

# Chapter 11

## Vehicular Data Analytics and Research Findings on Security, Economy and Safety



Madhusudan Singh 

**Abstract** This presentation has discussed Cyber security and safety for autonomous vehicles with the understanding of real time vehicular data. It has also given an understanding the analysis process and interpreting the vehicular data and finally conclude the course with the explanation of automotive cybersecurity research findings in economy and safety areas. This presentation has presented the vehicular data analytics and research findings on security, economy and safety. It provides cybersecurity and safety for intelligent autonomous vehicles, collection and understanding of available real-time vehicular data, understanding of analysis process and show process of data interpretation and finally it's discussed research findings to be drawing and conclude the impact of vehicular data in economy and safety.

### 11.1 Introduction: The Fundamentals of Automotive Cybersecurity

The basics of automotive cybersecurity focusing on safety and security. These are defined depending on the source of the threat. The formal definition of safety is the condition of being protected from the harm caused by non-intentional failure. It describes a situation when acquired values are harmed by accidental flaws and mistakes. It occurs when accidental flaws and mistakes occur such as technical errors, network failures, environmental disasters etc. It protects against potential or actual harm to acquired values. In the vehicular network, harm can occur at any time due to environmental causes or technical errors. Security, on the other hand, is the condition of being protected from harm caused by intentional human action or behaviors; it protects against potential or actual harm to acquired values [1].

If we take a closer look at similarities and differences between safety and security, we can see in Fig. 11.1 that, in essence, both concepts are about potential or actual

---

M. Singh (✉)

School of Technology Studies, Endicott College of International Studies, Woosong University,  
Daejeon, Republic of Korea

e-mail: [msingh@wsu.ac.kr](mailto:msingh@wsu.ac.kr)



**Fig. 11.1** Vehicle safety and security

harm to acquired values. When we look at safety and security needs regarding intelligent and autonomous vehicles, we introduce the concepts of protection and performance. Under safety [2], we examine knowledge and skills while under security we include roles and norms.

It is good to remember that safety and security are quality attributes that are part of an overall systems engineering process. This process has been standardized long before being implemented in the automotive industry thanks to ISO standards. Security ISO standards are established by first defining the security goals, then designing the functional security concepts, which is followed by designing technical security concepts, and in the last, defining software and hardware components to create a secure system.

## 11.2 Vehicle Safety and Security Relationship

The ultimate goal is to harmonize the security and safety aspects of automotive technology. Together, they form a wall which can provide security field monitoring, external interface protection and monitoring, in-vehicle update mobility and data security software updates, in-vehicle network protection and monitoring, and in-vehicle state of health monitoring. It's shown in Fig. 11.1.

### 11.2.1 Automotive Safety Begins with Security and Reliability

Without security and reliability, there is no automotive security. We will concentrate on device dependability, functional security, and on-time working safety. Device

