Cloud and IoT-based Emerging Services Systems

Sugam Sharma[1*], **Victor Chang**[2], **U Sunday Tim**[3], **Johnny Wong**[4], **Shashi Gadia**[4]

1. Center for Survey Statistics and Methodology, Iowa State University, Ames, Iowa, USA
2. International Business School Suzhou, Xi'an Jiaotong-Liverpool University, China
3. Department of Agricultural and Biosystems Engineering, Iowa State University, Ames, Iowa, USA
4. Department of Computer Science, Iowa State University, Ames, Iowa, USA

Email: sugam.k.sharma@gmail.com

Abstract. The emerging services and analytics advocate the service delivery in a polymorphic view that successfully serves a variety of audience. The amalgamation of numerous modern technologies such as cloud computing, Internet of Things (IoT) and Big Data is the potential support behind the emerging services Systems. Today, IoT, also dubbed as ubiquitous sensing is taking the center stage over the traditional paradigm. The evolution of IoT necessitates the expansion of cloud horizon to deal with emerging challenges. In this paper, we study the cloud-based emerging services, useful in IoT paradigm, that support the effective data analytics. Also, we conceive a new classification called CNNC {**C**louda, **NNC**louda} for cloud data models; further, some important case studies are also discussed to further strengthen the classification. An emerging service, data analytics in autonomous vehicles, is then described in details. Challenges and recommendations related to privacy, secuity and ethical concerns have been discussed.

Keywords. Emerging services, as-a-Service, analytics, cloud computing, IoT, Big Data, CNNC

1. Introduction

Emerging services and analytics promisingly hide the complex details of the comprehensive data processing from the end users and deliver a suave and plain results. The resulted outcomes are easily interpretable even by the technically naïve stakeholders (Chang, 2015; Chang et al., 2015), managers, and even a common user. The success of emerging services and analytics is largely depending upon the blending of various modern technologies and cloud computing, and IoT (Internet of Things) are just to name a few and are the core ingredients. The information age is shifting from traditional human-intervened Internet to Internet of Things (IoT) (Figure 1(a)), where the sensor embedded commodity, also called things, communicate among themselves (Chen, 2012) on the existing network resources and help facilitate the information collection and analytics with a very high degree of automation. The pool of IoT-enabled devices is growing rapidly and IoT footprint in increasing almost all in domains that includes trivial to complex applications such as smart grid (Monnier, 2013) to advanced smart cities (Zanella et al., 2014). The IoT "Things" include a diverse range of embedded objects or devices such heart monitoring implants, sensor equipped automobiles, thermostat systems and so on (Hwang et al., 2013). The increasing IoT maturity and the advancing cloud-based services are revolutionizing the information generation, collection, management and analytics. In IoT realm, the devices collect useful data and then share the data between other devices (Farooq et al., 2015); there are 9 billion such devices that exist today and the number is inflating. Evans (2011) believes this number will reach nearly 50 billion by year 2020 (Figure 1(b)), which substantiates the fact that the permeation of IoT is expanding in human life. This indicates that the number of new applications under IoT umbrella is increasing and consequently a massive amount of data is being generated at swift rate, called Big Data (Villars et al., 2011), where the social media and sensor embedded systems play central role in data inundation. As, the IoT-enabled devices access and process the data from several peer devices to constitute immediate decisions and swift actions, there is a continuous need for equally strong data model, equipped with robust data engineering and comprehensive analytical capabilities as the traditional data models are becoming inadequate in meeting the growing challenges that information-rich IoT evolution possess.

To appropriately accommodate and adequately address the growing IoT data challenges, the concept of cloud computing framework has emerged as a globally acceptable solution for secure and efficient data engineering and functionally-rich analytics for technically naïve stakeholders, director, managers to tech-savvy users. The backbone of the widely successful cloud adaptation is the secure and robust existing or evolving services that are delivered in the form of **-as-a-Service* and the state of the art as-a-Service cloud modality has gone beyond the core Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), Software-as-a-Service (SaaS), and Database-as-a-Service (DBaaS) (Curino, et al., 2011; Seibold and Kemper, 2012) and this paper highlights some of them that are highly relevant in IoT context.

