Journal of Cases on Information Technology
Volume 23 • Issue 3 • July-September 2021

Information Management Challenges in Autonomous Vehicles:
A Systematic Literature Review

Adrija Ghansiyal, G.B. Pant Government Engineering College, Delhi, India
https://orcid.org/0000-0003-1656-5340

Mamta Mittal, G.B. Pant Government Engineering College, Delhi, India

Arpan Kumar Kar, Indian Institute of Technology, Delhi, India
https://orcid.org/0000-0003-4186-4887

ABSTRACT

The focus of automobile industry is towards producing efficient driverless cars that are risk free and with zero tolerance to safety violations thereby following in the footsteps of autonomous robots. In this study, the author elaborates on the vulnerabilities relevant to internet of things technology implementation in these connected cars, commonly termed as internet of vehicles. This topic has already been discussed frequently by the research community; however, the main contribution of the paper is to establish the connection of information management with autonomous systems, an aspect that other literatures lack. The focus of the study is on presenting a brief introduction to the foundation technologies used in the connected vehicles. It also aims to summarize the various security methods that have been used infrequently and could be further explored in future research.

KEYWORDS

Autonomous Vehicles, Information Management, IoV, Self-Driving Cars, VANET

INTRODUCTION

Owing to the current advancement in technology, the autonomous industry's predilection for Autonomous Vehicles (AVs) is plausible. It has been observed that automobile companies have proliferated ever since leading market giants like Tesla, Volvo and Bosch have contributed towards this field of research and towards the field of Industry 4.0. The concept of self-driving cars was first introduced by Norman Bel Geddes in 1939 GM's exhibit which instigated the automotive industry to persevere in this domain. Thus, all the efforts are put forth to achieve a singleton goal of making these autonomous robots, a commercial product with complete social acceptance. Among the various technologies used in these self-driving cars, the most prominent one is, Internet of Things (IoT) which encompasses the ability to transfer data over a network without human interaction. Subsequently, the efficient operation of an AV requires extensive efficient information management for service delivery.

DOI: 10.4018/JCIT.20210701.oa5

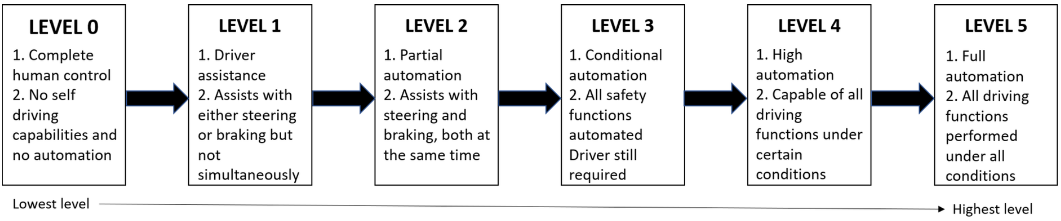
Information management enables the stakeholders to manage their data assets judiciously using information and communication technologies (ICTs) to make effective decisions and meet operational and strategic objectives. It is a cyclic process of collecting and identifying needs, storing and organising information, dissemination of products and services and ultimately destruction of information (Detlor, 2010). With the disembarkation of the shared communication, demand responsive transit and telematics-based system in AV, new information management methods are required to support this developing field of technology. Szilárd Szigeti *et al.* (Szigeti, Csiszár, & Földes, 2017) study presented a coherent model of the architecture and functions of the complex information system, taking into account its operators and users, which further aimed to aid in the future development of related projects.

According to Hussain and Zeadally (Hussain & Zeadally, 2019), an autonomous car can be defined as a computer-controlled entity which can automatically detect and identify the essential features in its surroundings and accordingly make decisions to operate smoothly without threat to ethical and safety standards. As suggested by the National Highway Traffic Safety Administration (NHTSA), they can be classified into levels of autonomy which is delineated in Figure 1. (The Evolution of Automated Safety Technologies, n.d.). Level 0 encompasses the vehicles with complete human control where functions are performed manually by the driver. Level 1 depicts 'driver assistance' which includes common functionalities present in majority of the cars nowadays, such as cruise control. 'Partial automation' is depicted by level 2, which activates in peculiar scenarios and aids in the automatic acceleration, steering and applying brakes in the car. However, the vehicle's independent decision is still considered to be the responsibility of the driver and therefore human alertness is a necessity. Level 3 refers to the 'conditional automation'. This activates when the favourable situations exist and the autonomous system can perform various driver tasks on its own along with the precaution that the driver must be prepared to overtake the controls whenever necessary. Level 4 corresponds to high automation which means on the suitable conditions of the surroundings, the AV can perform complete operations independently without any input from the human. Furthermore, in level 5, 'full automation' is expected and this is where self-driving is justified to its full potential. The vehicle underlying in this category can handle any road and any condition that a human driver can face thus the only input required from the driver is to enter destination. Indeed, within the purview of the discussed architecture, the automotive industry is currently as level 2+ (Ionita, 2017). Meanwhile, level 3 vehicles are commercially available, their competency is yet to be proved. However, in the current scenario, there is no strict definition for the levels of autonomy due to which, any level of autonomy is referred to as autonomous (Faisal, Yigitcanlar, Kamruzzaman, & Currie, 2019).

LITERATURE REVIEW

According to research conducted by McKinsey & Company, level 4 autonomy is expected to be available between 2020 and 2022, followed with full adoption in due course. Furthermore, Level 5 technology is expected to arrive by 2030 at the earliest, anticipating greater adoption by that time. The potential growth of this industry is estimated to rise tremendously from 2019 to 2026, approximately

Figure 1. Commonly referenced levels of Autonomy



LEVEL 0
1. Complete human control
2. No self driving capabilities and no automation

LEVEL 1
1. Driver assistance
2. Assists with either steering or braking but not simultaneously

LEVEL 2
1. Partial automation
2. Assists with steering and braking, both at the same time

LEVEL 3
1. Conditional automation
2. All safety functions automated Driver still required

LEVEL 4
1. High automation
2. Capable of all driving functions under certain conditions

LEVEL 5
1. Full automation
2. All driving functions performed under all conditions

ten times of the current scenario. The study from Portland, Oregon based Allied Market Research, predicted that global market for of this industry will be worth $556.67 billion with a compound annual growth rate of 39.47% by the end of 2026, which is a significant jump from the current estimation of $54.23 billion in 2019. The research highlighted that the hardware segment of AV which accounts for three-fifth of the total market revenue, is expected to dominate through 2019-2026. The study also highlighted that the services segment would register the fastest Compound annual growth rate (CAGR) of 46.17% during the estimated period. The report profiled the key players which are targeting this particular market domain, some of them are: Ford Motor Company, Volkswagen Group, General Motors, BMW, Toyota Motor Corporation, Renault-Nissan-Mitsubishi alliance, Tesla Inc. and AB Volvo.

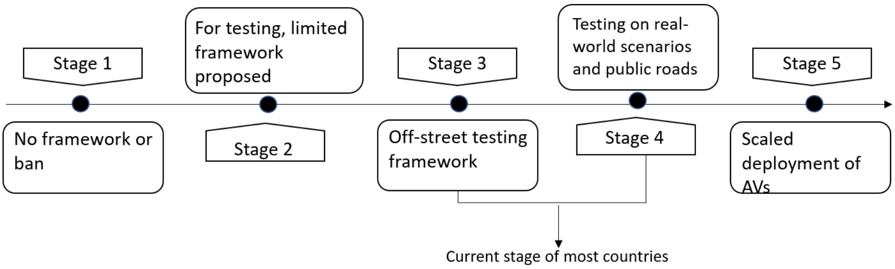
In addition to the acquisition of humongous data, IoT devices embedded in these driverless cars are also helpful in updating the pertinent algorithms that assist in decision making process opted by the automated driving system. Through this connectivity of things, communication is established within the network and information is shared among the interconnected devices, enabling them to keep track of road conditions, follow an optimized route and efficiently navigate through obstacles thus creating a reliable autonomous robot. All the relevant information is uploaded to a cloud server for analysing it and aiming for the improvement in the automation. This forms a major part of the Industry 4.0.

Thus, to make intelligent decisions, it entails interconnectivity of vehicles which is generally termed as Internet of Vehicles (IoV) and follows the paradigms of IoT (Abu Talib, Abbas, Nasir, & Mowakeh, 2018). Indeed, this technology has gained massive popularity in the recent past and various authors have done extensive research pertaining to its privacy and security threats. From the viewpoint of communication, the Vehicle-to-Everything (V2X) can be broadly classified into 3 categories enumerated as: (i) Vehicle-to-Vehicle (V2V) (ii) Vehicle-to-Infrastructure (V2I) and (iii) Vehicle-to-Cloud (V2C). The technologies used in connected cars are also shared with AV to incorporate the features of inter vehicular communication. One such technology is Vehicular Adhoc Network (VANET) which entails an On-Board Unit (OBU) integrated in the vehicle. VANETs have emerged as one of the most robust, reliable and rapidly-growing subdivisions of the Mobile Adhoc Networks (MANETs) (Arif, Wang, Zakirul Alam Bhuiyan, Wang, & Chen, 2019). Furthermore, Dedicated Short-Range Communication (DSRC) is used as the standard protocol of communication in this network, which is range constrained as well. The need for making crucial decisions from available assets and within a limited time window, necessitates this technology to be fast.

