, p.4].

ATTACKER INTENTION (EVIL, SELFISH, HONEST)

An attacker who tries to impair the performance of the system, for example, by compromising RSUs, is called an evil attacker [10]. In a selfish attack on the other hand, the attackers seek to gain an advantage for themselves through influencing the system, for example by manipulating traffic lights [10]. A third dimension consists of honest-but-curious attackers, who may violate the participants' privacy [50], for example, by gathering data about vehicle drivers [10], [51].

C. THREATS AND VULNERABILITIES

Figure 3 provides a short overview over the threats and vulnerabilities described in the following sections. It links a threat with the corresponding STRIDE category and the relevant components of the DFD outlined in the previous section. The coloring of threats represents the STRIDE category they have been assigned to. Physical data breach (Section IV-C), physical denial of service (Section IV-C) and physical compromising (Section IV-C) are three key physical attacks threatening the VFC system, arising due to the cyber-physical nature of the VFC system.

SPOOFING

Spoofing refers to attacks aimed at identity disguise within the VFC system. We identified four major threats impacting

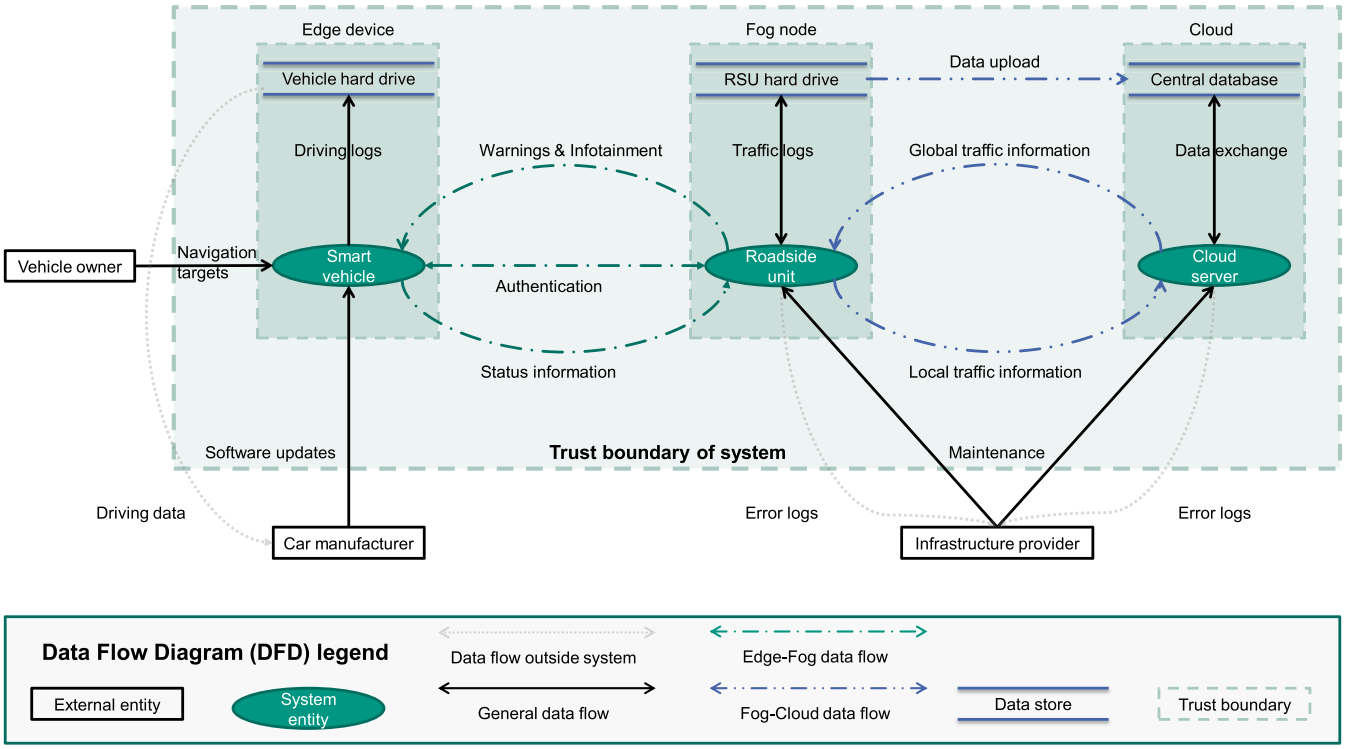


FIGURE 2. Data Flow Diagram (DFD) of our VFC system.

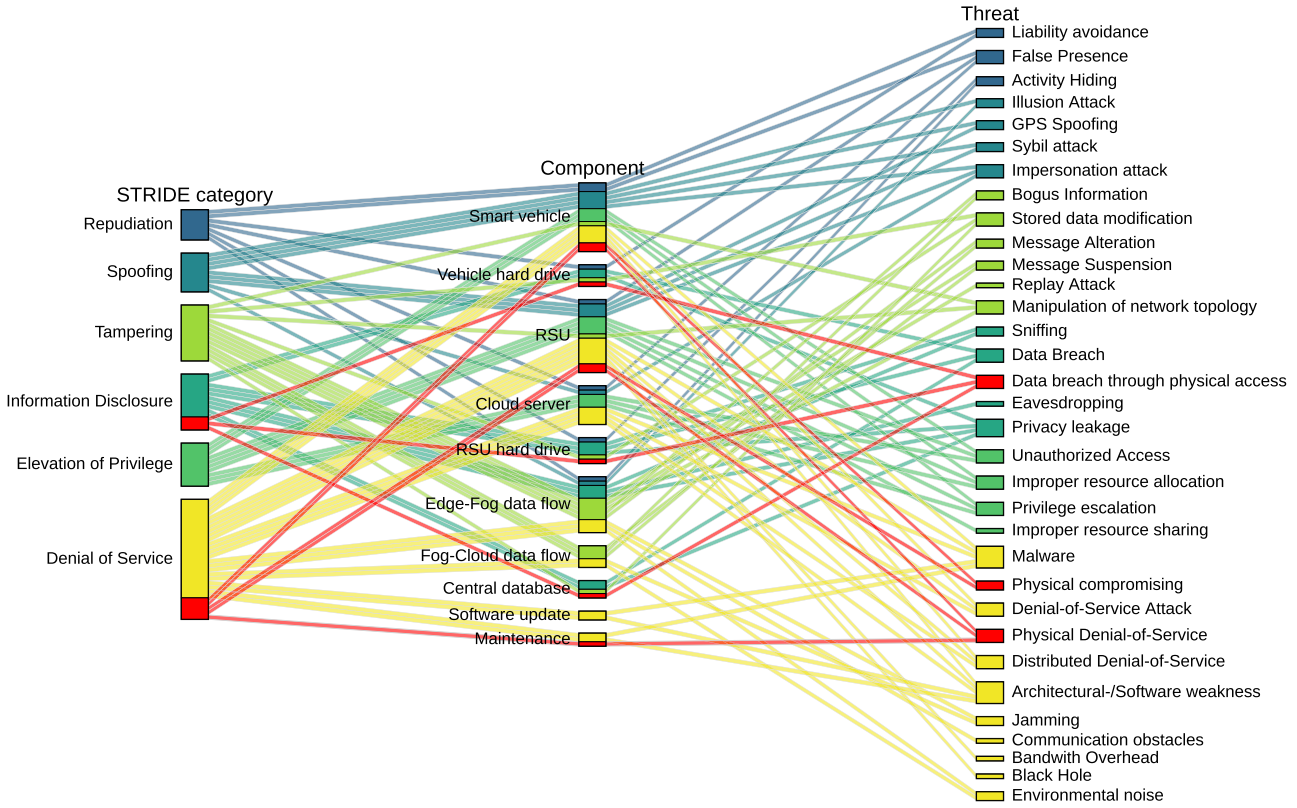


FIGURE 3. Threats matched to corresponding STRIDE categories and system components.

VFC security, namely impersonation attacks, sybil attacks, GPS spoofing, and illusion attacks. Table 4 summarizes threats belonging to the spoofing attack category.

IMPERSONATION ATTACK

In an impersonation attack, sometimes called rogue entity attack, attackers masquerade themselves as another identity

TABLE 4. Threats assigned to spoofing.

Threats	References	Short Description	Attacked Entities
Impersonation Attack	[32], [37], [49]–[56] E-1, E-2, E-4	Imitation of a legitimate user	Smart vehicle, RSU, Cloud server
Sybil Attack	[32], [37], [49], [56], [57] E-12	Introduction of ghost identities by one attacker	Smart vehicle, RSU
GPS Spoofing	[49], [55], [57], [58], E-9	Cheating on the GPS position	Smart vehicle, RSU
Illusion Attack	[49], [56], [57]	Broadcasting a traffic warning message to create illusion	Smart vehicle, Edge-Fog data flow

[E-4] [55]. In VFC, attackers could compromise another vehicle's user account, authenticate themselves to a fog node and impersonate this vehicle [E-2]. In case attackers successfully impersonate an edge device, a fog node's authentication mechanism cannot distinguish the attacker's fake credentials from proper credentials so that the system is vulnerable to malicious commands [53]. Evil and selfish attackers can also pretend to be authenticated as a fog node and to report data honestly with the aim to get benefits and/or to spread false information [32], [37], [49]. Attackers could introduce a fake fog node to launch a in literature well-known Man-in-the-Middle (MITM) attack by inserting themselves between sender and receiver [E-2]. They could also disguise themselves as a data center or the whole infrastructure even though the likelihood of occurrence is low [50]. Once pretending to be a VFC entity, attackers may send selected information to a fog network without the participating entities recognizing that the information originates from a dummy [E-1]. The usage of IP Spoofing allows attackers to remain anonymous during the attack [54].

SYBIL ATTACK

When performing a sybil attack, attackers jam the fog network by introducing false edge device identities. A legitimate vehicle believes that it has received a message from another legitimate vehicle even though it was sent by attackers. The real identity of the attackers cannot be detected [57]. This can lead to the generation of ''ghost'' vehicles through forged messages [56]. For the controller fog node and other vehicles, it looks like multiple different vehicles send messages but it is actually one attacker who broadcasts messages [37]. If, for example, a navigation service measures road traffic density to bypass congestion, attackers could gain free passage by introducing fake sybils on their route [E-12].

GPS SPOOFING

The GPS location of an entity is manipulated, which is harmful when this information is necessary to make certain decisions [E-9] so that GPS spoofing can be used to initiate serious attacks [58]. If attackers are cheating on their GPS position, nearby vehicles receive false location information [59]. This can be achieved by using a transmitter that generates localization signals that are stronger than real signals from GPS satellites [55], [57]. Attackers could tell a fog node their location on the highway and erroneously indicate that they are only moving at 10km/h, so the system assumes they are in slow-moving traffic. This would worsen a navigation system's service [E-9], among others. Furthermore, erroneous GPS locations could lead to a navigation system not detecting a traffic jam so that ''*people who rely on such a system or like to work with assistants would possibly encounter a traffic jam at an unexpectedly high speed*'' [E-9]. This is particularly critical in case of routing ambulances as fast as possible through traffic. Likewise, false GPS data may increase the chance of accidents because vehicles nearby may activate break or evasion routines automatically, leading to unforeseen and surprising vehicle behavior.