Today, a trend of migration, from on-premises to cloud environment, of applications from almost all possible areas is increasingly being observed to utilize the best offered services at substantially reduced cost of cloud computing; the progressive maturity of IoT is accelerating this migration. The need for the efficient and successful management and computation of the scalable Big Data motivates the scientific communities to devise and develop the new scalable systems. Consequently, the appeal introduces and inducts a high abundance of cloud and non-cloud data models; it becomes nearly impractical for a user to thoroughly access such a large set of data models to understand individual's technology in search for the most suitable cloud model. In this work, we harness the scientific name of the data models and introduce a novel CNNC {**C**loud**a**, **NNC**loud**a** | a- assisted, NN- No Name} classification. The CNNC classification is based upon the intuitiveness of the scientific name of the cloud data model and considers two types of cloud data models -1) the model contains the term "cloud" in their name (Clouda), and 2) the model doesn't have the word "cloud" in its name at all (NNClouda). In addition, some interesting case studies are also explored to further strengthening the core of CNNC classification amid the broadening spectrum of emerging services and analytics in IoT age.

Rest of the paper is structured as follows. Section 2 provides a brief overview of the emerging Services and analytics. This section expands on the concept of cloud computing and IoT. Also, explored are some of the emerging analytics techniques. Section 3 elaborates on the novel CNNC classification and investigates some key data models of Clouda and NNClouda type to further understand and validate the proposed classification. Section 4 discusses an interesting case study, focusing on data analytics in vehicular automation with various examples illustrated. Section 5 highlights on emerging cloud services with extended discussions on emerging services and analytics. Section 6 explains the impacts and benefits of this work to businesses. Section 7 presents the ethical issues on data analytics in vehicular automation. Finally, the paper is concluded in section 8.

2. Emerging Services and Analytics: Brief Overview

This section provides the brief overview of some core components of emerging services and analytics. The discussion on the emerging cloud services is elaborated a bit comparatively.

2.1 IoT

IoT is a network constituted by uniquely identifiable commodity objects or devices equipped with some sensing system (Ashton, 2009). IoT paradigm promotes a seamless amalgamation between the smart devices, scatter around us, and the physical world to ensure full automation that eventually ameliorates human life. Some of the examples of IoT-enabled commodity devices or things include heart monitoring implants, automobiles with embedded sensors, firefighter' devices, smart thermostat systems, and Wi-Fi enabled washer/dryers (Sundmaeker, 2010). As the arena of IoT is expanding, the number of IoT-enabled applications is also rapidly growing, which results in massive growth of smart devices in multiple order comparatively (Figure 1(b)). This swift increase in the number of sensing things is responsible for generating and storage of a plethora amount of Big Data at much faster rate. The data needs to be engineered and analyzed, which require robust services and analytical systems as the traditional techniques unable to successfully and efficiently accost such data stress.

2.2 Big Data

IoT paradigm is increasingly encouraging the ubiquitous connectivity of the intelligent objects within internal or external world. The continuous rapid growth of large number of IoT-enabled objects and storage technology have resulted into the massive amount of heterogeneous digital footprints and sizeable traces. A vast amount of data (IBM, 2012) is being generated by various sensing sources every day. The actual pattern and nature of such data is indistinct, but is certainly large, complex, heterogonous, structure and unstructured (O'Leary, 2013). Palermo (2014) demonstrates some important attributes of Big Data such as volume, variety, and velocity and some core constituents of IoT like sensor-embedded devices, intelligence for quick decision making, and connectivity for data sharing. Also, the rapid growth of sensing devices under IoT purview is generating such a large scale complex and heterogeneous data that the available computing capacity of the existing systems (Figure 2) unable to successfully match up the data challenges and today, this has emerged as one of the core issues for the data science community (Manyika et al., 2011; Hilbert and López, 2011). The storage capacity and also the processing power of the existing data computing systems are failed in handling the stress of Big Data.