Another addition to the IoV technology is the Social Internet of Vehicles (SIoV) which applies to the Social Internet of Things (SIoT) concept of empowering devices with consciousness (Butt, Iqbal, Shah, & Umar, 2018). This consciousness aids the smart devices in familiarising themselves with the surrounding devices on the basis of knowledge gathered, which is similar to human behaviour. This revolutionizing technology adds values to the existing VANET and aims to improve the existing Intelligent Transport System (ITS).

Furthermore, another prominent technology which is imperative in the modelling of the smart-vehicle is Artificial Intelligence (AI). R.B. Sulaiman (Bin Sulaiman, 2018) highlights various impacts on the legal, social and ethical challenges, and important environmental constraints associated with driverless cars. Research studies have shown that majority of these issues are due to lack of fail-proof software, undetailed maps and slow sensors. In May 2016, Tesla's car accident occurred while being in autopilot mode. It was quoted by Tesla in its blog post that brake failure occurred because both, the autopilot and the driver were unable to differentiate the white side of a tractor trailer from the brightly lit sky. This implied that the domain needed further exploration which led the researchers to shift their focus onto this area. Therefore, in order to make commercial launches of the AVs, multiple companies have planned various stages for the operation and testing of the autonomous system which is indicated in Figure 2.

Figure 2. Evolution of Autonomous Vehicle Regulation


Stage 1
No framework or ban
For testing, limited framework proposed
Stage 2
Stage 3
Off-street testing framework
Testing on real-world scenarios and public roads
Stage 4
Stage 5
Scaled deployment of AVs
Current stage of most countries

Besides the vast research studies presented in the field of autonomous systems, there is no concrete work done towards the information management regarding the Connected and Automated Vehicles (CAVs) and its relationship with the vehicular communication. Therefore, the purpose of this study is to determine major security concerns related to IoV and offer insights for the development of an information management system for an AV. Due to the open wireless access medium, the security and privacy becomes quite critical in VANETs (Ali, Hassan, & Li, 2019). Thereby, this review also attempts to identify threats and vulnerabilities of different sub-technologies under IoT that are used for vehicular assistance.

The paper has been organised into six sections. *Section 1* and *Section 2* present the description of AV along with its technologies. This section also provides an overview of the key issues encountered in that area. *Section 3* discusses the methodology adopted by the review along with the criteria for exclusion and inclusion of papers. Further, in *Section 4*, the product liability and the challenges and security concerns of technologies used in AV are presented, thereby answering the research questions. *Section 5* discusses the paper as a summary and the key points observed while the study was conducted. Finally, the future work and conclusion of the review is given in *Section 6*.

METHODOLOGY

The systematic literature review consists of four phases: the planning, conducting the research, reporting and the final result employed in the presented work. In the planning phase, the online digital libraries were referred to gather the required resources and after exclusion of irrelevant papers, the resulting journals were analysed. While conducting the research, the problems and solutions discussed by various authors is studied and have been discussed under 'Findings' section. Furthermore, the procedure followed in this systematic literature is depicted in Figure 3.

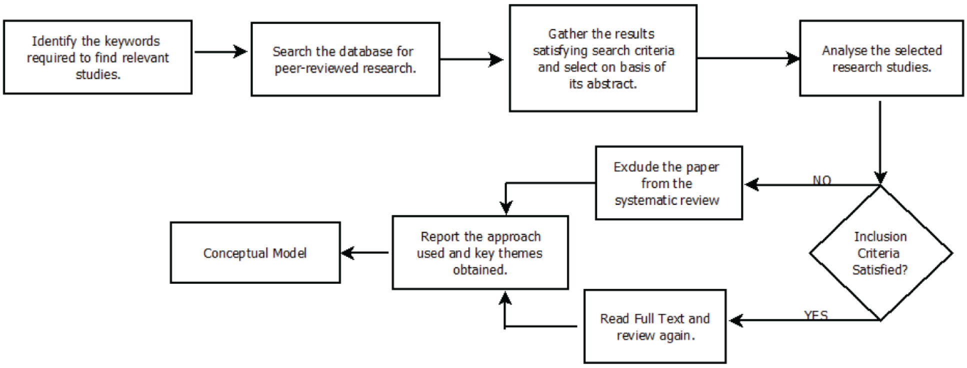
In this work, an attempt has been made to perform a survey of dominant complications faced by the technology and communication in CAVs and provide a systematic literature review for the same. The authors aim to answer the considered research questions in line with information management:

RQ1: How does AV use impact product liability?
RQ2: What are the main challenges for IoV communication?
RQ3: What are the main security concerns in an AV with respect to IoV?

Planning the Review

The most preferred knowledge source suitable for this systematic review is 'Scopus' database. It assisted in finding the required research studies that have been indexed and peer-reviewed in accordance with science-research. From Scopus, following (Chakraborty & Kar, Swarm Intelligence: A Review

Figure 3. Stages for selection process followed in this literature review


Identify the keywords required to find relevant studies.
Search the database for peer-reviewed research.
Gather the results satisfying search criteria and select on basis of its abstract.
Analyse the selected research studies.
Exclude the paper from the systematic review
NO
Inclusion Criteria Satisfied?
YES
Read Full Text and review again.
Report the approach used and key themes obtained.
Conceptual Model

of Algorithms, 2017), (Agarwal, Chauhan, Kar, & Goyal, 2017), (Chakraborty & Kar, A Review of Bio Inspired Computing Methods and Potential Applications, 2016), (Chauhan, Agarwal, & Kar, 2016) were referred for the approach analysis. Other research sources include: (i) IEEE Xplore Digital Library, (ii) Elsevier Science Direct, (iii) Wiley Online Library and (iv) Directory of open access journal. Other studies which were referred for research-based analysis are (Mittal, Goyal, Hemanth, & Sethi, 2019), (Mittal & Pandey, The Rudiments of Energy Conservation and IoT, 2019) and (Singh, Gahlot, Samkaria, & Mittal, 2019), which focused on IoT based intelligent systems.

Conducting the Review

The syntax used for searching the relevant studies for this review was based on Boolean operators. The keywords which were used in the search string followed AND/OR operators. The first thematic search was conducted using the following keywords: ("autonomous vehicle" OR "smart cars" OR "automated vehicle" OR "driverless cars" OR "connected vehicles"). This resulted in more than 88,294 journals and papers. Subsequently, the next thematic search consisted of following terms: ("information management") AND ("autonomous vehicle"). The final search comprised of: ("autonomous vehicle") AND ("artificial intelligence") AND ("vulnerabilities" OR "security threat" OR "limitations"). The search results were scrutinized, and relevant papers were taken into accounts based on their abstract or by reading full text if needed. Another search included the keywords: ("VANET" OR "V2X technologies" OR "vehicular adhoc networking" OR "IoV") AND ("attacks" OR "intrusion" OR "limitations") to extract the studies that could potentially answer the research questions.

Reporting the Review

The inclusion criteria considered the articles published between 2014 and 2019 because this period witnessed the sudden burst in the advancements and emergence of improved technology in this industry. Moreover, this study considered only the peer-reviewed research papers and the reports released by reputed and competent organisations. The inclusion criteria consisted of studies which aimed to provide information and solution for challenges faced by AV, through proposed models and algorithms. The articles that provided an introduction to the forthcoming technologies in connected vehicles and also the studies which focused on limitations and liabilities faced by underlying technologies in self-driving cars, were also included. The exclusion criteria considered the non-peer reviewed articles, unpublished papers and blog articles. In addition to that, research studies that only focused on history and establishment of the technology, were excluded. Microsoft Office Excel and Mendeley software were used to manage the literature gathered during the conduction of this study.

Result

A total of 112 papers were shortlisted that fulfilled the search criteria, out of which 82 articles were taken into account. Further, based on the extracts of the initial 112 papers, a graph is shown in Figure 4. Consequently, 8 papers were excluded from the study due to their nascent approach to the research questions and accordingly exclusion was done to remove irrelevant studies. Finally, the 68 papers that made it through, were read in full-text document, investigated and reviewed again. Figure 5 explains the frequency spread of the relevant studies selected across the considered time period. Along with them, 6 website articles were included in the research study which provided a better insight to the topic. The word cloud of Figure 6. illustrates the dominant keywords that are used in the final 62 selected articles.

