A Forensic Approach to Handle Autonomous Transportation Incidents within Gaia-X

Liron Ahmeti*, Klara Dolos*, Conrad Meyer*, Andreas Attenberger*, Rudolf Hackenberg†
*Research Unit, Central Office for Information Technology in the Security Sector
Munich, Germany
Email: poststelle@zitis.bund.de
†Dept. Informatics and Mathematics, OTH Regensburg
Regensburg, Germany
Email: rudolf.hackenberg@oth-regensburg.de

***Abstract*—The German Federal Office for Information Security (BSI) provides a guideline for IT forensics that describes the basic procedure for IT forensic investigations. With the development of autonomous vehicles and new innovative ecosystems such as Gaia-X, new mobility options will emerge, leading to new scenarios that require forensic investigation. Therefore, a forensic approach must be investigated to improve and create a comprehensive and adaptable guide for Gaia-X and autonomous mobility. A thorough analysis of the operational environment and threats is necessary. This approach examines two future forensic scenarios based on BSI guidelines and suggests a cloud-related preliminary measure.**

Keywords-Gaia-X; autonomous driving; digital forensic; cloud

I. Introduction

Autonomous driving is becoming increasingly essential and represents the future of mobility [1]. This technological revolution requires enormous data to ensure safety, efficiency and comfort [2]. This data could come from the Gaia-X ecosystem, an initiative to create a robust, secure and trustworthy data infrastructure for Europe [3]. Such data infrastructure builds the basis for developing novel mobility applications [4]. With the introduction of new autonomous functionalities of vehicles and the innovative operating environment, it is essential to maintain forensic analysis and security. Digital forensics is crucial to ensure that a quick and effective response is possible after security incidents or technical problems. Integrating advanced forensic methods into the autonomous vehicle ecosystem will play a crucial role in ensuring the resilience and reliability of these new technologies.

We have identified two possible forensic scenarios in the field of autonomous mobility that may arise with the introduction of autonomous driving technology. The first malicious scenario is manipulating the vehicle's control unit, which is responsible for activating autonomous driving. This manipulation also aims to enable autonomous driving when it is not allowed. The second scenario is a Distributed Denial-of-Service (DDoS) attack, interrupting vehicle and technical supervisor communication. Vehicles are then not allowed to drive autonomously, and a person needs to take control of the vehicle to enter a safe state. This can cause severe traffic jams[5]. We aim to evaluate these scenarios using current methods and analyze how a federated data infrastructure like Gaia-X can assist in the forensic investigation. Once we have defined the required investigations for two scenarios, we suggest a general procedure based on the guidelines provided by the German Federal Office for Information Security (BSI). It is crucial to acknowledge that process models are not rigid constructs but adaptive frameworks that can be adjusted to meet changing requirements. The rest of this paper is organised as follows. Section II describes the necessary background knowledge of the work. Section III explains digital forensics methods. Section IV performs a threat analysis for autonomous vehicles. Section V discusses malicious scenarios, their impact on autonomous systems and describes their forensic investigation. Section VI extends the forensic process and adapts the new possibilities provided by Gaia-X. Section VII summarises the results, discusses the applicability of the BSI guidelines, and provides an outlook on future research.

II. Background

A. Gaia-X

Gaia-X is an initiative to build a federated and secure data infrastructure to promote data sovereignty and interoperability. It is a collaborative effort to create a transparent and open ecosystem where data and services can be shared safely while respecting all stakeholders' autonomy and data sovereignty. This is achieved by developing data spaces, which are digital representations of different sectors, like healthcare, agriculture or mobility sectors, allowing multiple actors to exchange data with each other [6]. The architecture is built on three fundamental principles: federation, decentralisation and openness [7]. The federated approach allows different entities to interact within the ecosystem while retaining their autonomy. Decentralisation ensures operations without central control, promoting scalability and flexibility. The open architecture makes all aspects of Gaia-X visible and accessible. An essential aspect of Gaia-X is its Federation Services, which provide the basic framework for interaction within the ecosystem. These services include identity and trust management to ensure secure and authenticated participant engagement. An essential Federated Service is the Federated Catalogue. The Federated Catalogue is designed to help consumers find the most suitable data provider or services and keep track of relevant changes to those offers [7]. Providers register self-descriptions with universally resolvable identifiers to make them public in a Catalogue. The Catalogue then creates an internal representation of a knowledge graph using the linked data of the