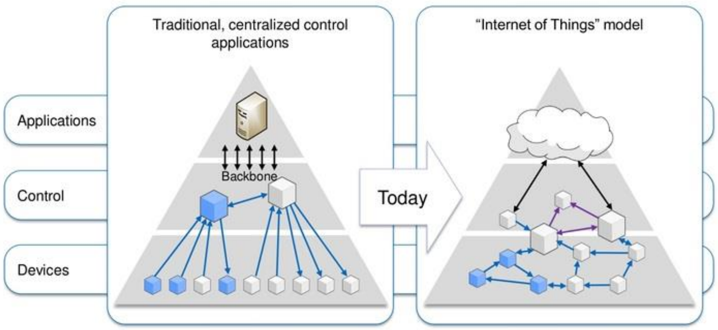

Figure 1(a). Traditional vs. IoT paradigm
(Source: db.in.tum.de/teaching/ws1314/industrialIoT/)

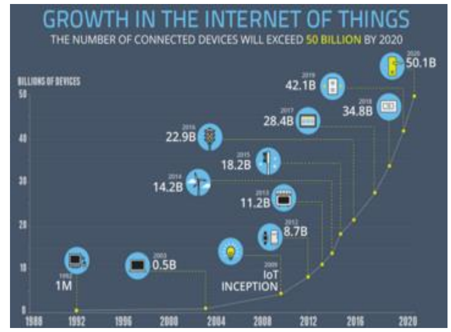

Figure 1(b). IoT growth over years
(Source: www.ncta.com/broadband-by-the-numbers/)

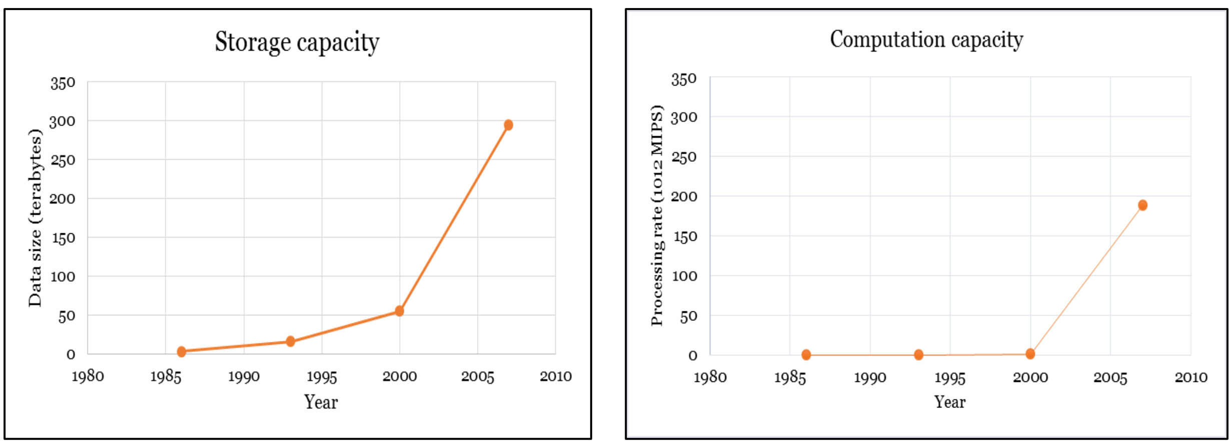

Figure 2. Storage vs. Computation capacity (Source: Hilbert et al., 2011)

As IoT and its applications are majorly impacting the human life, the scientific communities contemplate a broader outreach from the processing and sharing of Big Data across the variety of the several commodity devices around us. Consequently, the development of new capable services and analytics is encouraged to cater the current data processing and presentation need. The exploratory analysis of the various aspects of Big Data in cloud can help in understaing its important characterstics (Nugent et al., 2013) that may be very valueable to stakeholders and managers. Sharma et al. (2014, 2015a, 2015b) provide the elaborated discusisons on the characteristics and complexities of Big Data.