FINDINGS

The evolution of connected cars has undergone through various phases, out of which, five major phases discussed by X. Krasniqi and E. Hajrizi (Krasniqi & Hajrizi, 2016) are: (i) Research and Development era - Ideas and technologies that would pave the path for driverless cars were proposed during this era. (ii) The Embedded era - Smaller modules were embedded in cars which led to establishment of wireless communication. (iii) Infotainment era - This marked the integration of information and

Figure 4. Classifications based on the keywords found in the abstracts of research studies

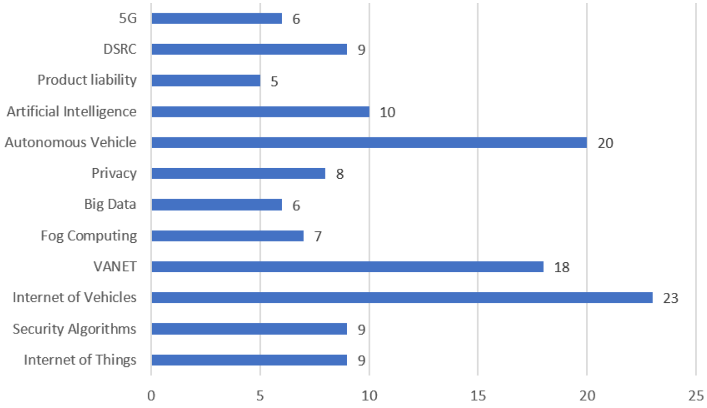


Figure 5. Distribution of the selected papers according to their year of publish

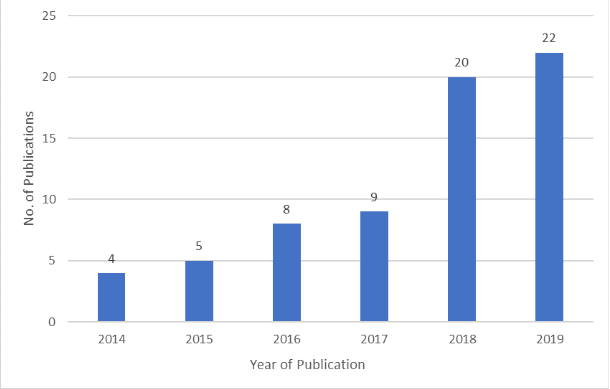
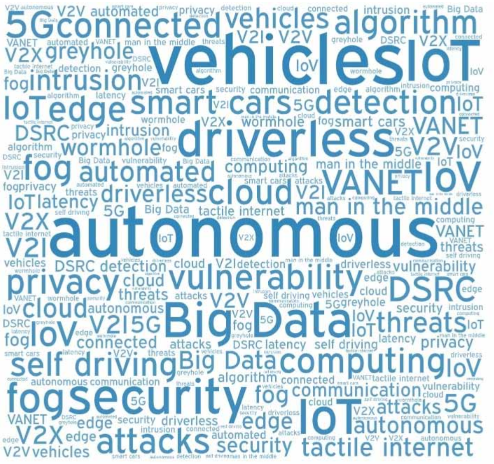


Figure 6. Word Cloud of the prominent keywords in observed in the selected studies



entertainment applications in the vehicle. (iv) V2X era - The communication between vehicles and infrastructure was introduced as an additional feature which would assist the AV in making better decisions. (v) New Mobility era - This refers to the future scenario when prototypes of AV will become society owned assets and carmakers would be competing for dominance.

Product Liability (RQ1)

The adoption of self-driving cars entails greater insights to the challenges and liabilities faced by the manufacturing companies and the researchers. Y.K. Dwivedi *et al.* (Dwivedi, et al., 2019) focused on challenges with regard to implementation of AI technologies categorised into various domains such as, (i) social (ii) data (iii) organisational and managerial (iv) political and legal (v) ethical challenges. According to the study, the amalgamation of AI technologies with AVs could result in a ginormous impact on industries in the terms of economical investments and working practices. The systematic literature review conducted by S. Urooj *et al.* (Urooj, Feroz, & Ahmad, 2018) reported liabilities and responsibilities during accidents and ethical decisions made by the AVs. The study accessed the liability of these car accidents under the situation where vehicle becomes unmanageable during a virus attack or some abrupt system failure. The authors assert that applying animal laws (for example, canine ownership liability) to automobile accidents is conceivable owning to the similarity in the purpose they both serve. However, the strict liability may discourage the consumers from purchasing this technology. Thus, products liability addressed to this issue, emphasizing that for casualties occurring in autonomous mode for "Disabled driver" and partially for "Diminished capabilities driver", AV manufacturer should be held responsible.

K. Grieman's (Grieman, 2019) study examines the potential liability for accidents of these robotic cars which could be allocated to the owner, the car's manufacturer, the manufacturer of AV components, or the government, according to the scenario encountered. It aims to address the difficulty faced by the product liability (Urooj, Feroz, & Ahmad, 2018) concerning the expenditure on the legal procedure involved in diagnosing the liability, and in identifying the reason behind AV's decision. The analysis primarily focused on fully autonomous vehicles with the limited scope of privately-owned vehicles. Thus, with the onset of Industry 4.0 and with an intention of bringing these self-driving cars into the market, manufacturers in tandem with a self-sufficient entity which is detached from the company, need to test the vehicles under consideration. This will strengthen the vehicle reliability in terms of safety and driving quality which abides to all the regulations on humane grounds and welfare of the society as well.

Challenges of IoV Communication (RQ2)

The intelligent driving systems are observed to exercise a fundamental feature - Vehicle following, which is made possible through IoV communication. Thus, requirement of detection and recognition of various automotive components is imperative for preventing collisions or accidents. J. Wang *et al.* (Wang, et al., 2016) developed a binary-levelled approach for the real time detection of vehicles and recognition of their brake lights using a multi-layer perception (MLP). The proposed model identified the vehicle by combining multi-layer Light Detection and Ranging (LiDAR) and a camera and the classification of the vehicle as “brake” or “normal” was done using the neural network. This approach resulted as a cost-effective and a robust solution. However, based on the discussions of various facets of self-driving cars, it is noted that one of the major issues encountered is the inefficiency of software and sensors employed in an AV, which establishes a direct link to IoV. Although IoV has provided a tremendous support in facilitating interconnectivity of AVs, it still faces many challenges that need to be examined in order to deliver a better and safer autonomous transportation.

Latency

In the coming age of connected cars, road safety will be of paramount importance which makes it necessary for communication to take place at higher data rate. Furthermore, wireless communication plays a vital role in providing synchronisation between different entities during transmission and reception of critical data like road conditions, traffic movements and pedestrian and vehicular movement. The current technologies that are widely used by the AVs are DSRC and 4G-cellular LTE. But due to their limitations in time-bound missions, 5G cellular communication has emerged into the industry with the aim to resolve this issue.

Currently, the dominant technology in the United States is DSRC, which enables V2V and V2I communication directly, without involvement of cellular or other infrastructure. A frequency spectrum of 75MHz in the 5.9 GHz band has been allotted for safety and mobility applications in Intelligent Transportations Systems (ITS). Although, this technology has support from major automobile companies like Honda, Toyota and Nissan, 5G has been favoured by Volkswagen and Ford Motor Company. Moreover, with the Chinese company Baidu completing a test of 5GLTE-enabled autonomous cars successfully, a significant increase in popularity of this technology was observed among the automakers. Subsequently, the combination of V2V communication in an ITS presents some obstructions as well, broadly specified into three scenarios: (i) the willingness to accept the security and operation rules by the car manufacturers (ii) ensuring the data confidentiality and maintaining user privacy over the network and (iii) the monetary support needed for developing and employing the suitable technologies into an AV (Arena & Pau, 2019).

The 4G network is a faster communication network in terms of sharing status and requesting rides, however it only acts as medium of transferring data and cannot aid in making intelligent decisions for the AVs (Tanwar, Tyagi, Budhiraja, & Kumar, 2019). 5G network communication provides another advantage by operating without relying on the field coverage of wide area network. 5G Vehicular Cloud Computing (VCC) systems use miscellaneous network access technologies for fulfilling the requirements of advanced services (Skondras, Michalas, & Vergados, 2019) hence this technology forms an essential component of the Industry 4.0. However, even after being a high speed and low power LTE System, another internet network emerged to provide wide availability, highly-secure end-to-end communication and reliable system along with low transfer latency of less than 1ms – Tactile Internet (TI). This state-of-the-art technology poses another challenge to the researchers, of how to integrate TI in AV. This remains an open question to the research community and requires further analysis which can be a part of future work.