 ISBN: 978-1-68558-156-5

self-descriptions that have been registered and are accessible [7]. This enables interfaces that enable users to query, search and filter service offerings. The Trust Framework is central to Gaia-X and embeds security and compliance to ensure all participants can operate in a secure digital environment [7]. Within the trust framework, a trust anchor acts as an authority that issues digital identities and is a central point of trust. It verifies that people are who they claim to be [8]. Participants who possess identities are natural persons, legal entities, and devices [3]. Identities are implemented through the Self-Sovereign Identity (SSI) concept. This feature empowers users to manage their digital identities and credentials autonomously without depending on centralised services [3]. The individual SSI wallet securely stores identity data, enabling direct and secure exchange without intermediaries.

B. Autonomous Driving

The SAE standard J3016 classifies autonomous vehicles according to their level of automation in road traffic [9]. The spectrum ranges from Level 0, which has no automation, to Level 5, which has full automation. Level 4, called high automation, does not require human intervention but only works under certain conditions. In Germany, a special law regulating Level 4 self-driving vehicles [5] [10]. This law defines specific operating areas and describes the conditions to be met to allow for autonomous control of vehicles. Based on this law, Mercedes-Benz has been approved for Level 4 autonomous parking, called the Intelligent Park Pilot, for seven of its models. This enables vehicles to drive autonomously only in multi-storey car parks [11].

C. Operational Domain Design

Autonomous driving systems are designed to operate under specific conditions. Operational Design Domain (ODD) models these specific conditions, including environmental, geographic and time-of-day constraints, and necessary traffic or roadway features [12]. The standard from BSI PAS1883 provides a detailed taxonomy for defining ODDs, aiming to secure implementation and communication between stakeholders such as manufacturers, regulators and service providers [12].

D. Technical supervisor

The technical supervisor for autonomous driving functions is defined in detail for the German law for highly automated driving [5]. The supervisor is a person who monitors the vehicle remotely, not continuously but based on specific events. This person is responsible for assessing and approving driving manoeuvres in critical situations, communicating with occupants and other road users during emergencies and utilizing technical systems to monitor and control the vehicle. As a part of the technical supervision of autonomous vehicles, specific data must be stored and monitored to ensure that the vehicle complies with technical and organizational requirements. This data includes the unique vehicle identification number, position data to track the geographic location, especially during critical events, the number of times the autonomous driving function is activated and deactivated and the time of use. Additionally, data on the times when alternative driving manoeuvres are enabled, and system monitoring data such as software status, environmental and weather conditions, networking parameters, the status of the safety systems, and vehicle acceleration in longitudinal and lateral directions must be recorded. This data is essential for monitoring and evaluating the vehicle's performance, operational safety and system reliability.

III. Digital Forensics

The "IT Forensics Guide" [13] offers a comprehensive framework for conducting IT forensic investigations. It outlines the step-by-step procedures for collecting and analysing digital evidence to resolve incidents. The guide covers strategic planning, operational measures, data collection, investigation, analysis and documentation. It is designed to be a practical model that can be used without specific software. The guide emphasises the importance of strategic preparation and data protection and is an essential reference for various forensic scenarios [13]. Closely related to challenges in the forensics of autonomous mobility, Schlepphorst et al. provide a detailed overview of methods that can be used for, e.g. Infrastructure as a Service, Platform as a Service and Software as a Service. The study defines evaluation criteria and compares digital forensics approaches, highlighting existing gaps and future requirements. It discusses the challenges of cloud forensics, such as collecting and analysing evidence across different cloud service models and suggests future research directions [14]. Du et al. provide an in-depth analysis of digital forensic process models. In their study, they discuss the evolution and categorisation of these models and the shift towards cloud-based evidence processing, which is referred to as Digital Forensics as a Service. The study overviews traditional and modern forensic models and highlights the benefits and challenges of integrating cloud forensics into practice [15]. Perumal et al. proposed a digital forensic investigation model for the Internet of Things (IoT) environment. The model was developed to address the challenges of digital forensics in IoT, such as the high number of interconnected devices and the complexity of the data they generate. The proposed model aims to simplify the forensic process from identification to evidence preservation and ensure effective handling of volatile data within IoT environments [16].