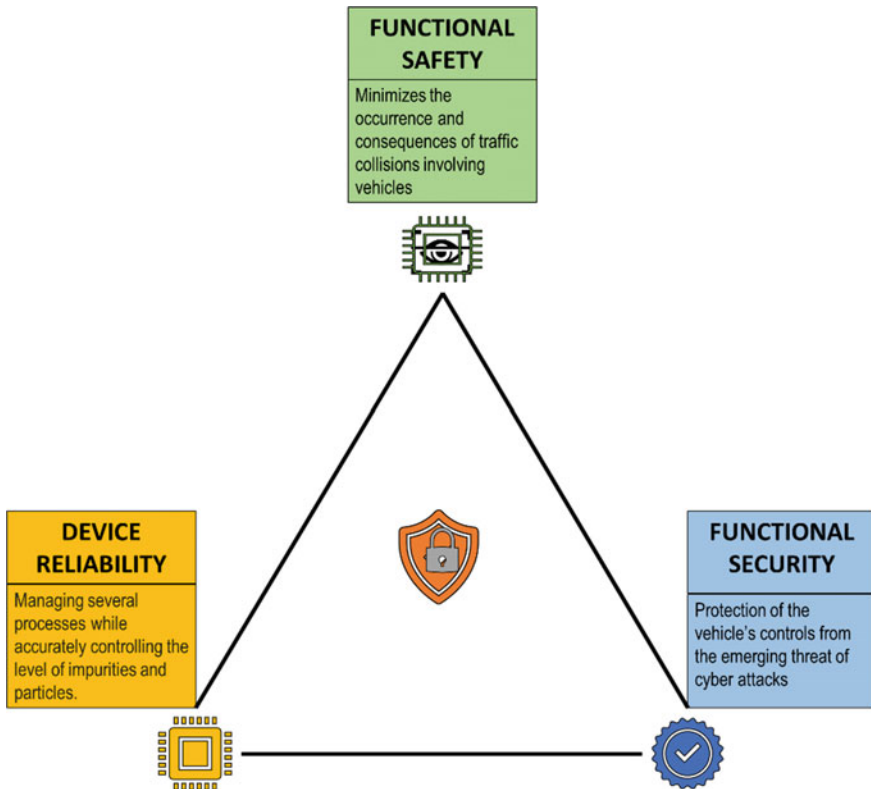


Fig. 11.2 Relationship between automotive safety, security, and reliability

dependability is important to deal with a few procedures while precisely controlling the degree of impurities and particles from entering the hardware before it can cause inside harm. It represents in Fig. 11.2. This is generally ensured by using ISO-compliant products. Functional Security is the protection of the vehicle’s controls from the emerging threat of cyber-attacks; these threats are highly dangerous in the automated driving scenario [3] where the driver has little to no control over the vehicle. Functional Safety is provided by the automotive manufacturer to minimize the occurrence and consequences of traffic collisions involving vehicles.

### 11.2.2 In-Vehicle Security Threats

In-vehicle security threats are a big component of the cyber security puzzle. These threats deal with the possible channels inside a vehicle that can be targeted for the purpose of compromising the security of the entire vehicle. There are primarily three potential methods to breach vehicular security: telematics hacking, smart phone

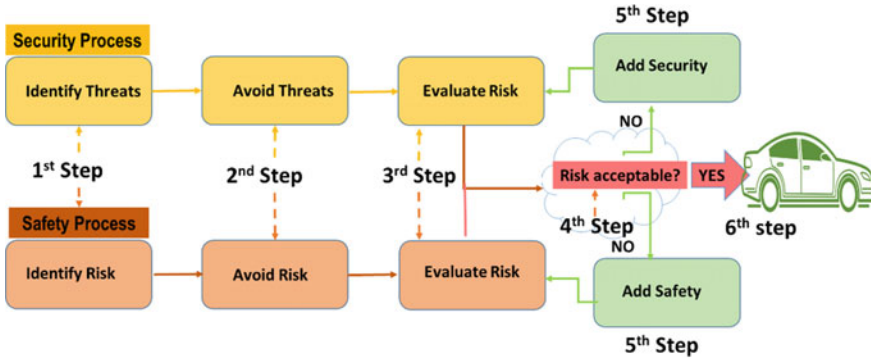


Fig. 11.3 Automotive security versus safety process

hacking, and stealing and hacking into the vehicle’s OBD port. In the diagram, we see that the way to break into a vehicle through telematics hacking is to link into the external NIC which can ultimately provide a passage to the Control Unit via the Gateway [4]. By hacking into the smartphone of the driver, the hackers can gain control of the internet-connected components such as ADAS, TMS, etc. which can provide a channel to the Control Unit through the Gateway by stealing the vehicle, or more specifically the OBD port, installed in the vehicle, the hacker that can reveal invaluable information about the driver and the vehicle itself.

### 11.2.3 Outside Vehicle Security Threats

Figure 11.3 has shown the potential in vehicle security threats, this section as discussed, the threats on the exist outside of the vehicle. All the electronic systems that are part of the vehicular environment, these are: the traffic management system, the roadside equipment (such as traffic lights), the nearby environment, software delivery/updates, the service cloud and the user’s mobile device. All six of these parts of the vehicular environment can threaten the security of the vehicle. The threats can affect all features of the system from traffic efficiency and safety, to fees and charges, vehicle interaction, and even the on-board infotainment system [5].