ILLUSION ATTACK

In an illusion attack, attackers broadcast a false traffic warning message to surrounding vehicles. If this message passes all validation processes, it is accepted and transmitted to further vehicles giving an illusion to other drivers [56], [57]. For example, reporting unjustified black ice warning on a street, so that the navigation systems recommend another route to other vehicles, can deliver the benefit of a clear passage to the attacker. False claims like these could also interfere with pre-aligned diplomatic routes, force detouring and thus bring safety hazards with them.

TAMPERING

Tampering refers to manipulation of data in any component of the VFC system. We identified six threats that are assigned to the tampering attack category, including bogus information, stored data modification, message alteration and suspension, replay attack, and manipulation of network topology (see Table 5).

BOGUS INFORMATION

A bogus information attack implies that wrong information is sent in the network such that the integrity in the VFC system is affected [E-3], [E-5], [60]. Bogus information could be wrong messages [E-7], [18], [55], [56] or injected information [E-8], [50], [52] which is deliberately manipulated [E-1], or forged GPS signals to mislead vehicles due to wrong location information [55]. When attackers are able to access a fog node, they could adjust or fake signals that are sent to a vehicle [E-8]. The potential damage caused by the infiltration of bogus information is compounded because the change is usually not detected and the system keeps running [E-1, E-7]. ''The fog node keeps running without it being detected that false information has been fed in. This means that you can manipulate this system much more precisely according to your own ideas'' [E-1]. Furthermore, the attackers ''could send false information that limits the functionality of my vehicle without the vehicle being able to recognize that it is

TABLE 5. Threats assigned to tampering.

Threats	References	Short Description	Attacked Entities
Bogus Information	[18], [37], [49], [50], [52], [55], [56], [60] E-1, E-2, E-3, E-5, E-7, E-8	Transmitting wrong information	Edge-Fog data flow, Fog-Cloud data flow
Stored Data Modification	[37], [49], [53], [55] E-1, E-2, E-3, E-4, E-7, E-11	Logs or stored data are modified	Vehicle hard drive, RSU hard drive, Central database
Message Alteration	[18], [37], [49], [50], [53], [55]–[57] E-2, E-3, E-4, E-5, E-9, E-12	Altering a sent message in transmission	Edge-Fog data flow, Fog-Cloud data flow
Message Suspension	[37], [49], E-3, E-7, E-9	Dropping messages or holding them before forwarding	Edge-Fog data flow, Fog-Cloud data flow
Replay Attack	[49], [53], [57], E-7	Replaying a previously transmitted message	Edge-Fog data flow
Manipulation of Network Topology	[55]	Modifying the topology information	Smart vehicle, RSU, Edge-Fog data flow

receiving false information'' [E-7]. Besides that, ''a vehicle itself could send wrong data, which might lead to wrong decisions in the fog'' [E-2]. The fog node and the edge devices or rather the connection between the two components is affected by the attack [E-1, E-2, E-3]. ''When the vehicle navigates and I just tell him, at the next traffic light it's green, you can drive over [...], then your vehicle would probably cross over. Or I say you turn right at the next light and you are not allowed to turn right. I could do something like that to manipulate the vehicle and do some sort of stupid thing'' [E-7].

STORED DATA MODIFICATION

Attackers could modify stored data in RSUs [E-3], [E-11] [37]. If the attackers are able to access the data (e.g., logs), they are able to insert, modify, replicate or delete data (e.g., to induce wrong decisions by law enforcement agencies or affect the storage's integrity [E-7], [37]). One could easily envision an attacker prying open a physical casing of an RSU in case its physical protection is insufficient [60]. The gained access to its interface could then lead to altering of the data stored on it [E-2, E-4]. This could result in decisions being made on the basis of the modified data, and thus these decisions being wrong [E-2]. The difficulty of modifying data might vary depending on the type of data so that it is probably more difficult to manipulate speed, safety distance or the brake information than broken components of a vehicle stored in the node [E-1]. A cascading failure could result ''if certain information in a fog node is manipulated and this information is incorrectly passed on to the other node, which then performs calculations etc. on this information: this can result in manipulative behavior from one fog node to all other fog nodes'' [E-1].

MESSAGE ALTERATION

In a message alteration attack, information that passes through an RSU is modified [56]. This weakness arises from a weak or not encrypted communication channel and can cause malfunctions that endanger the drivers' or pedestrians' safety [18], [37], [53]. Message alteration can be performed by MITM attackers that insert themselves between sender and receiver. This enables them to modify the original message [E-2], [E-3], [E-5], [E-9], [50], [57]. ''When it comes to designing the traffic light system, a MITM could perhaps pass on incorrect data about the traffic volume'' [E-3]. This attack is facilitated by improper access control and message encryption [55]. The messages could be altered by ''interspersing an interfering signal and thereby tipping any bits from 0 to 1'' [E-12]. For example, an RSU could advise a traffic light to turn red. However, this message will be modified so that the traffic light turns green and an accident may occur [E-3]. In addition, attackers ''could collect warnings for black ice from one fog node and change them so that everything seems to be fine, and send them to the other fog node, which should broadcast the warning. Then there would probably be a mass collision because everybody is relying on the information being correct and there is a wrong one coming'' [E-4].

MESSAGE SUSPENSION

If attackers capture an encrypted package, they might not be able to view the content but they could suspend the message [E-9]. A malicious RSU either drops messages [37] or holds them before selectively forwarding them [E-9], [37], [49]. This allows the attackers to keep information about accidents or sensitive information about themselves secret [37]. For example, the attackers could intervene between the traffic light and the corresponding RSU and block the signals [E-3]. Furthermore, if event processing is used, the attackers could either drop or re-schedule security relevant events, or forward manipulated ones [E-7]. Intercepting and suspending messages can be seen as a form of MITM attack [18].

REPLAY ATTACK

In a replay attack, attackers could ''*extract information, evaluate it and then, if necessary, intervene at the right place*'' [E-7] by transmitting it to another entity, supposedly one that is under control of the attacker. A previously transmitted message is replayed to, for instance, manipulate the vehicle locations [57]. Furthermore, an authentication session could be captured and then repeated by unauthorized parties [53].

MANIPULATION OF NETWORK TOPOLOGY

Attackers could also modify the topology information by hijacking the location of vehicles or fog nodes, or by injecting false links in the topology [55]. As a consequence, for example, data routing inside the fog network may be delayed, leading to further cascading or escalating effects (e.g., warning messages are not received in time).

TABLE 6. Threats assigned to repudiation.

Threats	References	Short Description	Attacked Entities
Liability Avoidance	[10], [18], [37]	Denying an action	Smart vehicle, Vehicle hard drive
False Presence	[37], E-1, E-7	Claiming to be in another location	Smart vehicle, RSU, Cloud server
Activity Hiding	[37]	Preventing activities from being logged	Edge-Fog data flow, RSU hard drive

REPUDIATION

Repudiation refers to denying actions that have already been executed within the system. We identified three threats that can be assigned to repudiation, namely liability avoidance, false presence, and activity hiding (refer to Table 6).

LIABILITY AVOIDANCE

Attackers could intend to deny a previous action. In an overall sense, attackers could deny to have sent data or a message [10], [18]. If the attackers cause a road accident, they may deny it by providing wrong information to RSUs or deleting outsourced storage data. Possible examples for messages that may be denied are application offloading requests or results, and data for crowdsensing or crowdsourcing [18]. Similar, a selfish attacker could consume fog services and then deny service usage afterwards [37].

FALSE PRESENCE

"An attacker could pretend to the cloud that the edge devices did something they haven't done" [E-7]. The VFC system is mostly highly location sensitive. Hence, an attack where the attackers claim to be present in a location without actually being there can be severe [37]. This could lead to a fog node thinking "that there is a large traffic jam, so other navigation systems would bypass such roads" [E-1]. A malicious navigation system provider could advertise that "the way [the provider] leads the routes, people actually get there much faster than all the others" [E-1].

ACTIVITY HIDING

Attackers intend to prevent their activities from being logged. Thereby, they cannot be convicted for their actions in future investigations [37]. Such activities could include location information of vehicles or hiding activities like acceleration or speed. Forensic science could be set back by this attack, especially when identifying a crime offender (e.g., in a car accident) without witnesses, heavily relying on data stored in vehicles, RSUs and nearby surveillance devices.

INFORMATION DISCLOSURE

Information disclosure refers to the revelation of data. Attacks in this category are not aimed at disrupting the system and can thus be categorized as passive. Threats assigned to information disclosure include sniffing, data breaches, eavesdropping, and privacy leakage, as seen in Table 7.

TABLE 7. Threats assigned to information disclosure.

Threats	References	Short Description	Attacked Entities
Sniffing	[18], [49], E-11	Reading communication between entities	Edge-Fog data flow, RSU hard drive
Data Breach	[37], [53], [55], [60] E-2, E-3, E-4, E-7, E-10, E-12	Stealing, disclosing data	Vehicle hard drive, RSU hard drive, Central database
Data Breach through Physical Access	[53], [55] E-7, E-12	Data breach achieved via physical actions	Vehicle hard drive, RSU hard drive, Central database
Eavesdropping	[18], [50], [51], [57] E-2, E-3, E-4, E-7, E-8, E-11	Secretly listening to private communication	Edge-Fog data flow
Privacy Leakage	[18], [32], [49], [50], [52], [55], [57], [58] E-2, E-3, E-5, E-7, E-8, E-12	Disclosing confidential information	Edge-Fog data flow, Vehicle hard drive, RSU hard drive, Central database

SNIFFING

In this attack scenario, attackers can analyze network traffic between entities within the VFC system [18]. An instance of sniffing is the interception of messages between vehicles and RSUs, thus targeting the fog-edge communication [E-11]. Snooping on cache and storage data is a similar attack, where the information stored on RSUs gets extracted by unauthorized entities [E-11], [18]. Sniffing on messages sent through unprotected communication channels requires little effort [18], making the use of encryption to shield these channels essential to the security of the VFC system.

DATA BREACH

As canonical security and privacy issue, data breaches characterize the theft, leakage or interception of sensitive information to a distrusted environment [18], [55], for example, due to inefficient or lacking encryption protocols. An attacker could for instance intercept vehicle location information to generate and sell personalized movement profiles of system users [E-2, E-3]. This affects all levels of the VFC system [E-2, E-3, E-4], with attackers having an incentive to attack entities on higher levels of the hierarchy compared to edge devices [E-4, E-10] due to their increased data storage capabilities. The indicated potential access to more information results in an increased financial incentive for attackers [E-2, E-7, E-10].