Heterogeneity in Communication Technology

Wireless communication technology is one of the fundamental parts of a connected vehicle directly affecting the implementation, interoperability and performance of the transportation applications (Qu, et al., 2017). Zhigang Xu *et al.* developed a model which recorded the GPS positions and certain parameters related to wireless communication in the test vehicles. Based on the results, authors drew a comparison between DSRC and 4G-LTE and provided a conclusion on which technology to prefer for different needs. For the non-safety applications, encompassing file download, transmission of traffic information or Internet access, 4G-LTE is preferred. Meanwhile, DSRC is favoured when focus is placed on safety applications, such as, avoidance of collision. According to Shailen Bhatt, president and CEO of the Intelligent Transportation Society of America, the split approach of choosing DSRC or 5G, would undermine the life-saving potential of the vehicle (Bigelow, 2019). This issue needs to be addressed since it directly affects the interoperability of the system, which is necessary for the AV.

DSRC permits two-way medium range wireless communication similar to WiFi. A. Fitah *et al.* (Fitah, Badria, Moughit, & Sahel, 2018) presented a study based on implementation of various tools to achieve a feasible mobility model for real vehicular traffic and analysing the performance of WiFi and DSRC on end-to-end delay, successful delivery rates and throughput. The result showed that DSRC outperforms WiFi in all three categories hence the mass adoption of the given technology was favoured. Furthermore, as an improvement to the existing communication technology, cellular 5G technology emerged and was promoted for its application in V2X connectivity by Jessica Nigro, General Manager of Technology and Innovation Policy at Daimler North America (Lewis, 2018). The 5G-V2X aimed to manage the high demands of reliability, throughput and low latency along with the better the security mechanisms as compared to LTE-V2X (Sharma, You, & Guizani, 2019).

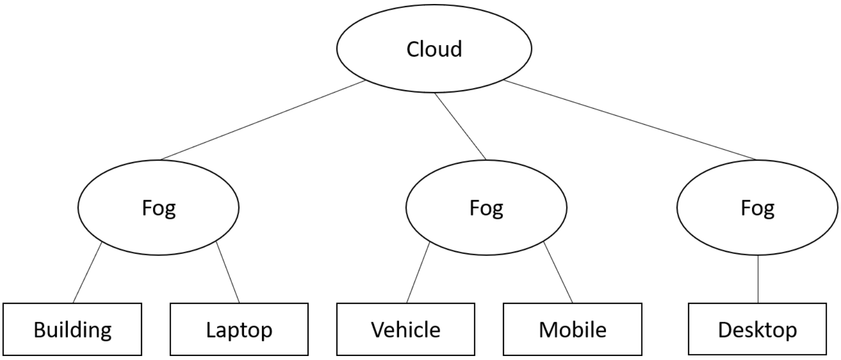
Data Generation and Big Data Management

The resource requirement for an AV is enormous. This is in view of the fact that a reliable infrastructure is needed to perform critical operations and is applicable to all the modern technologies that will be a part of the Industry 4.0. Thus, a study conducted by Intel in 2016 showed that a humongous amount of data would be generated by these ITS, approximately as much data as 3 billion people, assuming that average internet user produced 1.5GB data per day which approximates to 4000 GB per day (Barua, n.d.). The apportionment of this calculation is depicted in Table 1. In the generated data, the focus is placed on the hardware components of these vehicles Several sensors are used such as, gyroscope, odometers, magnetometer, accelerometer and a landscaping camera for localizing a landmark (Santos, Sappa, Oliveira, & de la Escalera, 2019). The factory vehicles employed for logistics and transportation generally use range sensors to perceive their surroundings (Yilmaz & Temeltas, 2019). Furthermore, industrial IoT collects ginormous amount of information about activities and events in the city and its inhabitants. This accumulation of big data welcomed another large set of solutions proposed for traffic monitoring, energy-saving systems and managing critical events and emergencies (Mijac, Androcec, & Picek, 2017). Therefore, the most suitable solution for data processing came into view – Fog computing. Its position in the communication hierarchy can be seen in Figure 7.

Table 1. The amount of data consumed by different real-time services integrated in a general AV

Component	Data Consumed (per sec)
Cameras	20-40 MB
RADAR	10-100 KB
SONAR	10-100 KB
GPS	50 KB
LIDAR	10-70 MB

Figure 7. Fog Computing architecture for facilitating faster cloud services for V2I and V2V communication (from broader perspective)



Wenchao Xu *et al.* (Xu, et al., 2018) discusses various challenges faced by IoV in the domain of Big Data: (i) Harsh Wireless Channel conditions – Interference caused due to tall building, overhead bridges and time varying traffic conditions has a direct impact on the V2V link performance. (ii) Spectrum Resource Shortage – Under high density of media rich applications of AVs, the allocated spectrum for DSRC becomes insufficient. (iii) High Mobility – Communication between mobile (vehicles) and stationary (infrastructure) elements of the network topology has frequent interruptions due to high velocity of cars and a limited coverage by the wireless technology.

All the generated data from sensors and other devices require high network bandwidth. Fog computing leverages the local storage as well as cloud storage advantages. It provides data processing and local storage capabilities to fog devices instead of frequently sending the data to the cloud (Atlam, Walters, & Wills, 2018). This enables data to be placed closer to the source, leading to faster access than cloud computing.

Prominent AI Issues

The effective detection of road boundaries on real-time basis is another critical application for the AVs. In 2019, Sun *et al.* (Sun, Zhao, Xu, Wang, & Min, 2019) suggested a 3D LiDAR data-based algorithm to extract irregular road boundaries and obstructed roads. The algorithm consisted of four steps which had been tested on "Xinda" autonomous vehicle and its average accuracy exceeded 93% with processing time of approximately 36.5ms/frame. This sublime performance established that the unification of new age technology and a good algorithm is intrinsic to a safer road transportation. Nie et al. (Nie, et al., 2016) presented a framework for decision making performed by the CAVs which aimed to provide a decentralized cooperative lane-changing system. The approach constituted of three modules: to predict vehicle's future state, generate a candidate decision and avoid those lane-changing decisions which result in vehicle collision or traffic deterioration. However, besides other limitations, the model overlooked communication latency as well. The sole purpose behind the research on this topic was to assist the automated vehicle when it would be merged with conventional traffic.

J. Guanetti *et al.* (Guanetti, Kim, & Borrelli, 2018) presented a survey on control of CAVs and focused on various techniques that would improve energy efficiency. Y. Zhang *et al.* (Zhang & Cassandras, 2019) investigated the overall impact of CAVs in the domain of energy consumption in different traffic scenarios presented as a function of the CAV penetration rate. Results validated via MATLAB and VISSIM simulation indicated that increased rates of CAV penetration produced significant improvement in energy efficiency, meanwhile, with the increasing traffic, the significance is reduced. I. Papamichail *et al.* (Papamichail, et al., 2019) identified the novel problems in traffic management and presented a summarized discussion on problems in relation with management systems for motorway traffic. Their work aimed to improve the vehicle automation and communication systems even in case of dynamic traffic environment. This research field, in particular, is considered to be as critical as the technology analysis in AVs and therefore requires a separate study to cover its entirety.

Driverless cars powered through AI technology, undergo extensive training in virtual simulations, in order to prepare for majority of the road events that occur commonly. However, the vehicle may fail to identify these events and cause error. In January 2019, Massachusetts Institute of Technology (MIT) announced that a model was developed by MIT and Microsoft researchers, that identified instances which are divergent from actual occurrences in the real world, referred to as "blind spots" (Self-driving cars, robots: Identifying AI 'blind spots', 2019). P. Keller (Keller, 2018) examined the privacy and cybersecurity issues raised by AI in these smart vehicles. In view of the fact that autonomous vehicles are intended transmission and acquisition of data from the infrastructure as well as from other vehicles, U.S. Supreme Court asserted its reservations regarding the collection of sensitive information for example, information about an individual's religion or health issues. Thus, according to recent study by Forbes (Rethinking Privacy For The AI Era, 2019), concerns with regard to user privacy have escalated with the rise of AI. The study reports that 9 out of 10 American internet users emphasised on the confidentiality of their online personal data and 67% are in favour of disciplinary action for privacy laws. J. Janai *et al.* (Janai, Güney, Behl, & Geiger, 2017) presented a survey on datasets used, methods employed and problems faced by the computer vision implemented in AVs. Their work focused on the real-world dataset acquisition, camera calibration, 2D and 3D object detection, motion and pose estimation and tracking systems deployed in a full-fledge autonomous transport system.

In order to follow correct direction and avoid roads that are blocked or congested, AV use maps which are different from those obtained via GPS systems of the mobile phones. These maps are more detailed in terms of distance from pedestrians, dimensions of the lane and height of the curb. Their storage requires extensive memory and immense processing power. Many efforts are done to acquire such precise maps using 3D LiDAR and odometry sensor but the changing environment and road conditions is a hurdle for the industry. Big data aims to solve this issue. Its acquisition based on IoV data is generated thorough two ways: (i) on-board, and (ii) on-road. On board data is used for monitoring vehicular status. Subsequently, the events occurring on road, which can be derived from on-board or other IoT sensors, are considered as on-road data.