### 11.2.4 Automotive Security vs. Safety Process

The security and safety validation cycle components one by one starting from step one of the security process. The first step is to identify the threats to the vehicle. In the second step we try to avoid security threats. In the third step, we evaluate risk. Once the risk is evaluated, we determine whether the risk is under an acceptable limit

or not. If it is not, then we deploy more security and safety features in the vehicular system [6]. We proceed only when we determine that the risk is acceptable. The safety process is very similar to the security process as we can see in Fig. 11.3. Since automotive security is ever evolving, so should the safety process that guards it. To achieve this, there is a very stratified process.

### 11.3 Vehicular Cloud Management System

The typical connected vehicle system consists of several technologies such as internet, cellular network, radio technology, Bluetooth and many more. These technologies serve as the communication channel for data transmission in the cloud system. That is where the data collected from the vehicle goes for processing and analysis. In this graphic, we can see an overview of the vehicular cloud management system which is incorporating everything from audio-video services to IT systems [7]. This cloud system serves as the all-inclusive hub for all the management and processing activities conducted on the network.

The all-inclusive possible protection from the cyber-attacks, integrate consumer devices, provide car-to-car and car-to-infrastructure communication through a secure channel [8]. It also has an on-board safety mechanism to keep the vehicle safe from the inside. This possible only by achieving what is called harmony among safety and security. It is depends greatly upon the level of trust between security and safety.

### 11.4 Vehicle Mobility Data Processing Methods

With regards to vehicle mobility information handling, things get precarious. There is an absence of uniform tasks and a standard portrayal of the vehicle's sensor collected data. Right up 'til the present time, there is no cloud classification for vehicle asset reallocation and asset sharing of data because of absence of interoperability. In Fig. 11.4 above we depict this problem trying to show that we have heterogeneous data, a high number of machines in the vehicle and data complexity. This is the reality but what do most people think about when autonomous vehicles are mentioned?

In below graph shows how perceptions regarding autonomous vehicles are changing. Here we can see that the public's perception has changed positively in seven major industrial countries of the world. All this within only one year. Based on this big leap forward shows that with people's trust increasing that would mean higher market expectations for autonomous vehicles in the near future as presents in Fig. 11.5.

The vehicle mobility data market size is growing and in later years we have seen continued acceleration of investments in all relevant technologies [9]. Currently, the shared mobility and the data market is worth \$30 billion. By 2030, it is expected