2.3 Based Cloud services

Based Cloud services (BCS) combine all different Cloud computing services altogether to produce greater impacts to the users an any services in place. BCS may include infrastructure as a service (IaaS), platform as a service (PaaS), software as a service (SaaS) and database as a service (DBaaS) (Sugam, 2016). IaaS provide the infrastructure for users to gain access to use Cloud services, store and save data, transfer and backup data between their computers and Clouds. PaaS offers the platform for the developers, users and service providers to access their services, data and requests better. SaaS allows users to use any Cloud services without using any programming but only interfaces to get their requests completed. Analytics can be used to get services requests completed in a few clicks. Apps on the smart phone can allow users to connect and request services, check status and make payment. All the data and information processed and stored in all these services will be handed by DBaaS, which can be either managed by the service providers or users depending on the requirements, chosen service packages and the purpose of doing DBaaS. The service often includes replication, mirroring, disaster recovery, backup and data retrieval. Figure 3 shows the architecture of the Cloud/IoT services, which connects to all of IaaS, PaaS, SaaS and DBaaS. Users do not need to know the complexity and can seamlessly use the services to get their requests completed.

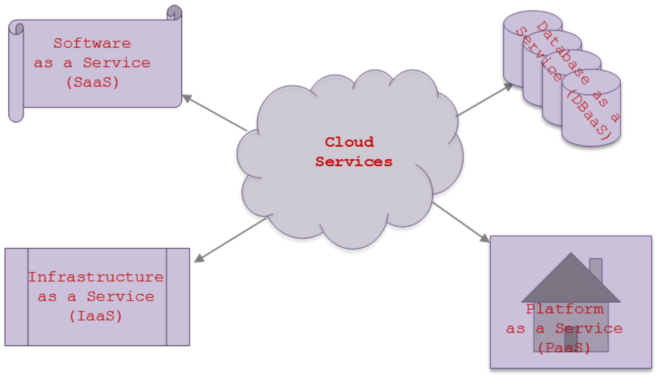

Figure 3. Base cloud services

2.4 Integrated cloud computing and IoT ecosystem

The growing smart communication among the things, especially the sensor equipped, under the purview of IoT is resulting into production of incredibly large amount of Big Data. Supported by the context-aware computing, Big Data is sufficient enough to address the nontrivial and comprehensive tasks with great degree of automation regardless the disciplines - financial, health, automobile, etc. Soon, the concept of IoT is going to deeply pervade through the human life intending to automate the routine chores. The ubiquitous sensing of all the devices around us emits enormous quantity of Big Data that needs to be stored, computed and visualized and analyzed in efficient manner. Today, cloud computing is the most recommended solution for above mentioned issues of Big Data that promises to deliver the efficient services as traditional commodities. The emerging cloud services are being appreciated for supporting the analyses of Big Data for naïve to elite experts such as stakeholder, mangers and data scientists for their routine tasks. The needs for the highly robust computing and analytical services to address and analyze the data-related challenges with the exceedingly reduced cost have further brought the service-rich cloud computing to forefront. The rising interest in IoT and cloud provisioning system has triggered the surge in cloud-housed comprehensive analytics. In this paper also, we have illustrated some important related cloud-based analytic services that are highly efficient for the dedicated tasks and data intensive applications, they have been developed for; gene structure prediction, image processing, predicting the relationship of customers and their purchasing patterns and web searches are some good examples of such data-rich applications and for the required appropriate analytical services to analyze their highly complex and heterogeneous data cloud is the pertinent choice from the security, efficiency and affordability aspects. Academia, industry and research communities are rapidly developing robust analytic frameworks and housing them in cloud environment, and are delivered and utilized as analytics-as-a-Service. In 2008, to deal with the collaborative complex computations, instead of data in the cloud, Cerri et al. (2008) devised an analytical framework in cloud, called knowledge in the cloud that delivered multifarious knowledge. Figure 4 shows the cloud computing and IoT ecosystem. It can be noticed that a sensing system, may differ in attributes, is embedded into the objects /devices around us. The device communication with cloud is facilitated through the robust cloud services. However, in IoT infrastructure a smart connectivity gateway, may be with the existing networks, is required to further strengthen the device communication.