According to N. George and J. Thomas (George & Thomas, 2018), security is one of the major issues, however, little attention has been dedicated to this field attributable to the large size of the network, speed of the vehicles, relevance of their geographic location and the intermittent interconnection. The paper highlights AI technique used for message authentication based on the prediction of vehicular positioning with that tracked in beacon thus, securing the communication network. In addition to that, researchers aim to explore the potential of AI to improve penetration testing and vulnerability identification of systems (Richard, Dargahi, Dehghantanha, & Raymond Choo, 2019).

Some Prevalent Security Concerns in an AV (RQ3*)*

VANET are a pre-requisite for AVs, providing communication between moving vehicles thus, appropriate identity and authentication mechanisms are statutory for a safe and secure data exchange. Any threat to this communication technology, is also a hinderance towards the transformation process that has begun with the Industry 4.0. Sari *et al.* (Sari, Onursal, & Akkaya, 2015) categorised the security issues in VANET on the basis of three main groups: availability, authenticity, and confidentiality. According to Chadha and Reena (Chadha & Reena, 2015), the issues are broadly classified into five categories: Technical issue, Security issue, Security requirement issue, Attackers on VANET and Attacks in VANET. Fazal *et al.* (Fazal, Shehzad, Tasneem, Dawood, & Ahmed, 2017) classifies the security challenges in IoT based on three aspects: Devices/Hardware, Network and Cloud/Server-Side. The following subsections exposes the security concerns classified into two categories: unavailability of resources and attacks on confidentiality.

Unavailability of Resources

With the intension of implementing intelligent decisions by the vehicle, information exchange is conventional. Furthermore, it becomes implicit that the network used for vehicular communication is highly exposed to the environment thus, threating its availability. Distributed Denial of Service (DDoS) attacks are a group of collaborative attacks performed by attackers threatening internet security and violating services (Manavi, 2018). They can be carried out by both insider or an outsider with the aim of making the network unavailable to the authentic users. In this, the traffic overload is caused by flooding or overwhelming the targeted VANET components with artificial requests resulting in insufficient processing of the valid messages. McKee *et al.* (McKee, Clement, Almutairi, & Xu, 2018) discusses various concepts adopted to develop more resilient security techniques. One such approach is, performing computation on encrypted data using homomorphic encryption, but on account of its highly specific requirements, the application of this technique becomes a challenge in itself. Further, next concept discussed was that of quantum-key distribution which had a limitation of operating range of ~21 km however, improvement can be made by enhancing the detectors.

Alheeti *et al.* (Alheeti, Gruebler, & McDonald-Maier, 2016) presented an intelligent Intrusion Detection System (IDS) to defend the external communication system from attacks such as grey-hole and rushing attacks which target the transmission of V2I communication. The proposed scheme was based on anomaly detection in the features extracted from a trace file and used a Feed-Forward Neural Network (FFNN) and a Support Vector Machine (SVM). The results indicated that SVM performance with an error rate of 0.19%, was better than FFNN however, FFNN was observed to be more efficient in determining abnormality as compared to SVM based IDS.

Attacks on Confidentiality

VANET being an open network give rise the issue of malicious interception by an unauthorised user. The communication established must be secure enough to block out any intrusion which could tamper the original messages, publish fake data or illegitimately collect sensitive information through eavesdropping. This ensures that authentic messages are being relayed across the network and decision made on basis of the retrieved data is reliable. Ahmad *et al.* (Ahmad, Adnane, Franqueira, Kurugollu, & Liu, 2018) conducted a study in which they focused on Man-In-The-Middle (MITM) attacks and different strategies that attackers adopt to launch this attack. It was observed that the victim network experienced threat to confidentiality, high delays in data transmission and data leakage.

Pei *et al.* (Pei, et al., 2018) proposed two 3D positioning schemes to ensure privacy and security of the system. The presented work applied on vehicle-to-roadside (V2R) and vehicle-to-vehicle (V2V) communications guaranteed the vehicle privacy through an agreement protocol which leveraged one-pass authenticated key mechanism. This was found to be secured against backdoored pseudorandom generators. IoT entails open connectivity, therefore HTTP servers of IoT can be easily compromised by unauthorised access and injection of malicious codes into the parameters of HTTP requests. Yong *et al.* (Yong, Liu, Yu, Huang, & Zhou, 2019) presented a novel architecture for detecting malicious activity. Their work based on Hidden Markov Model (HMM), intended to defend against the parameter injection attacks by utilizing both benign and malicious Web traffic.

Yang *et al.* (Yang, Chou, Tseng, Tseng, & Liu, 2019) introduced a concept applicable to vehicular networks, to ensure correctness of traffic events based on Blockchain consensus mechanism and aimed to reduce the danger involved with misleading driving routes. Ratnasih *et al.* (Ratnasih, Perdana, Wulandari, & Pratama, 2018) examined the performance of the reactive routing protocol on VANET with wormhole attack scheme. Wormhole attacks intend to capture packets at one location and tunnels them to another location which may cause the packets to be dropped. They concluded that throughput values increased with the changing of initial power scenarios as 35, 40 and 45 dB followed by drastic decline in the delay values. Performance based on changing the node density was also observed and found to be fluctuating. Tolba (Tolba, 2018) proposed a Trust-based Distributed Authentication (TDA) method to avoid collision attacks using the Channel State (CS) routing protocol.

The experiment results were compared with Interaction Collision Warning System (ICWA) and Cooperative Message Authentication Protocol (CMAP) which concluded that the proposed model displayed an improvement of 16% and 17% in the communication rate and security respectively, relative to ICWS and CMAP individually.

DISCUSSION

The current technological scenario of CAVs is fast-growing and result oriented, hence the research on its new models and improved technologies, the challenges and the limitations observed in the existing solutions of the problems is continuously evolving and has become a frequently used topic by the research society. However, it was observed that besides the prominent issues, ethico-legal issues and welfare of the society was also a source of concern among the researchers. Product liability and the regulations that need to be imposed on these robotic vehicles must be discussed upon and formulated responsibly, for progressing towards the sustainable deployment of automated vehicles on public roads (Bellet, et al., 2019). Once the guidelines are established, standard set of technologies that would be applied universally and accepted by the industry will be easier to identify and protocols used will be defined officially.

The current and the forthcoming technology employed by the AVs is still not completely robust and secure, possessing safety issues in different areas that need to be addressed. S. Dixit *et al.* (Dixit, et al., 2018) presented a review of methods employed for planning and tracking of trajectory in autonomous overtaking systems. They concluded that existing autonomous overtaking solutions work well with precise knowledge of the surroundings However, this favourable scenario is not possible in real-world conditions. This inference is sufficient for the companies to keep testing the models of the smart vehicles first, in the controlled environment and second, in the real-world situations. This is a necessary step for all the disciplines and departments involved in the production of these vehicles.

Theoretical Contribution

IoT facilitates the AV with the major functionality of gathering data, which aids in bridging the gap of human-machine interaction and assisting the algorithms of machine learning, to take safer and predictive decisions equivalent to a human driver, in cases of real-world events. Correspondingly another termed was coined for IoT used by these self-driving cars, known as IoV. Furthermore, the interconnectivity of these automated systems employs another technology, VANET, which raises a new set of challenges and security issues pertaining to external and internal attacks. The unauthorised access of this technology has the potential to become a dangerous threat.

This situation brings the companies and the researchers together and perform rigorous in-depth testing of the product before its release into the market. The technology embedded into the smart vehicles incorporates both hardware and software components that require to be examined with the aim to pinpointing any limitation wherein the system showcases failure in its “learning” and is unable to generate response according to the events which are expected to occur.

Thus, stages for the operational testing are planned by the automobile manufacturers. Various models have been presented for policy implications which include liability and regulation issues for the robotic cars, beneficial for both the consumers as well as the manufacturing companies. Earlier studies proposed the idea of applying strict liability which implies car ownership liability, however undertaking the responsibility of the automated systems solely by the owner would refrain them from investing in these future technologies. The research studies showcase that accidents occur under the autonomous mode due to a fault in the algorithm or hardware component failure, which compelled the policy makers to introduce product liability. This model emphasised on identifying the situation under which the accident occurred and on the basis of this analysis, the rightful owner, manufacturer or government is held liable for the actions. This substantiates the increase in manufacturer liability while personal liability is expected to decrease. The safety and security of an AV is imperative for the enterprise and placed at the top priority by the stakeholders (Adnan, Nordin, Bahruddin, & Ali, 2018). With the iterative training and testing models adopted by automotive sector, lack of good software and sensors was identified as a major hindrance in delivery of an efficient and secure autonomous transportation.