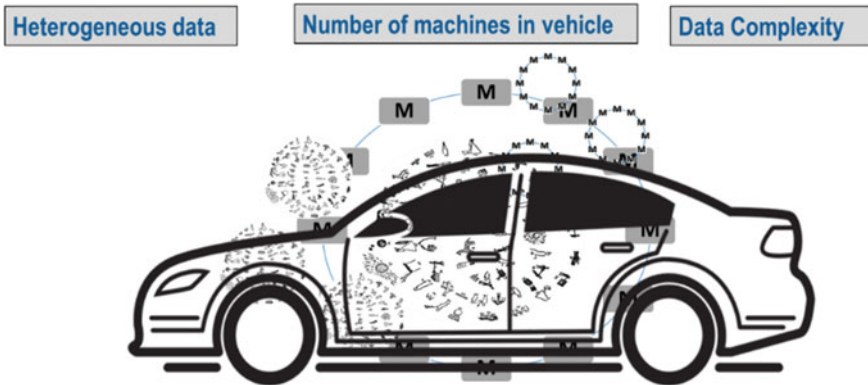


Fig. 11.4 Vehicle mobility data processing

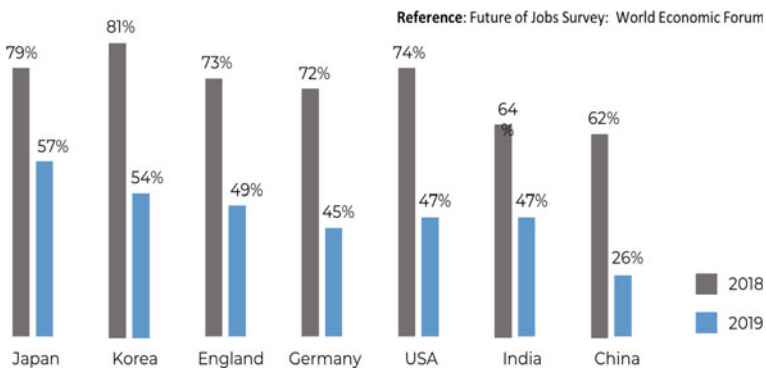


Fig. 11.5 Graph of perceptions regarding autonomous vehicles are changing

to grow over to over \$2 trillion according to the McKinsey & Company’s analysis report.

### 11.4.1 Overall Volume of Connected Car Data Transfer

While talking about the general volume of connected vehicle information transfer, we are anticipating gigantic development. This development will happen because there will be a tremendous increment in the volume of information move per-vehicle and it is evaluated that the absolute number of connected vehicles on the planet will increment at a fast rate with time represents in Fig. 11.6.

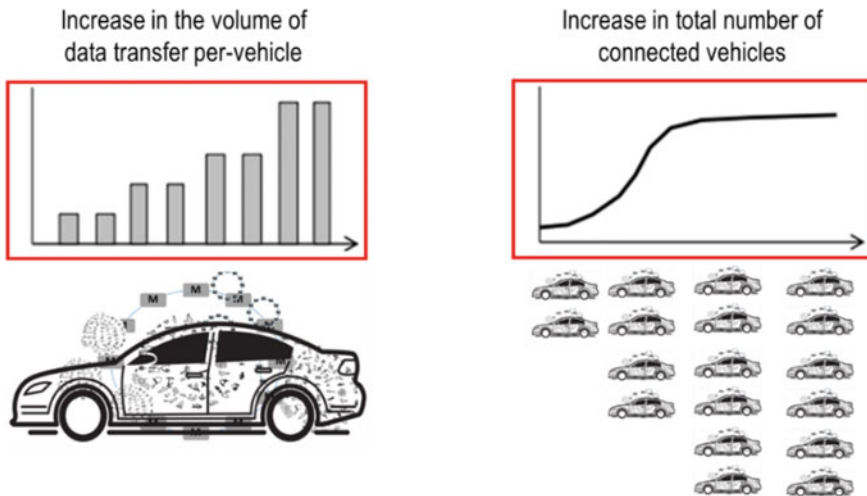
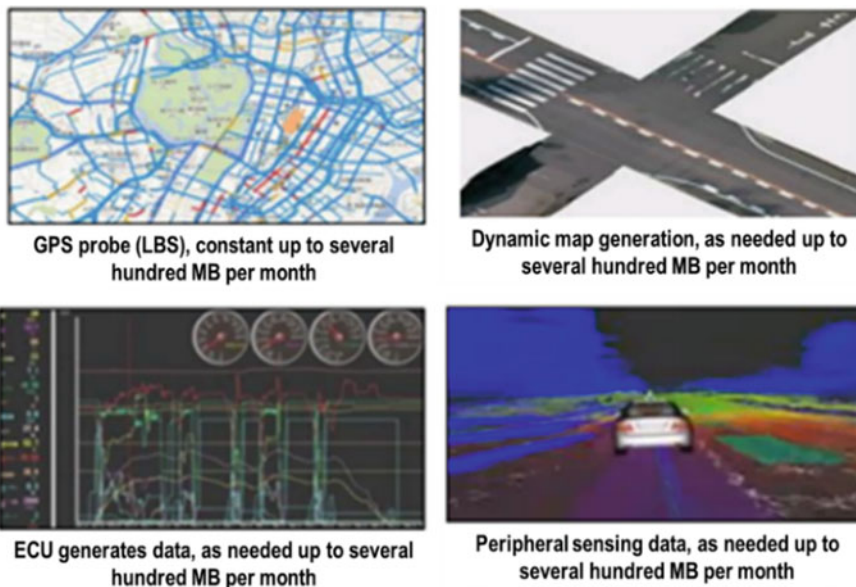