IV. Threat Analysis

Baig et al. [17] categorize the threats to autonomous driving into five groups: physical threats, interception threats, abuse threats, malicious code and data threats. Physical threats refer to direct physical interventions or attacks on the vehicle or its components. Interception threats are attacks against internally transmitted data between ECUs, vehicles and the cloud, such as man-in-the-middle attacks. Abuse threats can include traditional attacks, such as Denial of Service. Malicious code can be executed in integrated infotainment systems. Data threats concern the information stored in the intelligent vehicle

 ISBN: 978-1-68558-156-5

network, including information loss from a connected cloud and privacy infringement when reselling the vehicle.

In our case, we want to examine scenarios in the category of physical threats and threats of abuse. There are ways to manipulate your vehicle for financial gain, such as manipulating the odometer [18]. As vehicles become more advanced and connected to the outside world, exposing them to DDoS attacks may become profitable. In Germany, autonomous vehicles at Level 4 must continuously connect to a technical supervisor to drive autonomously [5]. If this requirement is not met, the vehicle cannot drive autonomously, and the in-vehicle person must take control of the vehicle. In Level 5 autonomous vehicles, where there is no steering wheel, the control cannot be handed over to the in-vehicle person, resulting in an emergency stop and the vehicle's malfunction.

V. Malicious scenarios

We handle forensic processing by identifying two scenarios that have resulted from previous threat analysis [17]. These guidelines serve as our framework for conducting a proper and thorough investigation. Our goal is to identify recurring patterns and issues through a comprehensive analysis. Based on the knowledge and experiences gained in such analyses, a general procedure for forensics can be developed.

For the first malicious scenario, we manipulate a control unit in the vehicle. We assume that sensor values are ignored during assessing the operating environment. Ignoring sensor values indicating, e.g., heavy rain or dense traffic, enables autonomous driving in situations where it is actually not permitted according to the authorisation.

In the second scenario, we investigate an incident where a vehicle has fallen victim to a DDoS attack. A DDoS attack occurs when several devices flood the target device with many requests, making it unavailable. DDoS attacks are often carried out by botnets consisting of many infected devices that simultaneously send requests to the victim. For instance, in 2022, Google successfully defended itself against a DDoS attack with 398 million requests per second [19]. Cloudflare was attacked by the Mantis botnet, which consisted of 5,000 bots and generated 26 million requests per second [20]. This flood of requests to vehicles could lead to a breakdown in communication, which is problematic for autonomous driving as the German Level 4 law requires uninterrupted communication with the technical supervisor [5].

A. Investigation Process

Our investigation follows the IT Forensics Guidelines established by the BSI [13], as illustrated in Figure 1. An incident investigation can be divided into two phases. The first phase is strategic preparation, which occurs before an incident occurs. During this preparation, measures are taken to facilitate a subsequent forensic investigation. This includes setting up logging mechanisms and defining a list of suitable tools. If an incident is identified, the second phase of the investigation begins with operational preparation. This involves identifying affected systems and data sources. During the data collection phase, suitable tools are chosen from the predefined list to secure the data from the identified sources. The collected data is analysed in the investigation phase to extract relevant information. This includes converting the data into usable formats for thorough analysis and identifying patterns or anomalies that indicate security incidents. In the analysis phase, data from different sources is correlated to establish associations, and additional data sources that require further analysis are identified. The measures taken must be meticulously documented in all these phases to ensure traceable results. This documentation is finalised in the documentation phase, and a results log is created from the preliminary documentation.