DATA BREACH THROUGH PHYSICAL ACCESS

A VFC system is also at risk from physical data breaches due to its cyber-physical nature [53]. Smart vehicles and especially RSUs need to locally store and aggregate data, which can be the target of adversaries through physical access [53]. Physical access to an RSU could for instance lead to a data breach that violates a user's privacy [E-7], [55]. Since smart vehicles are in possession of end users, it is "*essentially impossible*" to prevent physical access to system hardware [E-12]. In a realistic scenario, this access could for instance

be used to hack the vehicle's software to extract cryptographic keys from its system [E-12].

EAVESDROPPING

Unauthorized listening to data exchange between any two entities and capturing information that violates a user's privacy is considered eavesdropping [E-2], [E-4], [E-7], [51]. In the context of VFC this corresponds to the interception of wireless messages [E-8] or Bluetooth communication [E-7] between smart vehicles [E-4]. More concretely, attackers could place small Bluetooth receivers at intersections to permanently monitor the data traffic or (sensitive) information exchange in an area [E-7]. Since eavesdropping does not directly harm the system, it is difficult to discover [37]. Additionally it is noteworthy that internal attackers with "*detailed information which hardware components are used to realize the communication*" [E-3] have an inherent advantage over external attackers [E-3]. The mentioned MITM attackers could also launch an eavesdropping attack and gather sensitive information about users [E-2], [37], [50].

PRIVACY LEAKAGE

When sensitive vehicle, location or personal information [37] transmitted between or stored in edge, fog and cloud resources can be accessed by both internal adversaries or someone who is honest but curious [50], [57] it is called a privacy leakage [E-2, E-3, E-12]. Potential privacy attacks leading to exposure of confidential private information are route discovery attacks [58], storage information disclosure [E-2], network profiling [E-7], driver information disclosure [E-3], [E-12], [37] and hacking passwords [E-7], [50], among others. A potential implementation of such an attack could be the theft of data from a camera supervising an intersection leading to identification of pedestrians [E-2]. Adversaries could also intercept location data and combine it with vehicle licensing information to generate personalized movement profiles [E-3, E-5, E-7], potentially making target persons vulnerable [E-12]. Information disclosed in these ways has different privacy levels and different scope. With regards to privacy, smart vehicles contain the most sensitive information but with limited scope [E-8]. Extracted data is limited to the single device. RSUs encompass a wider scope of information from many local devices, yet the information content could be less sensitive than in edge devices due to aggregation, pseudonymization or anonymization functions [50]. The cloud level comprises the widest scope and but may store the least sensitive content among all entities within the VFC system that commonly relies on latency-aware prepossessing and aggregation of data.

DENIAL OF SERVICE

DoS attacks are referring to system disruptions that lead to unavailability. This classifies them as active attacks. DoS threats comprise jamming, malware, physical compromising, communication obstacles, bandwidth overhead, (distributed/physical) denial of service attacks, black holes, architectural or software weaknesses, and environmental noise, as summarized in Table 8.

TABLE 8. Threats assigned to Denial of Service (DoS).

Threats	References	Short Description	Attacked Entities
Jamming	[18], [49], [50], [53], [55], [57], [58], [60] E-9, E-11, E-12	Disturbing the signal	Edge-Fog data flow, Fog-Cloud data flow
Malware	[49], [50], [53], [57], [58] E-4, E-6, E-7, E-10	Injecting disruptive code	Smart vehicle, RSU, Cloud server, Software update, Maintenance
Physical compromising	[10], [49], [53] E-2, E-7	System disruption through physical capture of component	Smart vehicle, RSU
Communication Obstacles	[18], [53]	Physical objects prohibit communication	Edge-Fog data flow
Bandwidth Overhead	[49], [53], E-2, E-3, E-7, E-8	Limited capacity for communication	RSU
Denial of Service Attack	[18], [37], [49], [52], [53], [55], [57], [58] E-1, E-2, E-4, E-5, E-7, E-9, E-10, E-12	Fake requests overload the system	Smart vehicle, RSU, Cloud server
Physical Denial of Service	[49], [53], [55], [57] E-1, E-2, E-7, E-12	Incapacitating system components via physical actions	Smart vehicle, RSU, Maintenance
Distributed Denial of Service Attack	[18], [49], [50], [54], [55] E-2, E-7, E-8, E-11	Fake requests from different entities overload the system	Smart vehicle, RSU, Cloud server
Black Hole	[49], [57]	Disrupted node swallowing information	RSU
Architectural-/ Software Weaknesses	[49], [50] E-1, E-2, E-3, E-4, E-5	Weakness resulting from power cuts or erroneous source code	Smart vehicle, RSU, Cloud server, Software update, Maintenance
Environmental Noise	[53]	Natural noise disturbing the signal	Edge-Fog data flow, Fog-Cloud data flow

JAMMING

Attackers generate high-frequency noise to disrupt wireless communication channels, inhibiting the transmission of (critical) data within the system [E-9], [E-12], [57]. Jamming can either target specific frequencies with specialized devices [E-9] or more generally disturb all broadband wireless connections within an area [E-9], E-12]. An example attacker could use a high voltage traveling arc to locally disrupt all WiFi communication, thus also rendering the VFC system inactive in a narrow space [E-9]. Both the edge-fog and fog-cloud communication channels can be subject to this attack with the consequence that the affected fog or cloud resources get inaccessible to an extent that messages cannot pass among the entities [E-9], [37], risking unreachability of cloud servers and/or RSUs. Jamming is challenging to prevent when transmitting data by radio frequency with edge-fog

communication being at a particular risk due to it being inherently wireless [E-9].

MALWARE

Injecting malware into the VFC system can affect the operation of the network to a serious extent [E-4], [E-10], [58] and lead to, for example, software errors and security vulnerabilities [53]. Malware exists in many different forms and is aimed at compromising the availability of the system [49] by preventing main functions from being carried out, and can therefore be categorized as a DoS attack. While smart vehicles are at a particular risk of being infected [E-4], it is also possible for malicious actors to inject Trojans into various entities of the VFC system. The data stored on an RSU and its capabilities within the network make it a more attractive target compared to a vehicle [E-7]. Particular devastating attacks could also be caused by software back-doors from criminal suppliers [E-6].

PHYSICAL COMPROMISING

Attackers may launch malware attacks via hardware interfaces of entities, such as USB ports [E-2, E-7], if they have physical access to these interfaces [53]. While physical compromising is theoretically feasible on all levels of the hierarchy, RSUs and edge devices with insufficient physical protection are at a particular risk [E-7], [49]. This is caused by their widespread distribution over an area, complicating the provision of physical security compared to centralized data centers [E-2], [E-7], [10]. Once an RSU is compromised by physical means it can then be used to launch attacks disrupting the process of traffic control or other functionalities [10].

COMMUNICATION OBSTACLES

Communication obstacles can be physical objects placed between two communicating entities (e.g., in the VFC system between two vehicles or between a vehicle and an RSU) causing no line of sight [18]. This phenomenon can have serious consequences. As an example, an RSU that is responsible for traffic instructions at a crossing gets blocked by a communication obstacle so that edge devices from the north (cars and smart traffic lights) cannot receive its messages. In case of emergency traffic light management (e.g., green wave series of traffic lights for an ambulance) the message to the north traffic light ''turn red'' could fail to be delivered, putting lives at risk.

BANDWIDTH OVERHEAD

In VFC, low latency is important to avoid safety-critical issues and can be achieved by minimized distance and narrow bandwidth [53]. However, insufficient bandwidth capacity of RSUs to address the increased traffic data due to inefficient cryptography and authentication methods [53] leads to communication overhead, signal interference and signal issues as consequences [E-2], [E-8] [58]. Since Bluetooth communication, for instance, can only deal with certain frequency bands and limited quantities of devices, its bandwidth can easily be reduced by large numbers of units transmitting on the same spectrum [E-7].

Denial of Service (DoS) ATTACK

System overloading - such as flooding, spamming [58], fake requests [37] - can cause temporary service disruptions [E-4] in VFC. Breakdown of the system is achieved via sending a large number of requests from the same IP [E-2] or by spamming system entities with TCP packages once a connection is established [E-7]. While in theory all levels of the system are susceptible to DoS attacks, RSUs and especially smart vehicles are more at risk because of their limited storage and data processing capabilities [E-7, E-9]. However, it might be more enticing for attackers to focus on devices in the fog layer due to their intermediate role in the VFC hierarchy [E-1]. A typical DoS attack in the context of VFC could comprise multiple hacked vehicles or sensors spamming fog nodes or other vehicles with requests [E-1, E-5]. This type of attack is particularly effective in areas with dangerous traffic situations like railroad crossings [E-10]. On the other hand, taking over an RSU gives malicious actors the possibility of compromising road security by flooding individual vehicles with useless information [E-7]. In general, DoS attacks are threats of particular importance because they require little knowledge and can easily be conducted with cheap hardware [E-12].

Physical Denial of Service (PDoS) ATTACK

In addition to being vulnerable to canonical DoS attacks, the accessibility and visibility of RSUs (e.g., due to antennas [E-12]) enables adversaries to physically attack them with the goal of destruction [57]. Based on the information gathered from our interviews, we define a *PDoS attack as a DoS attack launched in the physical space causing unavailability of a digital service*. The PDoS attack thus exploits the cyber-physical manifestation of a system, where damage caused in the real world may have spillover effects into the cyber domain of the system. This stands in contrast to typical DoS attacks, which are executed purely in the digital space. If RSUs are, for instance, mounted on top of traffic lights, attackers could sever their antennas or cable connections using a bolt cutter [E-12]. In case the RSUs are placed on the ground, running them over unintentionally or intentionally with vehicles is also an option [E-2], E-12]. While it is possible that the destruction of an RSU results from natural causes like storms [E-1], evil and selfish attackers could be motivated by financial incentives or by a desire to disturb the VFC system on purpose [E-12]. Vandalism sparked by technophobia has already become an issue for autonomous vehicles and is also a conceivable threat to VFC systems [E-12], [61]. A more sophisticated physical attacker could also pry open an RSU's physical protection in order to deactivate it [E-4], E-12]. On the other hand, theft of components motivated by potential financial gains could result in a possible network disruption or power incision [37].

In an example case, on-site maintenance workers could easily strip RSUs or smart vehicles due to their small size [E-7]. Vehicle theft of course is going to be another common instance of this attack [E-10]. PDoS attacks are easy to conduct since they require little technical background and can be performed using everyday mechanical equipment like a bolt cutter.