Fig. 11.6 Volume of connected car data transfer

### 11.4.2 Connected Vehicles Generated Mobility Data Collection Methods

It is clear that connected vehicles generate a lot of mobility data but what kind of data are we looking for and what collection methods do we employ? We are looking for driving history data, vehicle status data, and driving behavior data. Driving history data is all the data stored by the vehicle during operation and the location data for when the vehicle is in motion. The vehicle status data is the kind of data that includes current status of the battery, engine temperature, fuel quantity, tire pressure, etc. Last, “driving habit data” as it is known includes actual data such as that of rapid acceleration, sudden stopping, etc. Driving history data such as location and speed data can be collected using connected mobile devices with the help of GPS. Vehicle Status data can be collected using the OBD-II device plugged into the vehicle. Driving behavior data can be collected using vehicle to everything communication as presented in vehicle mobility data collection.

If we look a bit deeper into what are the sources of all these mobility data points, we can observe that modern GPS probes and location-based services are generating hundreds of MB of data per month. Even the simplest dynamic map generation and real-time user tracking require 100 s of MB. The automotive electronic control unit that controls at least one of the electrical systems or subsystems in a vehicle likewise creates a few several MB data for every month. Last, even the peripheral detecting modules introduced in autonomous vehicles are producing comparative measures of data every month. Figure 11.7 has introduced the sources of vehicular mobility data.



**Fig. 11.7** Sources of vehicular mobility data

### ***11.4.3 Connected Vehicle Sensors and Data Collection***

Connected vehicles are a constellation of computer chips and mechanical, electrical, electronic sensors that are managed by information technology. One main purpose is data collection in ever increasing volumes since even current, non-connected vehicles process up to 25 gigabytes of data an hour. One can only imagine how much computing power a connected vehicle requires to manage vision, guidance and the mapping technology in order to process this ever-growing volume. In the 1970s, vehicles were 100% hardware while the projections for 2025 forecast that almost half will be software and new applications.

## **11.5 Vehicle Data Processing**

Vehicle data collecting and processing is of paramount importance. The data is meaningless if nothing happens after it is collected. In its raw form, data is of no use. The decentralized data collected must be uploaded to the cloud where raw data analysis, data processing, model design and data training takes place. We do all of this to get to meaningful information as presented in Fig. 11.8



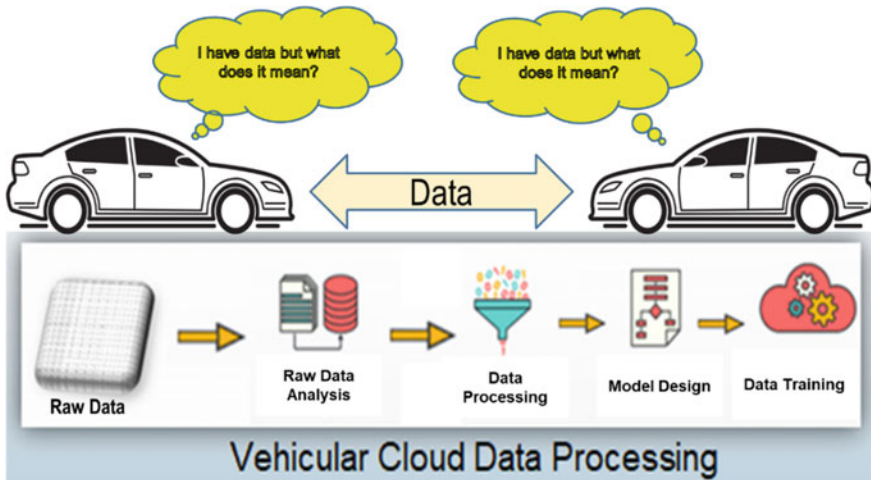


Fig. 11.8 Vehicular data processing

After collecting various types of data from the vehicle, it is processed at a high level before to extract meaningful information that can be used to improve the vehicle efficiency, driving behavior, vehicle safety, etc.