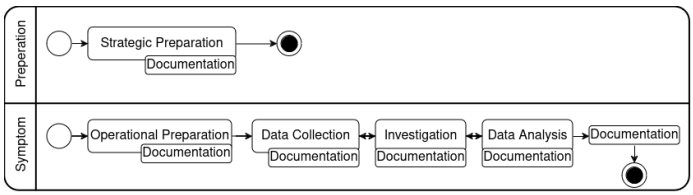

Figure 1: Forensic investigation procedure according to BSI guidelines

B. Sensor Manipulation

A vehicle owner, whose vehicle is designed to only operate autonomously in certain weather conditions, tampered with the vehicle's internal control units to misinterpret the sensors and enable autonomous driving in unsuitable weather conditions. As a result, an incident occurs. Figure 2 shows the sequence of events in this scenario.

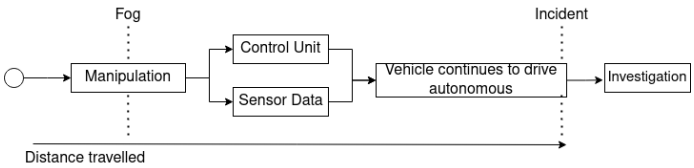

Figure 2: The procedure of the scenario: Sensor Manipulation

1) Strategic Preparation: In strategic preparation, some guidelines have been issued to oblige manufacturers to collect specific vehicle data and make it available for investigation. EU Regulation 2019/2144 sets guidelines for a standardised approach to in-vehicle data recording [21]. The concept includes the event-related data recording of important, anonymised vehicle data in the event of a collision. The Event Data Recorder (EDR) records relevant data such as speed, acceleration, braking behaviour and other vehicle-related information. Data recording occurs in a closed system where the data is overwritten, and no vehicle or owner identification is possible. According to the UN Regulations for the Approval of Vehicles with Automatic Lane Keeping Systems (ALKS), specific requirements are set for the Data Storage System for Automated Driving (DSSAD) [22]. The DSSAD records essential events such as automated driving system

 ISBN: 978-1-68558-156-5

activation and deactivation, overrides, emergency manoeuvres and collisions. Specific data such as timestamps, reasons for the event and the corresponding ALKS software version are recorded. The recorded data must be available following national and regional laws. The European Union mandates that the Event Data Recorder must be accessible through the On-Board-Diagnostic II (ODB-II) port. However, there is no designated interface for the DSSADS. The manufacturers must use a standardised communication interface and provide instructions on retrieving this data. In addition to the interfaces for data acquisition systems, other protocols can also be relevant for investigations. A popular communication protocol used in modern vehicles is Unified Diagnostic Services (UDS). This protocol facilitates communication between the vehicle's control units and a diagnostic device. It can be used to retrieve data from Electronic Control Units (ECUs) [23]. To record the communication between ECUs, the ODB-II can be used [24]. In the Gaia-X ecosystem, the Federated Catalogue can be used as an additional tool to request data. The Catalogue provides the data providers that match the description in the query. In an automated query to the providers, the data exchange is initiated in Figure 3.

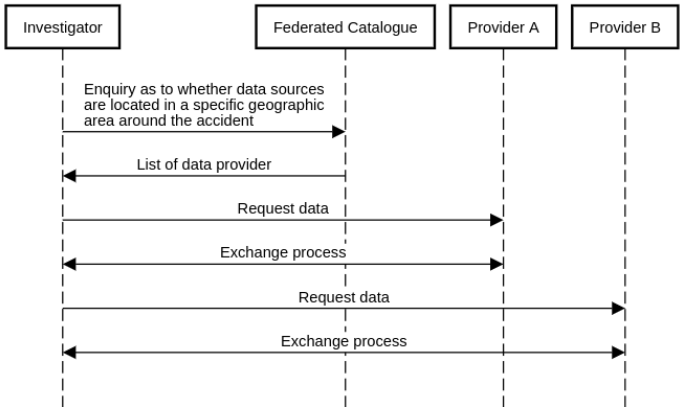

Figure 3: Architecture for the prevention of DDoS attacks

The strategic preparation leads to a list of tools that can be used for data collection in forensic investigations. The list is illustrated in Table I.