Distributed Denial of Service (DDoS) ATTACK

This attack is performed similarly to DoS attacks by flooding meaningless messages or resource requests to exhaust the resources of entities (mostly RSUs) [E-2], [37], [54]. It also has the same goal: Suspension of the system [E-7]. Unlike DoS attacks, DDoS is harder to detect and defend from because it is performed in distributed fashion by multiple malicious entities [E-2], [37]. Using, for example, a multitude of hacked cars would allow attackers to overload the system at a larger scale [E-2] compared to the targeting of single units like smart vehicles [E-7] or RSUs [E-7, E-8]. This could lead to large scale disruptions of traffic due to failing navigation services [E-7] and accidents [E-2], E-11], among others.

BLACK HOLE

In this kind of attack, attackers manipulate the network by embedding a faked malicious RSU that indicates it is part of the network while in reality the node does not exist. Inserting such a black hole RSU leads to redirecting messages to the false and non-existent network node, causing data loss [57]. A consequence of such an attack is the possible unavailability of the VFC system in a specific region due communication requests not being answered. Variations of this attack include the grey-hole, in which only network packages from certain sources are removed or the sinkhole, in which network traffic is first routed to an RSU before launching a subsequent attack from that RSU [49].

ARCHITECTURAL AND SOFTWARE WEAKNESSES

Hardware and software failures - resulting from erroneous source code or poor maintenance - as well as power cuts could disrupt the availability of the system [49], [50]. The overloading of a single RSU could for instance lead to cascading effects in the whole system if the level of component redundancy is not sufficient [E-1, E-2], which is an instance of an architectural weakness. Since the inherently hierarchical structure of the VFC system leads to multiple points of attack [E-5], it is also possible for false information to propagate up the hierarchy [E-1]. On the software side, real-world complex systems are prone to bugs and security holes which can be exploited [E-2], particularly on the vehicle level [E-1, E-2].

ENVIRONMENTAL NOISE

Surrounding noises can cause disruption to the communication channel or even stop communication entirely [53]. A common example of such a threat are possible network disruptions induced by a lightning storm, cutting off transmission of wireless data between entities in the system. Despite their being no malicious intent, environmental noise needs to be accounted for when designing a VFC system as the scale on which a disruptions occur may potentially be larger than those caused by human actors.

TABLE 9. Threats assigned to elevation of privilege.

Threats	References	Short Description	Attacked Entity
Unauthorizec Access	[18], [53], [58] E-1, E-2, E-8, E-10, E-11, E-12	Gaining access without authorization	Smart vehicle, RSU, Cloud server
Improper Resource Allocation	[37]	Gaining more resources than the fair share	Smart vehicle, RSU, Cloud server
Improper Resource Sharing	[37]	Being privileged of resource providing among other fog nodes	RSU
Privilege Escalation	[50], [57], E-10	Abusing legitimate privilege	Smart vehicle, RSU, Cloud server

ELEVATION OF PRIVILEGE

Elevation of privilege refers to unauthorized access to resources in the VFC system. Threats assigned to the elevation of privilege include unauthorized access, improper resource allocation, improper resource sharing, and privilege escalation, as summarized in Table 9.

UNAUTHORIZED ACCESS

Unauthorized entities may enter the VFC system pretending to be someone else and abuse this access [18]. On one hand, the takeover of edge devices like smart vehicles is a general problem in VFC and Internet of Things [E-1], E-2], [E-10], possibly leading to unauthorized access to RSUs [E-8]. Access for malicious actors to certificates in particular is hard to prevent [E-8] so that the system has to be designed under the assumption that a certain number of edge devices is controlled by attackers [E-12]. On the other hand, attacking the central cloud server leads to extensive access to the system and might thus be more desirable to attackers but also more challenging since cloud services typically employ robust security measures [E-10], [E-11].

IMPROPER RESOURCE ALLOCATION

Resources offered by RSUs are optimally allocated according to system requirements to ensure fairness among users, who can expect a fair share of the available heterogeneous resources like computational power, storage or networking resources. Attackers (e.g., vehicle drivers) can elevate their privilege to gain more of these resources so that a fair resource allocation is not ensured anymore [37]. This does not only result in benefits for the attacker but can also lead to an insufficient amount of resources distributed to other vehicles and affect the availability of services offered to them.

PRIVILEGE ESCALATION

External attackers can take control over parts of the system thus increasing their privileges by exploiting software bugs, design flaws or configuration oversight [E-10]. This attack can also be performed by internal adversaries that abuse their privileges and take advantage of their insider knowledge [50]. Different forms of privilege escalation commonly exist, such as vertical privilege escalation, where attackers can access functions or data reserved for higher privilege users (e.g., being able to write and read data into the data storage, instead of reading data only), or horizontal privilege escalation, where attackers gain access to functions or data that other users with similar privileges typically can access. Once further privileges are gained, the attackers can perform unauthorized actions, such as shutting down RSUs, extracting data, or changing resource allocations.

IMPROPER RESOURCE SHARING

In this attack scenario, an RSU increases its importance in the network, for example, by changing the network topology, performing DDoS attacks on other nodes to disturb their operation, or re-routing intercepted functions or calls of smart vehicles. As a consequence, a vehicle uses its resources more than the resources of other RSUs. In such cases, fair resource sharing among users is not guaranteed anymore, which imbalances the financial gain [37]. Selfish attackers can maximize profits of allied RSUs, while at the same time damage related RSUs in the network.

D. OUTLOOK ON THREAT MITIGATION STRATEGIES

To overcome the threats and vulnerabilities in VFC, relevant prevention, detection and mitigation strategies have been introduced in the literature. Some of them are common security concepts, like encryption or authorization mechanisms, and some are specific to VFC, like resource allocation- and trust management. Securing VFC systems is important, however, no "*absolute security*" can be guaranteed or achieved [E-9]. Besides threats, our literature review and interview findings reveal potential security concepts for VFC, which can also be assigned to STRIDE categories (refer to Table 10, Table 12, and Figure 4). In the following, we will briefly elaborate on potential security measures to guide future research.

Security plays an important role in making VFC systems both secure and safe to use. Without security concepts, the above mentioned attacks could cause chaos and disturbance [E-11] and could even have fatal consequences, jeopardizing the safety of people [E-4,E-5, E-8,E-19]. For the novel challenges that VFC brings, new security measures need to be developed to withstand them. Proper network isolation, for instance, addresses the security concern that a malicious RSU can transmit threats to connected RSUs [52], thus ensuring availability and undisturbed operation.

The confidentiality of VFC systems has also been emphasized by many authors and experts. As we have revealed, several attacks aim to disclose private information.

TABLE 10. Security concepts assigned to STRIDE categories.

STRIDE categories	Security concepts	Short description
Spoofing	Access control Authentication Message verification Protocols Trust management	Selectively restricting access based on identification Identity verification Verification of correctness through other entities Rules regarding communication Trust-based access control
Tampering	Encryption Fault detection Forensics Intrusion detection Isolation Message verification	Encoding information in cryptic form Detecting faulty operation Analytics to detect "crime" System to detect and identify intruders Minimizing connections to other parts of the system Verification of correctness through other entities
Repudiation	Authentication Message verification	Identity verification Verification of correctness through other entities
Information Disclosure	Anonymization Encryption Key management Protocols Role separation Trust management	Removing personal identifying information Encoding information in cryptic form Management of cryptographic keys Rules regarding communication Bundling of different authorization levels Trust-based access control
Denial of Service	Attack detection Backup Fault detection Firewall	Detecting (multiple) requests from malicious entities Redundancy of system elements Identifying faults with tolerancy level Network security to prevent unwanted communication
Elevation of Privilege	Authorization Patching Resource allocation Role separation	Official permission concept Regular security updates Fair allocation mechanism to distribute computational resources Bundling of different authorization levels

To preserve and secure privacy, novel mechanisms for encryption (searchable encryption [32], proxy (re-)encryption [32], [53]) and authentication (blind signature, pseudonym, anonymous identity based authentication [58], blockchain-based authentication [37]) have been introduced in extant literature. While these security measures ensure confidentiality, however, they don't deal with malicious entities that could have legitimate access to the system [50]. In this case, a trust management system can minimize the uncertainty of "*not knowing how my partner is going to behave*" by deploying reputational levels [50].

Complementing the literature, interviewed experts have indicated additional security measures that could remedy the aforementioned attacks (refer to Table 12). First of all, regular patching and undergoing relevant security updates [E-4] are critical both for smart vehicles and RSUs, as well as for the cloud. Security updates and patches could be controlled by the annual/ two-annual safety attestations from a certified authority (e.g., certification authorities or auditors) [E-4]. Firewalls including DDoS detection software and IP blocking mechanisms could also enhance the security and availability of the system [E-7]. Limiting the bandwidth and number of possible connections of an RSU may mitigate the possibility

TABLE 11. Overview over prior research in (vehicular) fog computing.

		Context of study	
		Fog computing in general	Vehicular fog computing
Focus of study	Examining system protection	**A** Typical research question: "*How can a fog computing system be protected?*" Example studies: [62]–[64]	**B** Typical research question: "*How can a VFC system be protected?*" Example studies: [16], [65]–[68]
	Identifying threats	**C** Typical research question: "*What are the most important threats to fog computing systems?*" Example studies: [12], [21], [69]–[72]	**D** **Typical research question:** *"What are the most important threats to VFC systems?"* **Example studies: [37], [59], this study**

of a (D)DoS attack as well [E-8]. Further security measures were mentioned such as flow trace protocols, certificates [E-10] and (open) standards [E-5, E-10] to protect the VFC system. To prevent data loss, data should be stored redundantly. In case an RSU cannot fulfill its function, the neighboring RSU, which has stored information of the disrupted RSU redundantly, could take over its place until the issue is solved [E-2, E-3]. On the other hand, system independence (e.g., a standalone functioning RSU without any connection to its neighboring RSUs) is able to restrict the disruption and prevent infecting other parts of the system [E-11].

V. RELATED WORK

This study developed a comprehensive threat model for VFC, aligning with and extending related research. Reviewing existing security-focused research on fog computing and VFC reveals that most existing studies make valuable contributions by examining the protection of fog computing systems, while neglecting to identify a threat model that considers VFC specifics.

Related work can be differentiated, among others, based on the context of the study (fog computing in general; or VFC) and its study focus (examining system protection; or identifying threats), as illustrated in Table 11. Based on this separation, quadrant A summarizes related works that focuses on technical safeguards for fog computing in general. For example, Yu et al. [63] propose a generic framework for constructing a fine-grained access control system that also guarantees security against side channel attacks, namely a fully secure leakage-resilient functional encryption scheme. Similar, a cryptographic solution to preserve data security in fog computing is proposed by Noura et al. [62].