In the above table on the left side we can see, what the collectible data looks like listed with names and descriptions. Respectively, on the right. The table shows again the data point name with a description of the actual information we obtain after the processing stage. Next, we will analyze the whole workflow from data collection, to information generation, to the final upload to the cloud.

### 11.5.1 Vehicle Cloud Data Processing

As we know that vehicle cloud data processing can be very tricky because we are talking about a lot of data that is both heterogeneous and complex. Let us look at the whole workflow from data ingestion to information generation in the cloud. After the collection, in the data ingestion platform the raw data along with the driver and vehicle meta data is ingested in a data lake. From there it is further processed by applying data cleaning, data exploration and feature engineering techniques. Now the data is ready to be put into a data normalization model or a machine learning model. These models can generate information and make relevant predictions for business functions such as insurance, car sharing, logistics, etc. The final information is displayed on a dashboard or a smart phone application. This information process generation runs in a cycle with new data continuously pouring in. Since the process runs over and over again, it leads an ever “smarter” or more refined model and thus provides more and more trustworthy information as represents in Fig. 11.9.

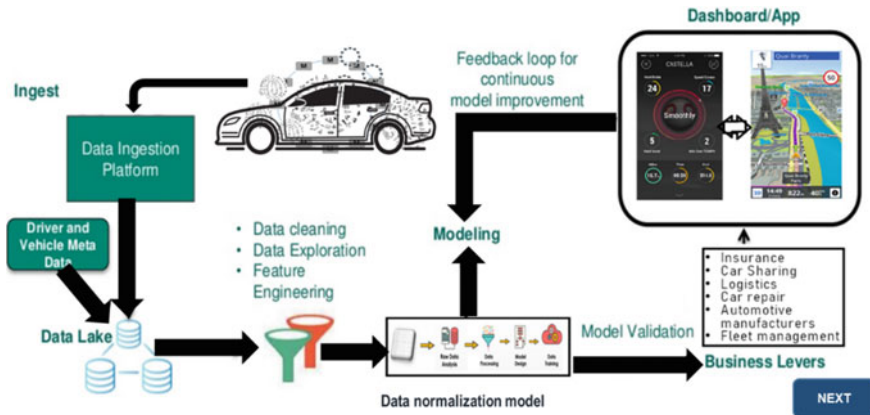


Fig. 11.9 Workflow of vehicle data processing

### 11.5.2 Vehicle Mobility Data Services

The present and future mobility data services. In the current environment, vehicle mobility data services are already in use in the areas of location-based solutions, determining a vehicle life cycle, in corporate vehicle management, and in services such as insurance, etc. However, in the future we expect that the mobility data will also be used for the vehicle sharing management system that it will provide and improve autonomous driving solutions, that manufacturers will be able to purchase data from the vehicle owner, that maintenance and accident history management will be available, that non-identified data utilization solutions will be implemented, and finally that biometric data collection will also be employed and utilized. With all these new and exciting possible future applications, the value and availability of the vehicle mobility data will go up exponentially.

The current situation regarding connected services offered by the Toyota Car manufacturing company. This particular car manufacturer offers emergency notification service, theft tracking, automatic map data updates, and operator assistance as shown in Fig. 11.10. This is possible mainly because of the OBD-II device mounted on these cars that provide real-time data. The manufacturer’s smart center provides various additional services such as traffic information and “look ahead” information services that stem from the big data vehicular database.