TABLE I: List of tools for extracting data from incidents involving vehicles

Category	Data	Extraction Methods
EDR	Anonymised vehicle data example: speed, braking	ODB-II
DSSAD	Events in automated Driving example: autonomous driving switched off	Manufacturer instructions
Diagnostic Data	Error Codes, ECU Software, Hashes	UDS
Communication	Messages between components	ODB-II
Data Provider	Weather, real time traffic, Roadside Unit data	Federated Catalouge

2) Forensic Investigation: Sensor manipulation can be suspected in different situations, such as standard maintenance or coincidentally. We focus on a vehicle which was involved in an accident. Initially, there is no evidence of tampering. However, the vehicle is identified as the primary relevant system during operational preparation. The vehicle control units that manage sensors for autonomous driving and the CAN communication channel are considered important sources of information. Weather data providers are also crucial as weather conditions affect autonomous driving. Additionally, technical control centres that the autonomous vehicle communicates with can provide valuable data for the investigation.

The vehicle's communication is recorded using OBD II as part of the data collection. UDS is used to secure the software and software hash of control units crucial for autonomous driving. Additionally, EDR and DSSAD data are also backed up. The Gaia-X Catalogue requests data from weather service providers and technical supervisors. Suitable Python scripts for statistical data processing and correlation recognition are selected during the data investigation phase. During the analysis of the DSSAD data, it was found that the autonomous driving function of the vehicle was activated. However, weather data for the region indicated dense fog, which should have prompted the vehicle to relinquish responsibility. The technical supervisor did not receive a request to take control of the driving manoeuvres. However, other vehicles of the same model in the area reported to the supervisor that autonomous driving was impossible due to fog. This data correlation suggests that some manipulation might have been involved. The manufacturer's original software can be compared with the downloaded software. This comparison reveals that the control unit software has been tampered with. Communication data indicates that the sensors are providing accurate values. However, control units have been overwritten to ignore these sensor values to such an extent that the autonomous functions are not being switched off.

C. DDoS Attack

In this scenario, we assume that multiple vehicles are attacked to disable them and disrupt city traffic by deliberately paralysing vehicles. According to the German regulation on the operation of motor vehicles with automated and autonomous driving functions, a central, Secure Electronic Control Unit (SECU) must be used for data transmission [25]. The SECU constitutes a single point of failure. A fully autonomous vehicle is stranded in traffic if communication with the outside world fails. Some projects, such as TransID, deal with such emergencies and want to create the necessary functionalities so autonomous vehicles can clear the way on their own [26]. In this malicious scenario, we assume that the evasion options have been exhausted.

1) Strategic Preparation: IP whitelists are used in network engineering to mitigate DDoS attacks by only processing requests from known IP addresses and ignoring requests from unknown addresses [27]. To protect against potential

 ISBN: 978-1-68558-156-5

attacks, we define measures to ensure that only compliant requests are processed within the Gaia-X ecosystem. Only requests from participants with a digital identity verified by a Gaia-X trust anchor are processed [3]. We use cloud agents to filter requests and verify their identity before forwarding them to our autonomous vehicle. In addition, all requests are logged for further analysis. The architecture of this process is illustrated in Figure 4.