A further stream of the literature focuses on the implementation of specific security measures for VFC systems, which is subsumed in quadrant B. To secure communication among vehicles, fog nodes and cloud servers, Wazid et al. [16] design a secure authenticated key management protocol. After mutual authentication between communicating entities, they establish session keys for secure communications. Likewise, Ma et al. [67] propose an authenticated key agreement protocol without bilinear pairing. Their protocol achieves mutual authentication, generates a securely agreed session key for secret communication, and supports privacy protection. Other security measures include an efficient revocation scheme for VFC using Merkle hash trees to provide a highly scalable mechanism for propagating revocation information [65]. In addition, several articles focus on the usage of blockchain to secure a VFC system, such as blockchain being used for anonymous authentication by Yao et al. [68], who introduce a blockchain-assisted lightweight anonymous authentication mechanism for fog computing services.

Related studies on technical safeguards inform our research when identifying prevalent security threats. More importantly, extant research provides the means to safeguard VFC systems, and can therefore be used as foundation to mitigate identified threats from this study. We also guide this stream of research by summarizing and synthesizing important security threats, supporting the development of further security safeguards and mapping of existing means to identified threats.

Quadrant C comprises literature which discusses security and privacy issues in a fog computing system. However, these works do not focus on VFC specifics but address threats on fog computing in general. For example, Khan et al. [12] provide a comprehensive overview of potential security issues in fog applications, determine the impact of those security issues, and discuss possible solutions. Likewise, Yi et al. [72] and Mukherjee et al. [70] outline challenges for security and privacy in fog computing as well. Potential threats for security and privacy issues of fog computing in Internet of Things environments are examined by Alrawais et al. [69] and Ni et al. [71]. Stojmenovic and Wen [21] analyze the application of fog computing in various scenarios and study security and privacy implications of fog computing with focus on the detection of man-in-the-middle attacks. While these example research articles provide valuable contributions, a detailed conceptualization of threats in a VFC context is currently lacking.

Prior research on VFC has already proposed potential threats or focused on overcoming specific threats by providing mitigation solutions [49], [53] (quadrant D). As such, Hoque and Hasan [37] provide a threat model for VFC, which also lists diverse threats and vulnerabilities like confidentiality, integrity, and availability attacks, among others. However, proposed threats lack theoretical and empirical validation, and corresponding threat descriptions remain

TABLE 12. An overview of potential security measures in VFC.

Security concept	References	Examples	Mitigates threats, e.g.
Access control	[49], [50], [53], [56], [58], E-1	Access control concept	Bogus information
Anonymization	[32], [53]	Anonymization of drivers' identity to preserve privacy	Privacy Leakage
Attack detection	[49], [53], [58], E-2, E-4, E-5	Abnormal behavior-, anomaly detection, Blocking malicious requests	Malware
Authentication	[18], [50], [53]–[56], [58] E-1, E-2, E-3, E-4, E-8, E-10, E-12	Public key infrastructure, Symmetric keys, Group signature	Unauthorized Access
Authorization	[49], [53], [56], E-10	Different authorization levels	Manipulation of Network Topology
Backup	[53], [58], E-2, E-3, E-4	Replication, Data backup	Stored Data Modification
Encryption	[10], [32], [37], [52], [53], [58], [73] [49], E-7	Message-, Communication channel-, Proxy encryption, Lightweight encryption, Hashes	Sniffing
Fault detection	[37], [49], [50], [56]	Fault tolerance, resilience, integrity analysis	Illusion Attack
Firewall	E-2, E-4, E-7, E-10	DDoS detection software, IP-blocking mechanism	Denial of Service Attack
Forensics	[10], [49], [50], [52], [53], [58]	Evidence-based digital forensics, Traffic-based analysis	Sybil Attack
Intrusion detection	[49], [50], [52], [53], [58]	Monitoring, Intrusion Detection System (IDS)	Black Hole
Isolation	[52]	Network isolation	Bandwith Overhead
Key management	[32], [53], [58], [73], E-12	Session keys, trusted authority, group key mechanism	Data Breach
Message verification	[49], [56], [58], E-12	Trustworthiness, plausibility of message, validation of emergency event	Illustion Attack
Patching	E-4	Security updates	Malware
Physical protection	[49], [50] E-1, E-4, E-7, E-11	Separate physical storage for logs	Physical compromising
Protocols	[50], [58] E-3, E-4, E-5, E-7, E-10	Standards, Security protocols, Policies	Bogus Information
Resource allocation	[37]	Resource allocation management	Improper Resource Allocation
Role separation	[50]	Role concept	Privilege Escalation
Trust management	[49], [50], [52], E-12	Establishing trust relationships between trust domains, Reputation management	Illusion Attack

short. In contrast, the study by Meneguette et al. [59] describes 12 threats in more detail but mainly takes an edge computing perspective, whereas this study focuses on fog computing while considering its connections to cloud services and edge devices. We build on these valuable research findings and not only synthesize their results, but also validate and enrich them through interviews with VFC experts. In addition, prior research has mostly neglected to consider physical attacks in threat modeling in which attackers have physical access to the components of a VFC system and the capability to harm those. In this study, we also considered a VFC system's cyber-physical nature and therefore gathered additional data on potential physical security threats.

VI. DISCUSSION

A. PRINCIPAL FINDINGS

Our study yields 33 threats (see Figure 3), which we grouped into the 6 STRIDE attack categories. The categories spoofing, tampering, information disclosure and DoS contain attacks that are consistently mentioned across both literature and interviewed experts. We note that some threats like liability

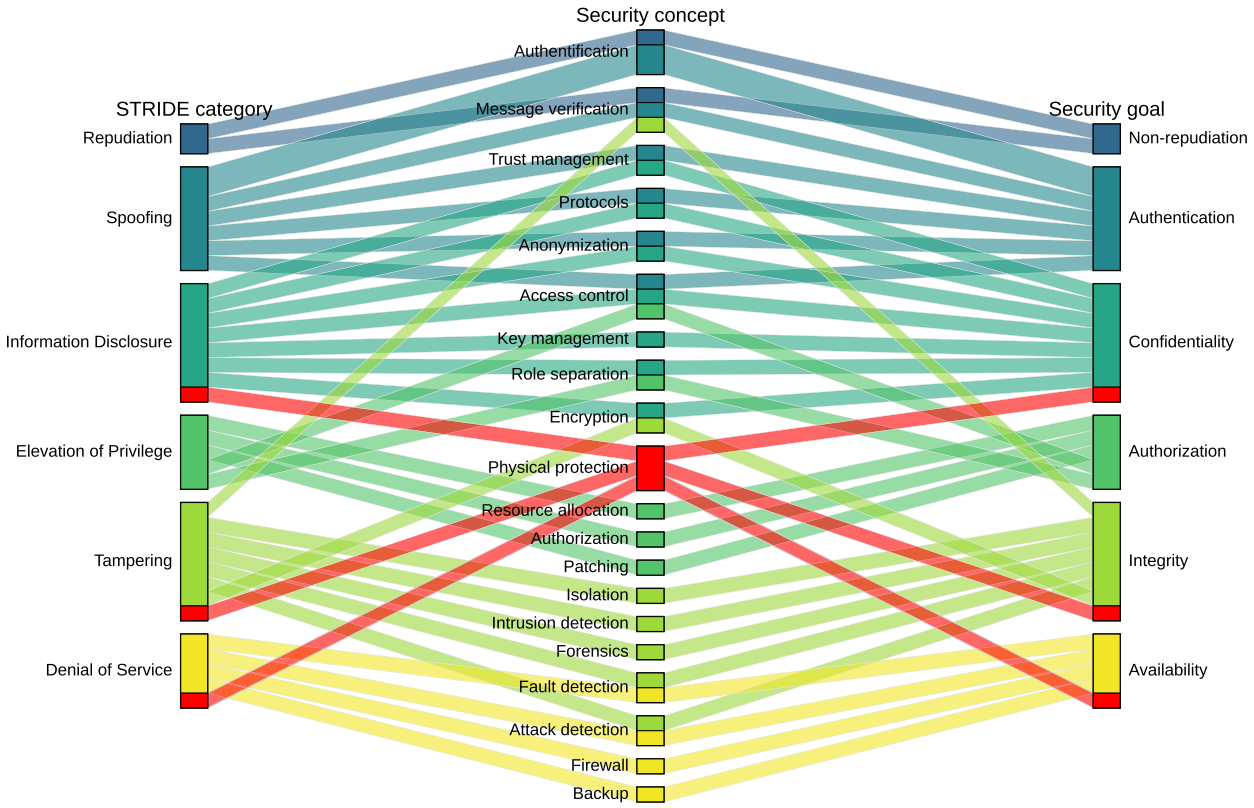


FIGURE 4. Connections between STRIDE categories, mitigation strategies and security goals.

avoidance or an illusion attack may be of more theoretical nature as they are referenced in multiple articles but could not be validated by the interviewed experts. Physical attacks on the other hand have been proposed in only two existing works [10], [37], yet are often mentioned in the expert interviews [E-1, E-2, E-4, E-7, E-10, E-11, E-12]. This underlines the importance of synthesizing knowledge from academic researchers and practitioners in the potential deployment of VFC systems.

Attackers may target different entities of the VFC system and potential entry points of them, including edge devices (e.g., smart vehicles), fog nodes (e.g., RSUs), cloud services, and data flows. Especially the interplay of and links between entities enables attackers to perform manifold attacks, such as impersonating smart vehicles to gain access to RSUs. Entities and corresponding threats should therefore not be treated in isolation but rather considered together in VFC threat models. Delving deeper into physical attacks, the experts also indicate that RSUs and smart vehicles are easier to physically attack compared to other technologies such as cloud services. The large amount of vehicles and RSUs as well as their scattered locations across a city makes them harder to survey and secure than data centers. Especially RSUs seem to be at a high risk of being physically attacked since they are at the core of the VFC system; further highlighting the importance of including physical attacks into a VFC threat model.

It should also be noted that several threats and attacks relate to compromising navigation systems, traffic routing, or the emergence of traffic congestion. While these threats may be burdensome for individual drivers that are on their way home after a demanding workday, they have a critical impact on businesses from the transportation sector (which rely on timely and safe delivery) and may even contribute to adverse effects on the whole economy. Road congestion is for example a very feasible result of many attacks described in Section IV and has been shown to have a negative relationship with overall employment in the economy [74].

In regard to our underlying attack model, we were also able to confirm different types of attackers, with varying capabilities and motives. Whereas we identified attack scenarios where active attackers seek to deliberately disrupt or destroy the functionality of the system (e.g., DoS attacks, jamming, and sniffing), our findings also show that selfish attackers may threaten the VFC system to gain an advantage for themselves through influencing the system (e.g., improper resource allocation or sharing).

Reflecting general characteristics of a VFC system, we want to note that it is a complex system per definition [8], exhibiting a high degree and amount of cyber-physical interdependencies within and beyond the system [75]. Such interdependencies raise the concern that an attack may have cascading or even escalating effects [E-10], not only leading to security and privacy issues, but also to dangers for

human life induced by failures in the VFC system's security measures [E-9, E-10, E-11]. We therefore propose that VFC systems can be regarded as a critical information infrastructure, referring to socio-technical systems comprising essential software components and information systems whose disruption or unintended consequences can have detrimental effects on vital societal functions or the health, safety, security, or economic and social well-being of people on a national and international level [76].