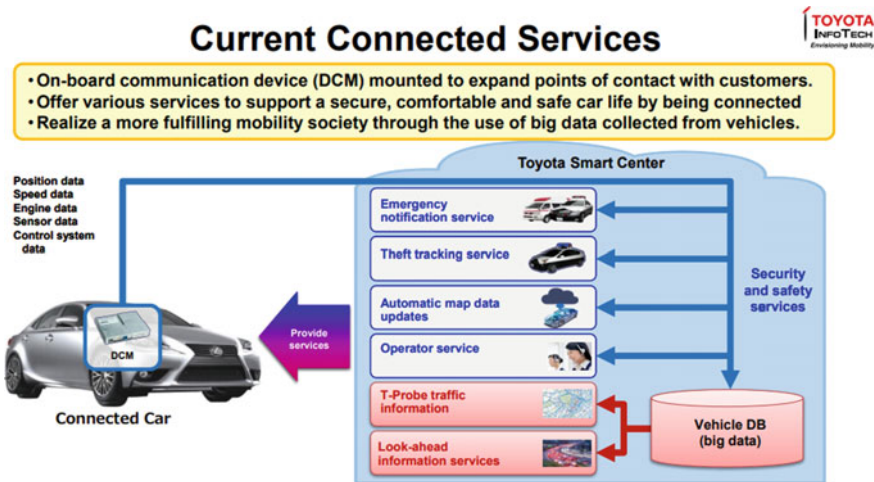








Fig. 11.10 Example Toyota vehicle connected services

### 11.5.3 Services Using Mobility Data

It is obvious that different kinds of data collected can be categorized based on the types and the services they can contribute to. Here under data category, we list the kinds of data collected. Such data as those regarding road condition, traffic volume, etc. are used today for real-map service for navigation but can also be used in the near future to provide a real-time road situation report which the driver can use in determining an efficient and safe route to their destination. It can also contribute to a 3-step conditional autonomous driving which means that the vehicle can take over all driving functions under certain circumstances. Data that describes vehicle condition is collected today by the OBD-II and can make emergency phone calls if there is an accident. In the future, it can be used in predicting vehicle functionality anomalies and help the driver schedule services remotely. It can also keep a certified and accurate vehicle history stored in the cloud that could be used when the car is sold in the future to determine the resale value. Last, vehicle usage data are used today by insurance companies to offer customized contracts and by fleet management systems. In the future, this data can be used to enhance the vehicle sharing platform services, facilitate large vehicles with special cargo on one control platform and share economic logistics infrastructure which is an essential part of all logistic systems as shown in Fig. 11.11.

**Services Using Mobility Data**

Data Category	Present	Estimated in 2020-2025
 <b>Road condition, traffic volume</b> (ex: road icing or fog, road congestion information, etc.)	 <ul style="list-style-type: none"> <li>- Real-time map service</li> </ul>	<ul style="list-style-type: none"> <li>- Real-time road situation report</li> <li>- 3-step Conditional autonomous driving *</li> </ul>
 <b>Vehicle condition</b> (ex: engine oil, airbag, fault code, etc.)	 <ul style="list-style-type: none"> <li>- OBD2 vehicle diagnosis</li> <li>- Emergency rescue system (e-call)</li> </ul>	<ul style="list-style-type: none"> <li>- Pre-predicting vehicle anomalies, scheduling remote services</li> <li>- Accurate vehicle history management (certified intermediate)</li> </ul>
 <b>Vehicle Usage</b> (ex: speed, position, average loading capacity)	 <ul style="list-style-type: none"> <li>- Customized insurance (UBI)</li> <li>- Fleet Management System (FMS)</li> </ul>	<ul style="list-style-type: none"> <li>- Enhanced vehicle sharing (P2P vehicle sharing)</li> <li>- Large vehicle, special cargo control platform</li> <li>- Shared Economic Logistics Service Infrastructure</li> </ul>

\* SOURCE: McKinsey Report(2018)
\* 3-step conditional autonomous driving: limited autonomous driving by artificial intelligence in the car. Driver intervention is required under certain circumstances.

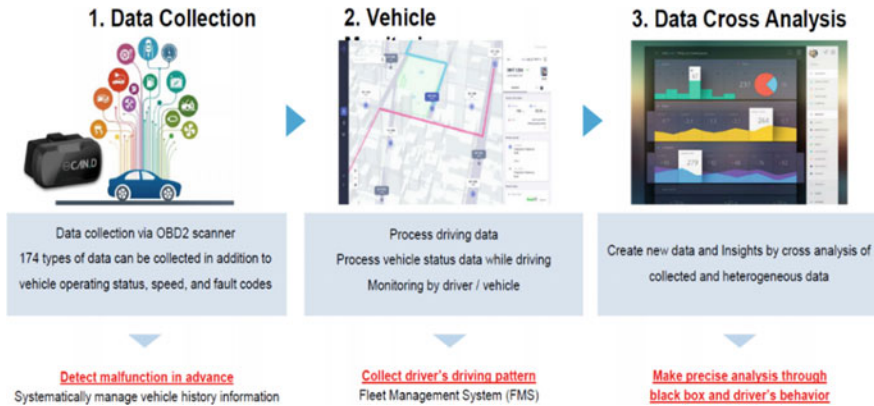
**Fig. 11.11** Services using mobility data