To achieve uninterrupted communicative ability in parallel with faster processing of data, it is important to determine the suitable technology facilitating low latency in communication. DSRC has been dominant in this industry with the support of enabling direct V2V and V2I connection. However, 5G technology has gained momentum in the recent years, providing additional benefits higher speed and low power consumption. Furthermore, to keep improving network communication, Tactile Internet was introduced which provided reliable end-to-end communication, data security and data availability to authorised and authentic users along with low transfer latency. With the emergence of variety of technology for communication, the heterogeneity in communication network poses a threat for the smooth implementation of the interactive ability of the smart vehicle, which is one of its essential features. This mainly concentrates on the widely used DSRC and the cutting-edge technology of 5G-LTE, which has left the autonomous industry divided into two parts.

The data acquired by these smart and automated vehicles is collected in large volumes from multiple sources. Therefore, it is essential to maintain an effective data processing system which can lead to faster access to storage than cloud computing. This resulted in adoption of fog computing that allowed processing on local storage. The gathered information in the system may present compatibility issues and may have missing values. Thus, it is crucial to acquire correct and complete data and pre-process it thoroughly while employing robust data mining methods. This will generate reliable and consistent results for the decision-making mechanisms tested in the prototypes (Zhu, Ge, Song, & Gao, 2018). Variety of state-of-the-art sensors and technologies along with Big Data techniques are integrated for detailed acquisition of the information and its maintenance.

The training of self-driving cars is carried out in controlled environment, where all the events are pre-defined and produced in virtual simulations. It is important to focus on the real-time decision-making capabilities of the vehicle. Thus, research papers have been presented that propose different algorithms and approaches which help in physical world manoeuvring and predict vehicle's future state. To achieve maximum benefits of the currently available technological tools, AI is the driving force behind the driverless cars. However, the intelligence is highly vulnerable to the privacy and cybersecurity issues. Hence, it is imperative to focus on the AI implemented techniques and their limitations.

Another component of the AV is VANET, which is important for the provision of the communication between moving vehicles. This entails data exchange with external entities that are untrusted. Therefore, for safe and secure connection to transpire, CIA (Confidentiality, Integrity and Availability) is the underlying approach in most of the models proposed in various research studies. The security concerns in an AV can be categorised based on different aspects and by distinct solutions adopted. Unavailability of resources which involves DoS, DDoS attacks, rushing and grey-hole attacks, can be addressed by the usage of encryption techniques and IDS systems. Meanwhile, the attacks on confidentiality (for example, MITM attacks, eavesdropping, hacking, wormhole attacks) are blocked through establishing authentication mechanisms created with the help of different protocols and algorithms.

Implications for Practice

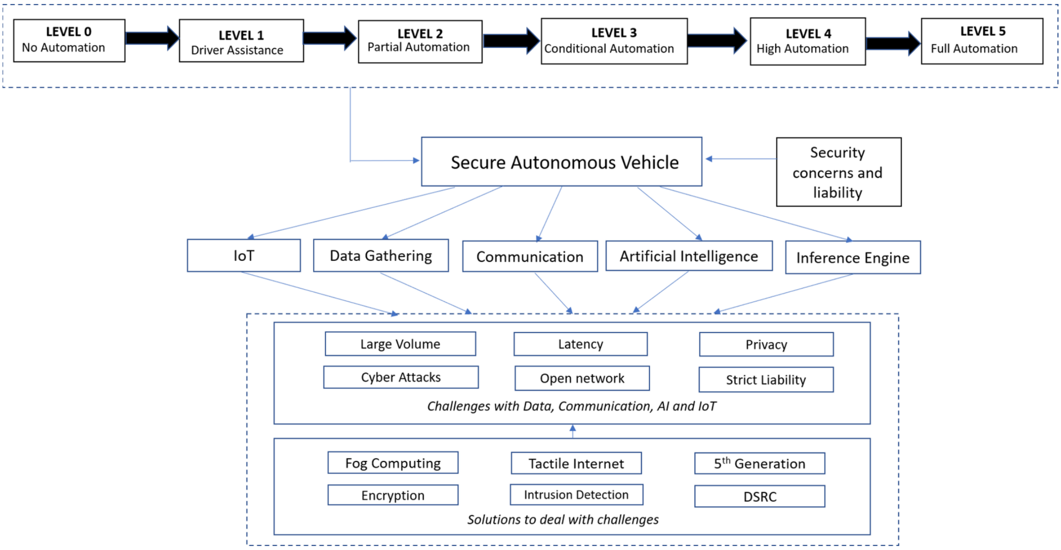
The continuing evolution of automotive technology has enabled the industry to achieve another innovation that has the potential to substantially affect safety, congestion, mobility for the disabled, energy use and land use - Automated Driving Systems (ADS). This autonomous vehicle technology is influenced by a number of factors such as: (i) the level of automation (ii) on-board devices, sensors (iii) data acquisition and its faster processing (iv) communication with vehicles and infrastructure (v) AI implementation, algorithms (vi) liabilities and regulations implied on AVs. This can be illustrated briefly in the technology diffusion model in Figure 8. From the selected papers, it can be inferred that the domain of security issues related to AVs is instrumental in the future of autonomous systems. However, some driverless cars can be seen in the real-world but, extensive effort is being put forth to prepare the product for the market and available to the consumers as a feasible commodity.

This presents a clear indication that researchers and manufacturers need to work in close association for the benefit of the organisation and the society. Contributions from both the sectors is essential for the development of a CAV as well as accelerating the process involved to do so. The information management model creation by the production companies would assist in improving the business processes involved and also aids in keeping track of the decisions made and operations performed in the past hence improving the likelihood of a profitable, safe and socially acceptable product. The study assumes the possibility of smart infrastructure to in existence and fully functional when the AV is brought to the real-world, hence this problem is still a major area of research for how to introduce the smart vehicles for the consumers in the cities without smart infrastructure or appropriate resources that facilitate the ADS. This topic needs a full-fledge investigation which would highlight the issue of smart infrastructure versus super cars with numerous complex and expensive sensors built in them and whether both are needed together or either one of them will suffice without another.

FUTURE RESEARCH AND CONCLUSION

The artificial intelligence in these cars is employed into various areas thus it possesses a great potential to influence the automation capabilities. Future researchers need to identify these areas and analyse the challenges that deeply impact the mass-production of driverless cars. Thus, the AI technology influencing the performance and decisions of these intelligent vehicles, that could aid in provision of a safer and cost-efficient transportation system, needs more attention. A secure and stable technology which makes smart decision at par with human intelligence is a support pillar for Industry 4.0. Another aspect is the integration of AV with conventional vehicular systems (human-driven vehicles) hence an exploratory study can be conducted which could be focused on the information management regarding the impact of vehicles on the traffic. Furthermore, this paper discusses the security concerns

Figure 8. To achieve a secure autonomous vehicle for its commercial use, a structured information model on the overview of the technology involved in the process is depicted



of the AV on broad view and presents the study with regard to the general issues that need concern when implementing the information management system. Therefore, another review paper can be formulated for IoV challenges that discusses the security threats and privacy issues in these CAVs along with in-depth analysis of each complication, its source, its target component and the current solution models proposed for it.

Technology for autonomous systems has veered the automotive industry to set forth in the Current Industrial Revolution (Industry 4.0), with the long-term hope for producing mass-market AVs. With all the progress and revolutionary efforts these companies have put in, it is estimated that Level 4 or Level 5 autonomy will be achieved by 2030 as per the prediction provided by survey reports. A study also reported that human errors are the cause of more than 90% of the accidents however the new generation AVs possess the capability to reduce such traffic collisions (Grieman, 2019). Therefore, with the proper addressal to liability issues concerning these autonomous systems and with sufficient training of the CAVs with regard to road safety, the automotive industry can proceed with the manufacturing of driverless cars for consumer use. The aim of this study is to provide an accumulated literature on the technological predicament faced by AVs with respect to IoT. This also preludes the solutions proposed in various research papers and new approach introduced to assist in overcoming the security threats. The current study encompasses data from 62 articles selected through extensive survey. Moreover, it paves the path for the researchers to understand the potential areas that need focus as well as further exploration in order to produce a better deliverable.