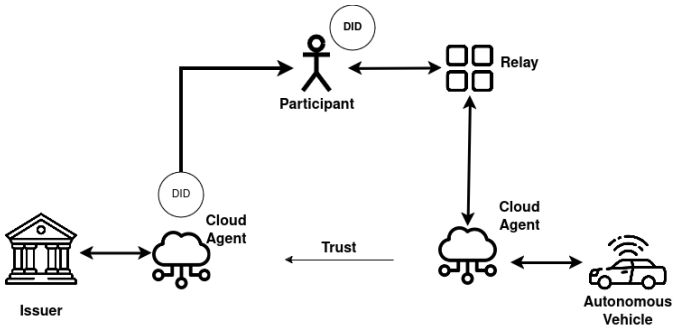

Figure 4: Architecture for the prevention of DDoS attacks

2) Forensic Investigation: The symptoms that require forensic investigation are autonomous vehicles that get into an emergency and come to a standstill due to DDoS attacks. An external attack is likely responsible if multiple vehicles within a small area experience a similar emergency. The cloud agents are identified as the relevant systems during the strategic preparation. These agents' log files are requested as part of the data collection process. In the data research phase, suitable Python scripts enable statistical data processing and correlation detection. In our scenario, we analyzed the data and found that the identities of the requests were involved in several attacks on vehicles. The traceability of digital identities makes it possible to identify offenders.

VI. Forensic Process for Gaia-X Services

After identifying potential threats and the possibility of automated data retrieval in Gaia-X, we have expanded the forensic process of BSI guidelines for incidents involving autonomous vehicles, illustrated in the Figure 5. In addition, we have established abstract procedures that are generally applicable for each step.

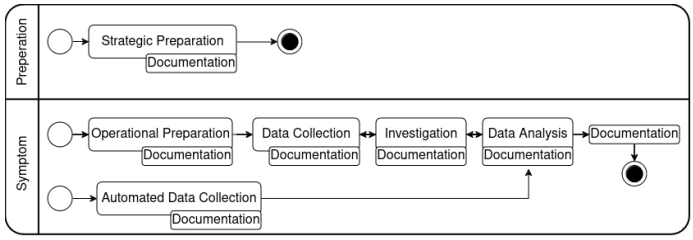

Figure 5: Architecture for the prevention of DDoS attacks

A. Strategic Preparation

A comprehensive list of standardized tools for strategic preparedness during autonomous vehicle incidents can be defined based on EU and UN guidelines [22] [21]. The federated Gaia-X services offer universal tools to support this process. The Gaia-X Catalogue can be used as a basis for data queries, eliminating the need to screen data providers beforehand. Interfaces with the data providers are also defined and can be found flexibly via the Catalogue during investigations. Moreover, software solutions can be developed to check data in real-time for anomalies and detect early symptoms. These solutions can be connected to the Catalogue to collect data automatically.

B. Operational Preparation

As part of operational preparation, tools necessary for future forensic processes are identified. We have previously determined that the Federated Catalogue can be used as a general tool for identifying and querying data sources, including the technical supervisor.

C. Data Collection

Data collection is possible through two different methods: manual and automatic. Manual data collection is extracted from sources using traditional methods after an incident, and the case is forensically investigated. Alternatively, specific approaches can be defined in strategic preparation to monitor data for symptoms continuously. These approaches directly communicate with the data sources in the Gaia-X ecosystem and can request the precise data required.

D. Investigation

Automated data collection assumes that only pertinent information is requested for the investigation. This procedure is based on predefined parameters and filters employed to collect only the specific data needed for a specific analysis or investigation. This process can eliminate the need for an investigation phase as long as there are no systems to be examined using traditional forensic methods.

E. Analysis

In many cases, additional analysis of individual test results is necessary. This phase remains unchanged from the phase outlined in the BSI guidelines. However, the volume of data is increasing, which is why we suggest developing AI methods capable of handling these large amounts of data.

F. Documentation

Accurate documentation of individual work steps is crucial in forensic investigations. With the advancement of automation in forensics, maintaining transparency and traceability of processes has become even more vital. The final report of such an investigation should contain the results and answer all the forensic questions, including what, where, when, how, who and what countermeasures were taken.

 ISBN: 978-1-68558-156-5

VII. Conclusion and Future Work

Based on the defined scenarios, we have concluded that the abstract approach of BSI is still valid. However, we have identified variations and ramifications that need to be addressed. We have presented that the core elements of Gaia-X can expedite forensic investigation and simplify offender analysis. Nonetheless, Gaia-X and the autonomous system are dynamic and flexible systems continuously evolving, making it challenging to define a standardized approach. It is crucial to acknowledge that process models are not rigid constructs but adaptive frameworks that can be adjusted to meet changing requirements. The abstract approach and the example scenarios provide guidance and a fundamental structure for the forensic approach in the mobility domain of Gaia-X to ensure effective results in forensic investigations. For future work, it is necessary to simulate the environment and establish a practical connection with Gaia-X as soon as it becomes functional. Additionally, the approach of DDOS defense via cloud agents must be implemented, and the feasibility of this method should be evaluated to determine its actual improvement.