B. IMPLICATIONS FOR RESEARCH AND PRACTICE

Our work provides several contributions to research and practice by verifying and extending findings from extant literature through expert interviews. Practitioners can obtain insights into possible attack vectors in VFC along with example guidelines on how to mitigate those threats. These findings may then be used in defining requirements for a VFC system from a security perspective. As the complexity of the system and the heterogeneity of its devices ensures that "*it will never be 100% secure*" [E-11], fallback solutions become all the more important for a real-world deployment [E-4, E-9, E-11, E-12]. Here we can highlight two technical aspects of particularly high significance for practitioners: First, the continuous provision of security updates on the system as well as on the device level [E-2, E-4, E-10]. Second, the use of encryption technologies that manage the trade-off between speed and safety in a manner that facilitates the deployment of the system [E-10, E-11]. Since an application of VFC is likely a costly endeavor, adapting RSU density based on traffic volume in an area may be a consideration in practice [E-11]. On the non-technical side, an inevitable basic prerequisite for the feasibility of VFC in the real world is the provision of a legal framework. Without a clear definition of responsibilities and liability (e.g., for installing security updates), a large-scale realization of VFC will be impossible.

For research, we provide three major contributions (refer to Table 13). First, our study bridges the gap between the currently scattered literature on VFC threats. In total, we identified 33 threats and explained important facets of them. Reviewing extant research and applying Khan et al. [12]'s STRIDE threat modeling and further interview coding techniques enabled us to synthesize and harmonize extant research with practitioners' knowledge, thereby unifying the diverse views in a comprehensive threat model. By assigning our findings to the attack categories proposed by the STRIDE model, we not only achieved theoretical abstraction but also support future research aiming to develop common security mitigation strategies that are associated with these categories. We also briefly elaborated on security measures that can be used to overcome the vulnerabilities of a VFC system that came apparent from our research review and interviews, thereby further guiding future research that aims at overcoming the surveyed threats. With our overview of threats and potential mitigation strategies in VFC we also shed light on research areas that warrant further attention.

Second, extant research often mentions potential threats barely or superficially, most often to motivate their research or security mitigation strategies. As a consequence, most of the proposed threats lack empirical validation and detailed descriptions. With this survey paper, we extend prior research by providing richer descriptions of identified threats. In particular, interviewing experts helped us to validate proposed threats from prior research and gather further information on these threats. By providing more detailed description of threats, we not only increase researchers' understanding, but also help them to define requirements and boundary conditions of VFC systems and potential security measures.

Third, physical attacks related to VFC have been neglected so far. For example, Hoque and Hasan [37] argue that extant threat models "do not consider the physical attacks" [37, p. 1056] and briefly state example physical attacks (e.g., "power incision, hardware tampering, RSU component theft, network disruption, storage theft, etc." [37, p. 1056]) to illustrate their potential impact in a VFC context. However, extant VFC research falls short in deriving and explaining physical attacks. To counteract this research gap, we particularly identified three physical attacks that may be used to threaten the VFC system but have not been thoroughly examined by prior research. Deepening the understanding of physical attacks through expert interviews allowed us to fill an important gap in extant research, thereby linking research and practice. Our findings on physical attacks also underline the importance of understanding VFC as a cyber-physical system, requiring not only security but also safety mitigation strategies.

C. LIMITATIONS

Nevertheless, our study comes with limitations. The literature review on threats and security measures relies on already published scientific articles on VFC. While there is more research available in the larger and more general fields of VANETs, fog or edge computing, we chose to limit the scope of our work to attacks and security solutions that are most relevant to the VFC context. We tried to overcome this limitation by adding interviews from several experts from both research and industry. The experts are mostly based in Germany and thus their opinions rely on local traffic situations and regulations, which might differ substantially from, for example, Asian countries or the USA, thereby reducing the generalizability of our findings to other countries. An avenue for future work on the practical side is thus the conduction of similar studies in other countries. Nevertheless, we tried to tackle this generalization issue by focusing on core technical capabilities of VFC that should be mostly independent from the applying country. Since the technologies underlying VFC are still immature and thus not yet widely deployed, finding practitioners and experts has been difficult. On the aspect of countermeasures we only briefly stated some possible security measures to mitigate identified threats but left it for future research to make a drill down and extensively analyse their usage and implications

TABLE 13. This study's major contributions to research.

Previous research gaps	This study's findings	Implications for research
Knowledge on VFC threats is still scarce and scattered across different research articles and disciplines	Threat model containing 33 threats and an initial discussion on security mitigation strategies	With this study, we synthesize and harmonize extant research and provide a structured threat model aligned with the STRIDE attack categories, helping to identify common security mitigation strategies that are associated with these categories.
Prior research commonly names and proposes threats briefly, but lacks empirical validation and rich descriptions	Empirical validation and richer descriptions of identified threats	With this survey paper, we extend prior research by providing richer descriptions of identified threats, thereby increasing our understanding and providing support to define requirements and boundary conditions of VFC system and security measures.
Physical attacks have been neglected in prior research	Identification of three physical attacks threatening a VFC system	We fill an important gap in extant research by raising awareness of physical attacks that underline importance of the cyber-physical manifestation of VFC.

in VFC. The VFC system architecture serving as basis for our study is a general model, omitting technical specifications and details. While we deemed this necessary to maintain the broad scope and general applicability of our threat model, it precluded the inclusion of security concepts and attacks that rely on certain architectural assumptions like specific networking protocols. We acknowledge that this may raise questions regarding generalizability of our work. Our work focuses on the identification of threats and omits a deeper investigation of technical solutions. This lack on the technical depth of providing solutions could be considered in future work. Lastly, the overview covers a number of 33 threats, this leads us to describe each threat on abstract level by leaving out technical details and concrete attacker scenarios.

D. CURRENT SITUATION IN GERMANY

We now take a brief look at the current situation of VFC in Germany, based on the information received from the expert interviews. There are already some existing prototypical field experiments and local pilot projects that are testing VFC related concepts, such as an "edge cloud" [E-9] with LTE and 5G, respectively. Besides, some providers are currently testing the fog concept with special antennas in dedicated test environments [E-6]. Unfortunately, the progression of VFC in Germany is slowed down by the multiplicity of actors (providers, OEMs, etc.) in this field and regulatory uncertainties, which complicates a joint development [E-6]. Nonetheless, the introduction of a fog layer in such a scenario provides significant improvements as it can improve communication efficiency through, for example, reduced latency and real-time response [6].

E. FUTURE RESEARCH

Our research also provides opportunities for further fruitful research. The threats identified in our work should be addressed by technical solutions in the future. Even if there are already standardised approaches for many issues, one should pay attention to the specifics in the VFC context. These include, for example, the various DoS attacks. Comparing the regulatory environment in different countries would allow the development of VFC systems as broadly applicable as possible, accelerating the deployment of the technology to the real world. A concrete example in how a regulatory environment may affect the development of technology is the example of autonomous driving: Germany's strict regulations do not allow Tesla's camera-based autopilot on its streets [77]. Consequently, German automaker Daimler relies on a safer, but more restricted system based on high-definition maps in its cars [78]. Since real word deployments of VFC hinge on the technical feasibility of the system, assessing different technical solutions and the trade-offs they provide may generate further insights into threats and security measures. An example of research in this direction may be the examination of encryption protocols with respect to speed and security in a VFC context. Lastly, the evaluation of system prototypes in dedicated test environments is a key area for future work. In Germany, this type of research is still in its infancy compared to countries like China or the USA. However, it is of critical importance on the way to a wide-spread application of VFC in the real world as it is needed to quantify and verify theoretical work.

VII. CONCLUSION

Vehicular fog computing offers huge benefits for individuals and the society, but also introduces unique security threats that should be mitigated with appropriate security measures. In this study, we synthesized prior research on VFC and interviewed security and fog computing experts to design a threat model for VFC. We assigned reviewed threats for a VFC system to the six attack categories of the STRIDE threat model, namely spoofing, tampering, repudiation, information disclosure, DoS, and elevation of privilege. We supplemented our results by conducting qualitative expert interviews, providing

us with deeper insights into identified threats and the identification of novel threats. In particular, we examined physical attacks that have been neglected by extant research so far. Beyond that, we briefly elaborated on security measures that enable to overcome the vulnerabilities of such a VFC system and associated these mitigation strategies with the components of STRIDE, particularly highlighting physical attacks.

APPENDIX. ACRONYMS

DFD	Data Flow Diagram
DoS	Denial of Service
DDoS	Distributed Denial of Service
IDS	Intrusion Detection System
MITM	Man-in-the-Middle
NIST	National Institute of Standards and Technology
PDoS	Physical Denial of Service
RSU	Roadside Unit
VANETs	Vehicular ad hoc Networks
VFC	Vehicular Fog Computing

REFERENCES

[1] K. Murata, C. Boberg, R. Kawamura, J. Obstfeld, and S. Tabet. (Feb. 2019). *Driving Data to the Edge*. [Online]. Available: https://aecc.org/wp-content/uploads/2019/03/AECC_Presentation_for_MWC_2019_Final2.pdf

[2] Y. Gao and A. Wachtel. (2017). *Connected Cars on the Road to 5G: Cross-Industry Whitepaper Series: Empowering Our Connected World*. [Online]. Available: https://www-file.huawei.com/-/media/corporate/pdf/x-lab/17-huawei-whitepaper-connected-car-on-the-road-to-5g-v2.pdf?la=en-ca

[3] M. Cäsar, R. Mehl, S. Tschödrich, M. Pauli, B. Ruther, R. Wendt, D. Blöchl, A. Stotz, M. Völkoi, S. Wei, and W. Dupont. (2019). *Connected Vehicle Trend Radar*. [Online]. Available: https://www.capgemini.com/wp-content/uploads/2019/08/Connected-Vehicle-Trend-Radar.pdf

[4] A. Benlian, W. J. Kettinger, A. Sunyaev, and T. J. Winkler, "The transformative value of cloud computing: A decoupling, platformization, and recombination theoretical framework," *J. Manage. Inf. Syst.*, vol. 35, no. 3, pp. 719–739, Jul. 2018.

[5] H. Zhou, T. Wu, X. Chen, S. He, D. Guo, and J. Wu, "Reverse auction-based computation offloading and resource allocation in mobile cloud-edge computing," *IEEE Trans. Mobile Comput.*, early access, Jul. 18, 2022, doi: 10.1109/TMC.2022.3189050.

[6] J. Li, T. Zhang, J. Jin, Y. Yang, D. Yuan, and L. Gao, "Latency estimation for fog-based Internet of Things," in *Proc. 27th Int. Telecommun. Netw. Appl. Conf. (ITNAC)*, Nov. 2017, pp. 1–6.