REFERENCES

Abu Talib, M., Abbas, S., Nasir, Q., & Mowakeh, M. (2018). Systematic literature review on Internet-of-Vehicles communication security. *International Journal of Distributed Sensor Networks*, *14*(12). Advance online publication. doi:10.1177/1550147718815054

Adnan, N., Nordin, S. M., Bahruddin, M. A., & Ali, M. (2018). How trust can drive forward the user acceptance to the technology? In-vehicle technology for autonomous vehicle. *Transportation Research Part A, Policy and Practice*, *118*, 819–836. doi:10.1016/j.tra.2018.10.019

Agarwal, N., Chauhan, S., Kar, A., & Goyal, S. (2017). Role of human behaviour attributes in mobile crowd sensing: A systematic literature review. *Digital Policy. Regulation & Governance*, *19*(2), 168–185. doi:10.1108/DPRG-05-2016-0023

Ahmad, F., Adnane, A., Franqueira, V., Kurugollu, F., & Liu, L. (2018). Man-in-the-middle attacks in vehicular ad-Hoc networks: Evaluating the impact of attackers' strategies. Sensors (Switzerland), 18(11).

Alheeti, K., Gruebler, A., & McDonald-Maier, K. (2016). Intelligent intrusion detection of grey hole and rushing attacks in self-driving vehicular networks. *Computers, 5*(3).

Ali, I., Hassan, A., & Li, F. (2019). 4 1). Authentication and privacy schemes for vehicular ad hoc networks (VANETs): A survey. *Vehicular Communications*, *16*, 45–61. doi:10.1016/j.vehcom.2019.02.002

Arena, F., & Pau, G. (2019). An overview of vehicular communications. *Future Internet, 11*(2).

Arif, M., Wang, G., Zakirul Alam Bhuiyan, M., Wang, T., & Chen, J. (2019). A survey on security attacks in VANETs: Communication, applications and challenges. *Vehicular Communications, 19*.

Atlam, H., Walters, R., & Wills, G. (2018). Fog Computing and the Internet of Things: A Review. *Big Data and Cognitive Computing, 2*(2).

Barua, S. (n.d.). *Flood of Data Will Get Generated in Autonomous Cars*. Retrieved from Auto Tech Review: https://autotechreview.com/features/flood-of-data-will-get-generated-in-autonomous-cars

Bellet, T., Cunneen, M., Mullins, M., Murphy, F., Pütz, F., Spickermann, F., Braendle, C., & Baumann, M. F. (2019). From semi to fully autonomous vehicles: New emerging risks and ethico-legal challenges for human-machine interactions. *Transportation Research Part F: Traffic Psychology and Behaviour*, *63*, 153–164. doi:10.1016/j.trf.2019.04.004

Bigelow, P. (2019). *A new connected-car battle: Cellular vs. DSRC*. Retrieved from Automotive News: https://www.autonews.com/mobility-report/new-connected-car-battle-cellular-vs-dsrc

Bin Sulaiman, R. (2018, 5 16). Artificial Intelligence Based Autonomous Car. SSRN *Electronic Journal*. 10.2139/ssrn.3167638

Butt, T. A., Iqbal, R., Shah, S., & Umar, T. (2018). Social Internet of Vehicles: Architecture and enabling technologies. *Computers & Electrical Engineering*, *69*, 68–84. doi:10.1016/j.compeleceng.2018.05.023

Chadha, D., & Reena. (2015). Vehicular Ad hoc Network (VANETs): A Review. *International Journal of Innovative Research in Computer and Communication Engineering*, *3*(3).

Chakraborty, A., & Kar, A. (2016). A Review of Bio Inspired Computing Methods and Potential Applications. *Lecture Notes in Electrical Engineering*, *396*, 155–161. doi:10.1007/978-81-322-3589-7_16

Chakraborty, A., & Kar, A. (2017). Swarm Intelligence: A Review of Algorithms. *Modeling and Optimization in Science and Technologies*, *10*, 475–494. doi:10.1007/978-3-319-50920-4_19

Chauhan, S., Agarwal, N., & Kar, A. (2016). Addressing Big Data Challenges in Smart Cities: A Systematic Literature Review. *Info*, *18*(4), 73–90. doi:10.1108/info-03-2016-0012

Detlor, B. (2010). Information management. *International Journal of Information Management*, *30*(2), 103–108. doi:10.1016/j.ijinfomgt.2009.12.001 PMID:20543892

Dixit, S., Fallah, S., Montanaro, U., Dianati, M., Stevens, A., Mccullough, F., & Mouzakitis, A. (2018). Trajectory planning and tracking for autonomous overtaking: State-of-the-art and future prospects. *Annual Reviews in Control*, *45*, 76–86. doi:10.1016/j.arcontrol.2018.02.001

Dwivedi, Y., Hughes, L., Ismagilova, E., Aarts, G., Coombs, C., Crick, T., Duan, Y., Dwivedi, R., Edwards, J., Eirug, A., Galanos, V., Ilavarasan, P. V., Janssen, M., Jones, P., Kar, A. K., Kizgin, H., Kronemann, B., Lal, B., Lucini, B., & Williams, M. et al. (2019). Artificial Intelligence (AI): Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. *International Journal of Information Management*, 101994. doi:10.1016/j.ijinfomgt.2019.08.002

Faisal, A., Yigitcanlar, T., Kamruzzaman, M., & Currie, G. (2019). Understanding autonomous vehicles: A systematic literature review on capability, impact, planning and policy. *Journal of Transport and Land Use*, *12*(1), 45–72. doi:10.5198/jtlu.2019.1405

Fazal, K., Shehzad, H., Tasneem, A., Dawood, A., & Ahmed, Z. (2017). A Systematic Literature Review on the Security Challenges of Internet of Things and their Classification. *International Journal of Technology and Research*.

Fitah, A., Badria, A., Moughit, M., & Sahel, A. (2018). Performance of DSRC and WIFI for intelligent transport systems in VANET. *Procedia Computer Science*, *127*, 360–368. doi:10.1016/j.procs.2018.01.133

George, N., & Thomas, J. (2018). Authenticating Communication of Autonomous Vehicles with Artificial Intelligence. In *IOP Conference Series: Materials Science and Engineering*. Institute of Physics Publishing. doi:10.1088/1757-899X/396/1/012017

Grieman, K. (2019). Hard Drive Crash An Examination of Liability for Self-Driving Vehicles. *JIPITEC*, 294.

Guanetti, J., Kim, Y., & Borrelli, F. (2018). Control of connected and automated vehicles: State of the art and future challenges. *Annual Reviews in Control*, *45*, 18–40. doi:10.1016/j.arcontrol.2018.04.011

Hussain, R., & Zeadally, S. (2019). Autonomous Cars: Research Results, Issues, and Future Challenges. *IEEE Communications Surveys and Tutorials*, *21*(2), 1275–1313. doi:10.1109/COMST.2018.2869360

Ionita, S. (2017). Autonomous vehicles: From paradigms to technology. *IOP Conference Series. Materials Science and Engineering*, 252.

Janai, J., Güney, F., Behl, A., & Geiger, A. (2017). Computer Vision for Autonomous Vehicles: Problems, Datasets and State-of-the-Art. *ISPRS Journal of Photogrammetry and Remote Sensing*.

Keller, P. (2018). Autonomous Vehicles. *Artificial Intelligence and Law*.

Krasniqi, X., & Hajrizi, E. (2016). Use of IoT Technology to Drive the Automotive Industry from Connected to Full Autonomous Vehicles. *IFAC-PapersOnLine*, *49*(29), 269–274. doi:10.1016/j.ifacol.2016.11.078

Lewis, P. (2018, September 14). *Point/Counterpoint: 5G or DSRC for Connected Vehicle Technology*. https://www.enotrans.org/article/point-counterpoint-5g-or-dsrc-for-connected-vehicle-technology/

Manavi, M. T. (2018). Defence mechanisms against Distributed Denial of Service attacks: A survey. *Computers & Electrical Engineering*, *72*, 26–38. doi:10.1016/j.compeleceng.2018.09.001

McKee, D., Clement, S., Almutairi, J., & Xu, J. (2018). Survey of advances and challenges in intelligent autonomy for distributed cyber-physical systems. *CAAI Transactions on Intelligence Technology*, *3*(2), 75–82. doi:10.1049/trit.2018.0010

Mijac, M., Androcec, D., & Picek, R. (2017). Smart City Services Driven by IoT: A Systematic Review. *Journal of Economic and Social Development*, *4*(2).

Mittal, M., Goyal, L., Hemanth, D., & Sethi, J. (2019). Clustering Approaches for High-Dimensional Databases: A Review. *WIREs Data Mining Knowl Discov*.

Mittal, M., & Pandey, S. (2019). The Rudiments of Energy Conservation and IoT. *Energy Conservation for IoT Devices*, 1-17.