Acknowledgements

This paper was written as part of the project GAIA-X 4 Advanced Mobility Services in the project family Future Mobility funded by the Federal Ministry of Economics and Climate Protection (BMWK).

References

[1] "Size of the global autonomous vehicle market in 2021 and 2022, with a forecast through 2030," Statista, 2023, Available from https://www.statista.com/statistics/1224515/av-market-size-worldwide-forecast/. (retrieved: 2024-03-01).

[2] "KI und Daten – Herausforderungen auf dem Weg zum autonomen Fahren," Federal Ministry for Economic Affairs and Climate Action of Germany, 2020, Available from https://www.bmwk.de/Redaktion/DE/Downloads/W/ws5-praesentation-ki-und-daten.pdf. (retrieved: 2024-03-01).

[3] B. Maier and N. Pohlmann, "Gaia-X Secure and Trustworthy Ecosystems with Self Sovereign Identity," Gaia-X European Association for Data and Cloud AISBL, White Paper, 2022.

[4] "Gaia-X 4 Future Mobility," German Aerospace Center (DLR), Available from https://www.dlr.de/en/ki/research-transfer/projects/gaia-x-4-future-mobility. (retrieved: 2024-03-01).

[5] "Gesetz zur Änderung des Straßenverkehrsgesetzes und des Pflichtversicherungsgesetzes - Autonomes Fahren," Federal Council Germany, 2024, Available from https://bmdv.bund.de/SharedDocs/DE/Anlage/Gesetze/Gesetze-19/gesetz-aenderung-strassenverkehrsgesetz-pflichtversicherungsgesetz-autonomes-fahren.pdf. (retrieved: 2024-03-01).

[6] T. Coenen and N. Walraevens and G. Terseglav and A. Lampe and I. Lakaniemi and U. Ahle and L. Raes and B. Lutz and N. Reisel and W. Van Den Bosch and G. Vervaet and M. Delannoy, "Gaia-X and European Smart Cities and Communities," Gaia-X, White Paper, Oct. 2021, Version 21.09.

[7] "Gaia-x Architecture Document - 22.04 Release," Gaia-X, Architecture Documentation, version 22.04, Apr. 2022.

[8] "Gaia-X Trust Framework - main version (fb420580)," Gaia-X, 2022, Available from https://gaia-x.gitlab.io/policy-rules-committee/trust-framework/trust%5Fanchors/. (retrieved: 2024-03-01).

[9] O.-R. A. D. (Committee, *Taxonomy and definitions for terms related to driving automation systems for on-road motor vehicles*. SAE international, 2021.

[10] A. Kriebitz, R. Max, and C. Lütge, "The german act on autonomous driving: Why ethics still matters," *Philosophy & Technology*, vol. 35, no. 2, p. 29, Apr. 2022, ISSN: 2210-5441. DOI: 10.1007/s13347-022-00526-2. [Online]. Available: https://doi.org/10.1007/s13347-022-00526-2.

[11] "Nächster Schritt beim fahrerlosen Parken," Mercedes-Benz, 2024, Available from https://group.mercedes-benz.com/innovation/produktinnovation/autonomes-fahren/naechster-step-beim-fahrerlosen-parken.html. (retrieved: 2024-03-01).

[12] "PAS 1883:2020 Operational Design Domain (ODD) taxonomy for an automated driving system (ADS) – Specification," British Standards Institution, 2020, Available from https://www.bsigroup.com/globalassets/localfiles/en-gb/cav/pas1883.pdf. (retrieved: 2024-03-01).

[13] "IT Forensics Guide," Threat Report, 2011, Available from https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Leitfaden_IT-Forensik.pdf?__blob=publicationFile&v=1. (retrieved: 2024-03-01).