[7] M. Gomes and M. L. Pardal, "Cloud vs fog: Assessment of alternative deployments for a latency-sensitive IoT application," *Proc. Comput. Sci.*, vol. 130, pp. 488–495, Jun. 2018.

[8] M. Iorga, L. Feldman, R. Barton, M. J. Martin, N. Goren, and C. Mahmoudi, "Fog computing conceptual model," Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Tech. Rep. 500-325, Mar. 2018.

[9] K. Jiang, C. Sun, H. Zhou, X. Li, M. Dong, and V. C. M. Leung, "Intelligence-empowered mobile edge computing: Framework, issues, implementation, and outlook," *IEEE Netw.*, vol. 35, no. 5, pp. 74–82, Sep. 2021.

[10] C. Huang, R. Lu, and K.-K. R. Choo, "Vehicular fog computing: Architecture, use case, and security and forensic challenges," *IEEE Commun. Mag.*, vol. 55, no. 11, pp. 105–111, Nov. 2017.

[11] T. Fleck, K. Daaboul, M. Weber, P. Schörner, M. Wehmer, J. Doll, S. Orf, N. Sußmann, C. Hubschneider, M. R. Zofka, and F. Kuhnt, "Towards large scale urban traffic reference data: Smart infrastructure in the test area autonomous driving Baden-Württemberg," in *Proc. Int. Conf. Intell. Auton. Syst.* Cham, Switzerland: Springer, 2018, pp. 964–982.

[12] S. Khan, S. Parkinson, and Y. Qin, "Fog computing security: A review of current applications and security solutions," *J. Cloud Comput., Adv., Syst. Appl.*, vol. 6, no. 1, p. 19, 2017.

[13] R. K. Naha, S. Garg, D. Georgakopoulos, P. P. Jayaraman, L. Gao, Y. Xiang, and R. Ranjan, "Fog computing: Survey of trends, architectures, requirements, and research directions," *IEEE Access*, vol. 6, pp. 47980–48009, 2018.

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

[15] Z. Ning, J. Huang, and X. Wang, "Vehicular fog computing: Enabling real-time traffic management for smart cities," *IEEE Wireless Commun.*, vol. 26, no. 1, pp. 87–93, Jun. 2019.

[16] M. Wazid, P. Bagga, A. K. Das, S. Shetty, J. J. P. C. Rodrigues, and Y. H. Park, "AKM-IoV: Authenticated key management protocol in fog computing-based internet of vehicles deployment," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8804–8817, Oct. 2019.

[17] F. Qu, Z. Wu, F.-Y. Wang, and W. Cho, "A security and privacy review of VANETs," *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 6, pp. 2985–2996, Dec. 2015.

[18] M. A. Hoque and R. Hasan, "Towards an analysis of the architecture, security, and privacy issues in vehicular fog computing," in *Proc. SoutheastCon*, Apr. 2019, pp. 1–8.

[19] M. Howard and D. Le Blanc, *Writing Secure Code: Practical strategies and Proven Techniques for Building Secure Applications in a Networked World*, 2nd ed. Redmond, WA, USA: Microsoft Press, 2003.

[20] R. Khan, K. McLaughlin, D. Laverty, and S. Sezer, "STRIDE-based threat modeling for cyber-physical systems," in *Proc. IEEE PES Innov. Smart Grid Technol. Conf. Eur. (ISGT-Eur.)*, Sep. 2017, pp. 1–6.

[21] I. Stojmenovic and S. Wen, "The fog computing paradigm: Scenarios and security issues," in *Proc. Federated Conf. Comput. Sci. Inf. Syst. (ACSIS)*, vol. 2, M. Ganzha, L. A. Maciaszek, and M. Paprzycki, Eds., Sep. 2014, pp. 1–8.

[22] E. M. Tordera, X. Masip-Bruin, J. Garcia-Alminana, A. Jukan, G.-J. Ren, J. Zhu, and J. Farre, "What is a fog node a tutorial on current concepts towards a common definition," 2016, *arXiv:1611.09193*.

[23] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, "Fog computing and its role in the Internet of Things," in *Proc. 1st MCC Workshop Mobile Cloud Comput. (MCC)*, New York, NY, USA, 2012, pp. 13–16, doi: 10.1145/2342509.2342513.

[24] Z. Mahmood, Ed., *Fog computing: Concepts, Frameworks and Technologies*. Cham, Switzerland: Springer, 2018.

[25] K. Kai, W. Cong, and L. Tao, "Fog computing for vehicular ad-hoc networks: Paradigms, scenarios, and issues," *J. China Universities Posts Telecommun.*, vol. 23, no. 2, pp. 56–96, Apr. 2016.

[26] P. Mell and T. Grance, *The NIST Definition of Cloud Computing*. Gaithersburg, MD, USA: NIST, 2011.

[27] A. Sunyaev, *Internet Computing—Principles of Distributed Systems and Emerging Internet-Based Technologies.*, 1st ed. Cham, Switzerland: Springer, 2020.

[28] W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu, "Edge computing: Vision and challenges," *IEEE Internet Things J.*, vol. 3, pp. 637–646, 2016.

[29] X. Wang, Z. Ning, and L. Wang, "Offloading in internet of vehicles: A fog-enabled real-time traffic management system," *IEEE Trans. Ind. Informat.*, vol. 14, no. 10, pp. 4568–4578, Oct. 2018.

[30] Y. Xiao and C. Zhu, "Vehicular fog computing: Vision and challenges," in *Proc. IEEE Int. Conf. Pervasive Comput. Commun. Workshops (PerCom Workshops)*, Mar. 2017, pp. 6–9.

[31] I. Benbasat and R. W. Zmud, "The identity crisis within the is discipline: Defining and communicating the discipline's core properties," *MIS Quart.*, vol. 27, no. 2, pp. 183–194, Jun. 2003.

[32] J. Ni, A. Zhang, X. Lin, and X. S. Shen, "Security, privacy, and fairness in fog-based vehicular crowdsensing," *IEEE Commun. Mag.*, vol. 55, no. 6, pp. 146–152, Jun. 2017.

[33] H. Hartenstein and L. P. Laberteaux, "A tutorial survey on vehicular ad hoc networks," *IEEE Commun. Mag.*, vol. 46, no. 6, pp. 164–171, Jun. 2008.

[34] R. K. Naha and S. Garg, "Multi-criteria-based dynamic user behaviour-aware resource allocation in fog computing," *ACM Trans. Internet Things*, vol. 2, no. 1, pp. 1–31, Feb. 2021, doi: 10.1145/3423332.

[35] L. Gao, T. H. Luan, B. Liu, W. Zhou, and S. Yu, "Fog computing and its applications in 5G," in *5G Mobile Communications*. Cham, Switzerland: Springer, 2017, pp. 571–593.

[36] J. Youn, "Vehicular fog computing based traffic information delivery system to support connected self-driving vehicles in intersection environment," in *Advances in Computer Science and Ubiquitous Computing*. Cham, Switzerland: Springer, 2018, pp. 208–213.

[37] M. A. Hoque and R. Hasan, "Towards a threat model for vehicular fog computing," in *Proc. IEEE 10th Annu. Ubiquitous Comput., Electron. Mobile Commun. Conf. (UEMCON)*, Oct. 2019, pp. 1051–1057.

[38] R. Hasan, S. Myagmar, A. J. Lee, and W. Yurcik, "Toward a threat model for storage systems," in *Proc. ACM workshop Storage Secur. Survivability (StorageSS)*, New York, NY, USA, 2005, pp. 94–102, doi: 10.1145/1103780.1103795.

[39] N. Shevchenko, T. A. Chick, P. O'Riordan, T. P. Scanlon, and C. Woody, "Threat modeling: A summary of available methods," Carnegie Mellon Univ., Softw. Eng. Inst., Pittsburgh, PA, USA, Tech. Rep., 2018.

[40] M. Howard and S. Lipner, *The Security Development Lifecycle: SDL: A Process for Developing Demonstrably More Secure Software*. Redmond, WA, USA: Microsoft Press, 2006.

[41] M. C. Lacity, S. Khan, A. Yan, and L. P. Willcocks, "A review of the IT outsourcing empirical literature and future research directions," *J. Inf. Technol.*, vol. 25, no. 4, pp. 395–433, Dec. 2010.

[42] M. L. G. Shaw and B. R. Gaines, "Comparing conceptual structures: Consensus, conflict, correspondence and contrast," *Knowl. Acquisition*, vol. 1, no. 4, pp. 341–363, Dec. 1989. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S104281438980010X

[43] L. A. Palinkas, S. M. Horwitz, C. A. Green, J. P. Wisdom, N. Duan, and K. Hoagwood, "Purposeful sampling for qualitative data collection and analysis in mixed method implementation research," *Administration Policy Mental Health Mental Health Services Res.*, vol. 42, no. 5, pp. 533–544, Sep. 2015, doi: 10.1007/s10488-013-0528-y.

[44] J. Corbin and A. Strauss, *Basics of Qualitative Research*, 4th ed. Newbury Park, CA, USA: Sage, 2015.

[45] S. Jones and J. Hughes, "Understanding IS evaluation as a complex social process: A case study of a U.K. Local authority," *Eur. J. Inf. Syst.*, vol. 10, no. 4, pp. 189–203, Dec. 2001, doi: 10.1057/palgrave.ejis.3000405.

[46] O. Volkoff, D. M. Strong, and M. B. Elmes, "Understanding enterprise systems-enabled integration," *Eur. J. Inf. Syst.*, vol. 14, no. 2, pp. 110–120, Jun. 2005, doi: 10.1057/palgrave.ejis.3000528.

[47] C. Abraham, M.-C. Boudreau, I. Junglas, and R. Watson, "Enriching our theoretical repertoire: The role of evolutionary psychology in technology acceptance," *Eur. J. Inf. Syst.*, vol. 22, no. 1, pp. 56–75, Jan. 2013, doi: 10.1057/ejis.2011.25.

[48] C. Urquhart, H. Lehmann, and M. D. Myers, "Putting the 'theory' back into grounded theory: Guidelines for grounded theory studies in information systems," *Inf. Syst. J.*, vol. 20, no. 4, pp. 357–381, May 2009.

[49] A. T. Sheik and C. Maple, "Edge computing to support message prioritisation in connected vehicular systems," in *Proc. IEEE Global Conf. Internet Things (GCIoT)*, Dec. 2019, pp. 1–7.

[50] R. Roman et al., "Mobile edge computing, fog: A survey and analysis of security threats and challenges," *Future Gener. Comput. Syst.*, vol. 78, pp. 680–698, Jan. 2018.

[51] M. Li, L. Zhu, and X. Lin, "Privacy-preserving traffic monitoring with false report filtering via fog-assisted vehicular crowdsensing," *IEEE Trans. Services Comput.*, vol. 14, no. 6, pp. 1902–1913, Nov. 2021.