Nie, J., Zhang, J., Ding, W., Wan, X., Chen, X., & Ran, B. (2016). Decentralized Cooperative Lane-Changing Decision-Making for Connected Autonomous Vehicles*. *IEEE Access: Practical Innovations, Open Solutions*, *4*, 9413–9420. doi:10.1109/ACCESS.2017.2649567

Papamichail, I., Bekiaris-Liberis, N., Delis, A. I., Manolis, D., Mountakis, K.-S., Nikolos, I. K., Roncoli, C., & Papageorgiou, M. (2019). Motorway traffic flow modelling, estimation and control with vehicle automation and communication systems. *Annual Reviews in Control*, *48*, 325–346. doi:10.1016/j.arcontrol.2019.09.002

Pei, Q., Kang, B., Zhang, L., Choo, K., Zhang, Y., & Sun, Y. (2018). 12 1). Secure and privacy-preserving 3D vehicle positioning schemes for vehicular ad hoc network. *EURASIP Journal on Wireless Communications and Networking*, *2018*(1), 271. doi:10.1186/s13638-018-1289-9

Qu, X., Xu, Z., Li, X., Zhao, X., Zhang, M. H., & Wang, Z. (2017). DSRC versus 4G-LTE for Connected Vehicle Applications: A Study on Field Experiments of Vehicular Communication Performance. *Journal of Advanced Transportation*.

Ratnasih, P. D., Wulandari, T., & Pratama, M. (2018). Performance Analysis of Reactive Routing Protocol on VANET with Wormhole Attack Schemeaper. *Jurnal Infotel, 10*(3), 138-143.

Rethinking Privacy For The AI Era. (2019). Retrieved from Forbes: https://www.forbes.com/sites/insights-intelai/2019/03/27/rethinking-privacy-for-the-ai-era/#30ed27017f0a

Richard, D. M., Dargahi, T., Dehghantanha, A., & Raymond Choo, K.-K. (2019). A systematic literature review and meta-analysis on artificial intelligence in penetration testing and vulnerability assessment. *Computers & Electrical Engineering*, *75*, 175–188. doi:10.1016/j.compeleceng.2019.02.022

Santos, V., Sappa, A. D., Oliveira, M., & de la Escalera, A. (2019). Editorial: Special issue on autonomous driving and driver assistance systems. *Robotics and Autonomous Systems*, *121*, 121. doi:10.1016/j.robot.2019.103266

Sari, A., Onursal, O., & Akkaya, M. (2015). Review of the Security Issues in Vehicular Ad Hoc Networks (VANET). *International Journal of Communications, Network and Systems Sciences*, *08*(13), 552–566. doi:10.4236/ijcns.2015.813050

Self-driving cars, robots: Identifying AI ‘blind spots’. (2019). Retrieved from Massachusetts Institute of Technology: https://www.sciencedaily.com/releases/2019/01/190125094230.htm

Sharma, V., You, I., & Guizani, N. (2019). *Security of 5G-V2X: Technologies, Standardization and Research Directions*. Academic Press.

Singh, R., Gahlot, A., Samkaria, R., & Mittal, M. (2019). IoT based Intelligent Robot for various Disasters Monitoring and Prevention with Visual Data Manipulating. *International Journal of Tomography and Simulation*, *32*(1), 89–99.

Skondras, E., Michalas, A., & Vergados, D. (2019). Mobility management on 5G Vehicular Cloud Computing systems. *Vehicular Communications*, *16*, 15–44. doi:10.1016/j.vehcom.2019.01.001

Sun, P., Zhao, X., Xu, Z., Wang, R., & Min, H. (2019). A 3D LiDAR Data-Based Dedicated Road Boundary Detection Algorithm for Autonomous Vehicles. *IEEE Access: Practical Innovations, Open Solutions*, *7*, 29623–29638. doi:10.1109/ACCESS.2019.2902170

Szigeti, S., Csiszár, C., & Földes, D. (2017). Information Management of Demand-responsive Mobility Service Based on Autonomous Vehicles. *Procedia Engineering*, *187*, 483–491. doi:10.1016/j.proeng.2017.04.404

Tanwar, S., Tyagi, S., Budhiraja, I., & Kumar, N. (2019). Tactile Internet for Autonomous Vehicles: Latency and Reliability Analysis. *IEEE Wireless Communications*, *26*(4), 66–72. doi:10.1109/MWC.2019.1800553

The Evolution of Automated Safety Technologies. (n.d.). Retrieved from NHTSA: https://www.nhtsa.gov/technology-innovation/automated-vehicles-safety

Tolba, A. (2018). Trust-Based Distributed Authentication Method for Collision Attack Avoidance in VANETs. *IEEE Access: Practical Innovations, Open Solutions*, *6*, 62747–62755. doi:10.1109/ACCESS.2018.2875906

Urooj, S., Feroz, I., & Ahmad, N. (2018). Systematic Literature Review on User Interfaces of Autonomous Cars: Liabilities and Responsibilities. *International Conference on Advancements in Computational Sciences (ICACS)*, 1-10. doi:10.1109/ICACS.2018.8333489

Wang, J., Zhou, L., Pan, Y., Lee, S., Song, Z., Han, B., & Saputra, V. (2016). Appearance-based Brake-Lights recognition using deep learning and vehicle detection. 2016 IEEE Intelligent Vehicles Symposium (IV), Gothenburg, 815-820. doi:10.1109/IVS.2016.7535481

Xu, W., Zhou, H., Cheng, N., Lyu, F., Shi, W., Chen, J., & Shen, X. (2018, 1 1). Internet of vehicles in big data era. *IEEE/CAA Journal of Automatica Sinica, 5*(1), 19-35.

Yang, Y., Chou, L., Tseng, C., Tseng, F., & Liu, C. (2019). Blockchain-Based Traffic Event Validation and Trust Verification for VANETs. *IEEE Access: Practical Innovations, Open Solutions*, *7*, 30868–30877. doi:10.1109/ACCESS.2019.2903202

Yilmaz, A., & Temeltas, H. (2019). Self-adaptive Monte Carlo method for indoor localization of smart AGVs using LIDAR data. *Robotics and Autonomous Systems*, *122*, 122. doi:10.1016/j.robot.2019.103285

Yong, B., Liu, X., Yu, Q., Huang, L., & Zhou, Q. (2019). Malicious Web traffic detection for Internet of Things environments. *Computers & Electrical Engineering*, *77*, 260–272. doi:10.1016/j.compeleceng.2019.06.008

Zhang, Y., & Cassandras, C. G. (2019). An impact study of integrating connected automated vehicles with conventional traffic. *Annual Reviews in Control*, *48*, 347–356. doi:10.1016/j.arcontrol.2019.04.009

Zhu, J., Ge, Z., Song, Z., & Gao, F. (2018). Review and big data perspectives on robust data mining approaches for industrial process modeling with outliers and missing data. *Annual Reviews in Control*, *46*, 107–133. doi:10.1016/j.arcontrol.2018.09.003

Adrija Ghansiyal is a Computer Science and Engineering graduate from G. B. Pant Govt. Engineering College, Okhla, New Delhi. She has completed her internships in LASTEC lab, DRDO (Defence Research and Development Organisation) on security systems based employed in laser fence and also in Ramco Systems Ltd. working on ERP (Enterprise resource planning) modules. She has also worked on a project, "Drowsiness detection system using heart-rate variability" and has project in the Deep Learning technology.

Mamta Mittal (PhD) graduated in Computer Engineering from Kurukshetra University Kurukshetra in 2001 and received Masters' degree (Honors) in Computer Engineering from YMCA, Faridabad. Her Ph.D. is from Thapar University, Patiala in Computer Engineering and has a rich experience of more than 16 years. Presently, working at G.B. PANT Government Engineering College, Okhla, New Delhi (under Government of NCT Delhi) and supervising Ph.D. candidates of GGSIPU, New Delhi. She is working on DST approved Project "Development of IoT based hybrid navigation module for mid-sized autonomous vehicles". She has published many SCI/SCIE/Scopus indexed papers and Book Editor of renowned publishers.

Arpan Kar (PhD) is Associate Professor in the Information Systems area at DMS, IIT Delhi, India. His research interests are in the domain of data science and AI/ML applications, digital transformation, internet ecosystems, social media, blockchain and ICT-based public policy. He has authored over 120 articles in Elsevier, IEEE, Springer, ACM, Taylor & Francis, and Emerald and edited/authored 6 research books. His research has been cited over 1600 times. He is on the Editorial Board / Associate / Coordinating / Editor of reputed journals like Int. J. of Information Management, Information Systems Frontiers, Global J. of Flexible Systems Management and Int. J. of Elec. Government Research. Previously, he has worked for IIM Rohtak, IBM Research, and Cognizant Consulting. He has also generated over 15 Crores rupees through research, advocacy and training projects from national and international MNCs and governments. Over the years, he has received numerous awards and recognitions for his contributions in research from several organizations including the Association of Indian Management Schools, International Federation for Information Processing, Elsevier, Tata Consultancy Services, Project Management Institute, IIT Delhi and IIM Rohtak.