## 11.6 Future Data Mobility for Connected Vehicles

The future mobility data management for connected vehicles, the process can be summarized into three steps: First is data collection via the OBD-II scanner which can detect malfunction in advance. Second, from the vehicle we process all of the collected driving data and from this data we can determine the driver’s driving pattern. Finally, by conducting data cross analysis, we can create new insights through cross analysis of collected and heterogeneous data. This can offer us insight in the driver’s behavior as shows in Fig. 11.12.

## 11.7 Summary

In this chapter we gave discussed the vehicle data Safety and Security, relationship between Automotive safety, security and reliability, In vehicle Security threats, outside Vehicle security threats, automotive security versus Safety Process, vehicular cloud management system, automotive trust between safety and security vehicle mobility data processing, vehicle mobility data market size, volume of connected car data transfer, vehicle mobility data collection. Also shows the sources of vehicular mobility data, connected vehicle sensors and data collection, vehicular Data



**Fig. 11.12** Future data mobility for connected vehicles

Processing and workflow of vehicle data processing, services using mobility data, and discussed the future data mobility for connected vehicles.

**Acknowledgements** This research was funded by Woosong University Academic Research in 2021.

## References

1. R. Pal, A. Prakash, R. Tripathi, D. Singh, Analytical model for clustered vehicular ad-hoc network analysis. *ICT Express* (2018). <https://doi.org/10.1016/j.ict.2018.01.001>
2. J.E. Meseguer, C.T. Calafate, J.C. Cano, P. Manzoni, Driving styles: a smartphone application to assess driver behavior, in *2013 IEEE Symposium on Computers and Communications (ISCC)*, Split (2013), pp. 000535–000540. <https://doi.org/10.1109/ISCC.2013.6755001>
3. Y. Zhang, W. Lin, Y. Chin, Data-driven driving skill characterization: algorithm comparison and decision fusion. *SAE Technical Paper 2009-01-1286* (2009). <https://doi.org/10.4271/2009-01-1286>
4. D. Singh, M. Singh, I. Singh, H.-J. Lee, Secure and reliable cloud networks for smart transportation services, in *The 17th IEEE International Conference on Advanced Communication Technology (ICACT2015)*, Phnix Park, South Korea (2015), pp. 358–362
5. Pal, N. Gupta, A. Prakash, R. Tripathi, Adaptive mobility and range-based clustering dependent MAC Protocol for vehicular Ad Hoc networks. *Wireless Pers. Comm.* 1–16 (2017)
6. Y. Chen, M. Fang, S. Shi, W. Guo, X. Zheng, Distributed multi-hop clustering algorithm for VANETs based on neighborhood follow. *EURASIP J. Wirel. Comm. Netw.* **1**, 98–109 (2015)
7. X. Yang, Y.K. Chia, S. Sun, H.F. Chong, Mobile data off-loading through a third-party WiFi access point: an operator's perspective. *IEEE Trans. Wireless Commun.* **13**, 5340–5351 (2014)
8. D. Singh, M. Singh, I. Singh, H.J. Lee, Secure and reliable cloud networks for smart transportation services, in *The 17th IEEE International Conference on Advanced Communication Technology (ICACT2015)*, Phnix Park, South Korea, 1–3 July (2015)
9. D. Singh, G. Tripathi, S. C. Shah, R.R. Righi, Cyber-physical surveillance system for the internet of vehicles, in *IEEE World Forum on Internet of Things WF-IoT 2018*, 5–8 February 2018, Singapore, pp. 551–556 (2018)