[52] B. Z. Abbasi and M. A. Shah, "Fog computing: Security issues, solutions and robust practices," in *Proc. 23rd Int. Conf. Autom. Comput. (ICAC)*, Sep. 2017, pp. 1–6.

[53] Z. Bakhshi and A. Balador, "An overview on security and privacy challenges and their solutions in fog-based vehicular application," in *Proc. IEEE 30th Int. Symp. Pers., Indoor Mobile Radio Commun. (PIMRC Workshops)*, Sep. 2019, pp. 1–7.

[54] A. Hussein, I. H. Elhajj, A. Chehab, and A. Kayssi, "SDN VANETs in 5G: An architecture for resilient security services," in *Proc. 4th Int. Conf. Softw. Defined Syst. (SDS)*, May 2017, pp. 67–74.

[55] W. Ben Jaballah, M. Conti, and C. Lal, "Security and design requirements for software-defined VANETs," *Comput. Netw.*, vol. 169, Mar. 2020, Art. no. 107099.

[56] S. A. Soleymani, A. H. Abdullah, M. Zareei, M. H. Anisi, C. Vargas-Rosales, M. K. Khan, and S. Goudarzi, "A secure trust model based on fuzzy logic in vehicular ad hoc networks with fog computing," *IEEE Access*, vol. 5, pp. 15619–15629, 2017.

[57] Y. Lu, C. Maple, T. Sheik, H. Alhagagi, T. Watson, M. Dianati, and A. Mouzakitis, "Analysis of cyber risk and associated concentration of research (ACR)2 in the security of vehicular edge clouds," in *Proc. Living Internet Things, Cybersecurity IoT*, 2018, pp. 1–12.

[58] A. Khan, M. Ishtiaq, S. Anwar, and M. A. Shah, "A survey on secure routing strategies in VANETs," in *Proc. 25th Int. Conf. Autom. Comput. (ICAC)*, Sep. 2019, pp. 1–6.

[59] R. Meneguette, R. De Grande, J. Ueyama, G. P. R. Filho, and E. Madeira, "Vehicular edge computing: Architecture, resource management, security, and challenges," *ACM Comput. Surveys*, vol. 55, no. 1, pp. 1–46, Jan. 2023, doi: 10.1145/3485129.

[60] A. T. Sheik, C. Maple, T. Watson, H. Alhagagi, N. S. Safa, and S. Woo-Lee, "A threat based approach to computational offloading for collaborative cruise control," in *Proc. 2nd Int. Conf. Internet Things, Data Cloud Comput. (ICC)*, H. Hamdan, D. E. Boubiche, H. Toral-Cruz, S. Akleylek, and H. Mcheick, Eds., 2017, p. 175.

[61] M. Schwall, T. Daniel, T. Victor, F. Favarò, and H. Hohnhold, "Waymo public road safety performance data," Waymo, Mountain View, CA, USA, Tech. Rep., Oct. 2020.

[62] H. Noura, O. Salman, A. Chehab, and R. Couturier, "Preserving data security in distributed fog computing," *Ad Hoc Netw.*, vol. 94, Nov. 2019, Art. no. 101937. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1570870519303634

[63] Z. Yu, M. H. Au, Q. Xu, R. Yang, and J. Han, "Towards leakage-resilient fine-grained access control in fog computing," *Future Gener. Comput. Syst.*, vol. 78, pp. 763–777, Jan. 2018. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167739X17301310

[64] H. Kim, E. Kang, D. Broman, and E. A. Lee, "Resilient authentication and authorization for the Internet of Things (IoT) using edge computing," *ACM Trans. Internet Things*, vol. 1, no. 1, pp. 1–27, Feb. 2020, doi: 10.1145/3375837.

[65] A. Alrawais, A. Alhothaily, B. Mei, T. Song, and X. Cheng, "An efficient revocation scheme for vehicular ad-hoc networks," *Proc. Comput. Sci.*, vol. 129, pp. 312–318, Jun. 2018.

[66] J. Kang, R. Yu, X. Huang, M. Wu, S. Maharjan, S. Xie, and Y. Zhang, "Blockchain for secure and efficient data sharing in vehicular edge computing and networks," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4660–4670, Jun. 2019.

[67] M. Ma, D. He, H. Wang, N. Kumar, and K.-K. R. Choo, "An efficient and provably secure authenticated key agreement protocol for fog-based vehicular ad-hoc networks," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8065–8075, Oct. 2019.

[68] Y. Yao, X. Chang, J. Misic, V. B. Misic, and L. Li, "BLA: Blockchain-assisted lightweight anonymous authentication for distributed vehicular fog services," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 3775–3784, Apr. 2019.

[69] A. Alrawais, A. Alhothaily, C. Hu, and X. Cheng, "Fog computing for the Internet of Things: Security and privacy issues," *IEEE Internet Comput.*, vol. 21, no. 2, pp. 34–42, Mar. 2017.

[70] M. Mukherjee, R. Matam, L. Shu, L. Maglaras, M. A. Ferrag, N. Choudhury, and V. Kumar, "Security and privacy in fog computing: Challenges," *IEEE Access*, vol. 5, pp. 19293–19304, 2017.

[71] J. Ni, K. Zhang, X. Lin, and X. S. Shen, "Securing fog computing for Internet of Things applications: Challenges and solutions," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 1, pp. 601–628, 1st Quart., 2018.

[72] S. Yi, Z. Qin, and Q. Li, "Security and privacy issues of fog computing: A survey," in *Wireless Algorithms, Systems, and Applications*, vol. 9204, K. Xu and H. Zhu, Eds. Cham, Switzerland: Springer, 2015, pp. 685–695.

[73] A. Jolfaei and K. Kant, "Privacy and security of connected vehicles in intelligent transportation system," in *Proc. 49th Annu. IEEE/IFIP Int. Conf. Dependable Syst. Netw.-Supplemental Volume (DSN-S)*, Jun. 2019, pp. 9–10.

[74] J. Jin and P. Rafferty, "Does congestion negatively affect income growth and employment growth? Empirical evidence from U.S. Metropolitan regions," *Transp. Policy*, vol. 55, pp. 1–8, Apr. 2017. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0967070X16302475

[75] F. Petit, D. Verner, D. Brannegan, W. Buehring, D. Dickinson, K. Guziel, R. Haffenden, J. Phillips, and J. Peerenboom, "Analysis of critical infrastructure dependencies and interdependencies," Argonne Nat. Lab., Argonne, IL, USA, Tech. Rep. ANL/GSS-15/4, 2015.

[76] T. Dehling, S. Lins, and A. Sunyaev, "Security of critical information infrastructures," in *Information Technology for Peace and Security*. Cham, Switzerland: Springer, 2019, pp. 319–339.

[77] J. Ewing. (Jul. 2020). *German Court Says Tesla Self-Driving Claims Are Misleading*. [Online]. Available: https://www.nytimes.com/2020/07/14/business/tesla-autopilot-germany.html

[78] D. AG. (2021). *Introducing Drive Pilot: An Automated Driving System for the Highway*. [Online]. Available: https://www.daimler.com/documents/innovation/other/2019-02-20-vssa-mercedes-benz-drive-pilot-a.pdf

[79] Y. Yao, X. Chang, J. Misic, and V. Mišić, "Reliable and secure vehicular fog service provision," *IEEE Internet Things J.*, vol. 6, no. 1, pp. 734–743, Feb. 2019.

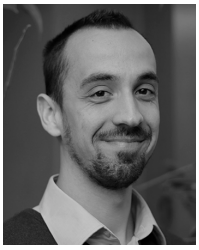
TIMO KLEIN received the bachelor's degree in economics from the University of Mannheim, Mannheim, Germany. He is currently pursuing the master's degree in economics engineering with the Karlsruhe Institute of Technology (KIT). His studies at KIT are focused on computer science and practical applications of machine learning algorithms. He is writing his master's thesis at the Institute of Applied Informatics and Formal Description Methods, KIT. His research interests include application of machine learning to autonomous and networked driving systems with a particular focus on reinforcement learning.

TANJA FENN received the bachelor's degree in information systems from the University of Passau. She is currently pursuing the master's degree in information systems with the Karlsruhe Institute of Technology (KIT). In her master's thesis at the Institute for Program Structures and Data Organization (IPD) she focuses on change detection in high-dimensional data streams. Her main research interests include security and privacy friendly system architectures and applied machine learning techniques.

ANETT KATZENBACH received the bachelor's degree in commerce and marketing from the Budapest Business School and Business Administration, Kempten University of Applied Sciences. She is currently pursuing the master's degree in business information systems with the Karlsruhe Institute of Technology (KIT). She is writing her master's thesis at the Institute of Applied Informatics and Formal Description Methods, KIT. Her research interests include semantic web technologies and their practical applications and vehicular fog computing. Her research appeared in the ESWC 2021 Scientific Conference.

HEINER TEIGELER received the degree in information systems from the University of Cologne. He is currently pursuing the Ph.D. degree with the Institute of Applied Informatics and Formal Description Methods, Karlsruhe Institute of Technology (KIT), Germany.

He is also a Research Associate at the research group Critical Information Infrastructures (CII). His research interests include trustworthy internet technologies and IT certifications. His research appeared in international journals, such as the *Business & Information Systems Engineering*, and leading scientific conferences, including the European Conference on Information Systems and the Hawaii International Conference on System Sciences.



SEBASTIAN LINS received the Ph.D. degree in information systems from the University of Cologne, Germany.

He is currently a Postdoctoral Researcher with the research group Critical Information Infrastructures (CII), Institute of Applied Informatics and Formal Description Methods, Karlsruhe Institute of Technology (KIT), Germany. His work has been published in international journals, such as the IEEE TRANSACTIONS ON CLOUD COMPUTING, the *ACM SIGMIS Database*, the *Decision Sciences*, the *Electronic Commerce Research*, and the *Communications of the Association for Information Systems*, and conference proceedings, such as International Conference on Information Systems and the European Conference on Information Systems. His main research interests include trustworthy internet technologies as well as understanding and enhancing the effectiveness of IS certifications.

ALI SUNYAEV is currently a Professor with the Karlsruhe Institute of Technology, Germany. His research interests include reliable and purposeful information systems within the scope of critical infrastructures, cloud computing services, information security solutions, trustworthy AI, auditing/certification of IT, and innovative health IT applications. His research work accounts for the multifaceted use contexts of digital technologies with research on human behavior affecting IT and vice versa. His research appeared in journals, including the *Journal of Management Information Systems*, the *Journal of Information Technology*, the IEEE TRANSACTIONS ON CLOUD COMPUTING, the IEEE TRANSACTIONS ON SOFTWARE ENGINEERING, and the *ACM Computing Surveys*. His research work has been featured in a variety of media outlets.