[14] S. Schlepphorst, K.-K. R. Choo, and N.-A. Le-Khac, "Digital forensic approaches for cloud service models: A survey," in *Cyber and Digital Forensic Investigations: A Law Enforcement Practitioner's Perspective*. Cham: Springer International Publishing, 2020, pp. 175–199, ISBN: 978-3-030-47131-6. DOI: 10.1007/978-3-030-47131-6_8. (retrieved: 2024-03-01).

[15] X. Du, N. Le-Khac, and M. Scanlon, "Evaluation of digital forensic process models with respect to digital forensics as a service," *CoRR*, vol. abs/1708.01730, 2017. DOI: 10.48550/arXiv.1708.01730. (retrieved: 2024-03-01).

[16] S. Perumal, N. M. Norwawi, and V. Raman, "Internet of things(iot) digital forensic investigation model: Top-down forensic approach methodology," in *2015 Fifth International Conference on Digital Information Processing and Communications (ICDIPC)*, 2015, pp. 19–

 ISBN: 978-1-68558-156-5

23. DOI: 10.1109/ICDIPC.2015.7323000. (retrieved: 2024-03-01).

[17] Z. A. Baig *et al.*, "Future challenges for smart cities: Cyber-security and digital forensics," *Digital Investigation*, vol. 22, pp. 3–13, 2017, ISSN: 1742-2876. DOI: https://doi.org/10.1016/j.diin.2017.06.015. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1742287617300579.

[18] A. Heflich, "Odometer manipulation in motor vehicles in the EU," Tech. Rep., 2018, Available from https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU(2018)615637, version 1.6.0. (retrieved: 2024-03-01).

[19] "Google Cloud mitigated the largest DDoS attack peaking above 398 million RPS," Google Cloud, 2022, Available from https://cloud.google.com/blog/products/identity-security/google-cloud-mitigated-largest-ddos-attack-peaking-above-398-million-rps. (retrieved: 2024-03-01).

[20] "Cloudflare mitigates 26 million request per second DDoS attack," Cloudflare, Inc., 2022, Available from https://blog.cloudflare.com/26m-rps-ddos/. (retrieved: 2024-03-01).

[21] "Regulation (Eu) 2019/2144 Of The European Parliament And Of The Council," European Parliament and Council of the European Union, 2019, Available from https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A32019R2144. (retrieved: 2024-03-01).

[22] "UN Regulation No. 157 - Automated Lane Keeping Systems (ALKS)," United Nations, 2021, Available from https://unece.org/transport/documents/2021/03/standards/un-regulation-no-157-automated-lane-keeping-systems-alks. (retrieved: 2024-03-01).

[23] M. Shridhar Kuntoji, V. Medam, and V. Devi SV, "Design of UDS Protocol in an Automotive Electronic Control Unit," in *Recent Developments in Electronics and Communication Systems*, 2023, pp. 255–262.

[24] B. I. Kwak, J. Woo, and H. K. Kim, "Know your master: Driver profiling-based anti-theft method," in *2016 14th Annual Conference on Privacy, Security and Trust (PST)*, 2016, pp. 211–218. DOI: 10.1109/PST.2016.7906929.

[25] "Verordnung zur Regelung des Betriebs von Kraftfahrzeugen mit automatisierter und autonomer Fahrfunktion und zur Änderung straßenverkehrsrechtlicher Vorschriften," Federal Council Germany, 2022, Available from https://www.bundesrat.de/SharedDocs/drucksachen/2022/0001-0100/86-22.pdf. (retrieved: 2024-03-01).

[26] M. Lu *et al.*, "Transaid deliverable 9.5: Transaid final conference," 2020.

[27] M. Yoon, "Using whitelisting to mitigate ddos attacks on critical internet sites," *IEEE Communications Magazine*, vol. 48, no. 7, pp. 110–115, 2010, ISSN: 1558-1896. DOI: 10.1109/MCOM.2010.5496886.

 ISBN: 978-1-68558-156-5