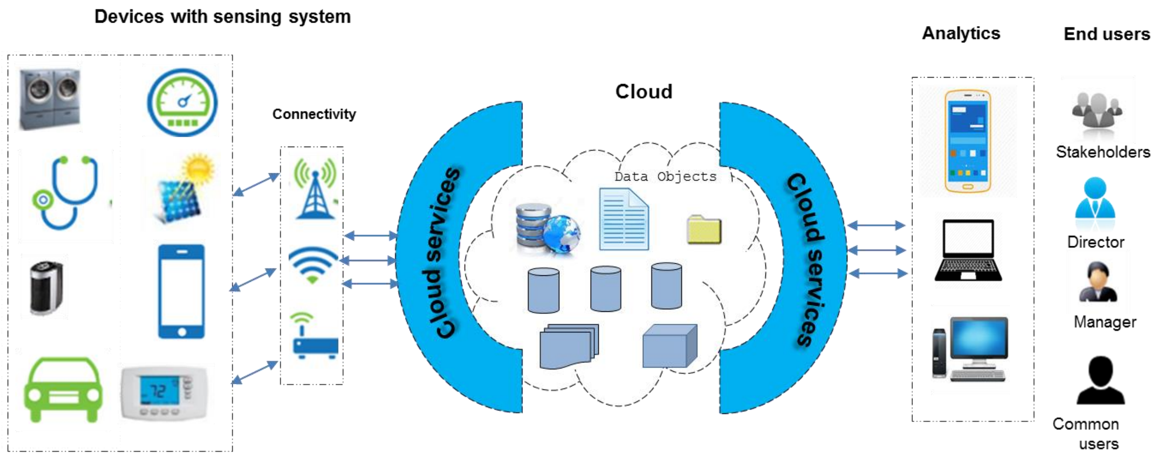

Figure 4. Cloud computing and IoT ecosystem

The devices proactively generate the heterogeneous Big Data, which is housed in the cloud in various formats and is available for analysis through robust cloud services. Therefore, the communication between the cloud and the external word is feasible only through robust and reliable cloud services.

2.5. Machine learning and predictive analytics

Machine learning and its supported predictive analytics provide the intelligent and efficient processing of data and, the wide usage of these analytical technologies has brought them to fore in data science, especially for the new incarnation of data into Big Data. The machine learning algorithms help recognize the subtle association of the variables in the dataset, and satisfying all the input criterions, the analytical systems quickly deliver the output, presented in the desired form that is easily interpretable by the end users or stakeholders (Chen and Zhang, 2014). The predictive analytics are highly sought in business domain in the view to elevate the product sale. These techniques are useful in predicting the items types, a customer may be interested to buy and the associated approximate spending (Kumar, 2008). As the customer behaviors is closely predictable using the predictive modeling and this enhances the expansion of the business opportunities and also the customer may be recommended and served with special offers and discounts.

2.6. Agile methodology

The stakeholders always desire to have the even the comprehensive software products ready in a shorter time. Also, the functional or visual requirements related to that specific product from the stakeholders change several times over the span of that product development. To accommodate all such limitations, restrictions, and complexity and to promisingly deliver the robust software systems in smaller time span, standard agile development is highly efficient (Zhang, Cheng, and Boutaba, 2010).

2.7. Statistical analytics

The evolution of data science in the form of Big Data has brought the statistical analytics to forefront regardless the domain. The stakeholders are applying the statistical approaches on their customer databases to derive useful and accurate recommendations to improve their business. Also, some statistical frameworks such as R programing have gained unexpected popularity due to its rich set of statistical libraries; which are capable to produce the quick results and their ability for swift, effective and on-the-spot variation in presentation as desired by the end users or stakeholders. Also, regression testing is one of the highly sought mechanism in statistical analysis along with the easily interpretable presentation of the crucial outcomes (Antcheva et al., 2009; Miner et al., 2009).

2.8. Visual analytics

With the recent advancements of data science, where data has taken a more complex shape in the form of Big Data, visual analytics have become extremely relevant to deliver the elegant and informative presentations of the highly complex data processed for the end users. Visual analytics also come equipped with some sophisticated statistical models to be used by the end users or stakeholders (Antcheva et al., 2009; LaValleet al., 2013) to obtain the desired interpretation. In business domain, the visual analytics are extremely used to envisage the market and business trends and customer shopping behavior in order to improve the future decision making to elevate the business.

3 CNNC Classification for Emerging Services Models

With the growing projection of IoT smart, embedded, and sensing devices (Evans, 2011), the number of available cloud-powered models for Big Data management is increasing; every month, the inclusion of several new models is being obviously observed and claim to deliver the effective solutions when deal with Big Data. As the number of the cloud providers is rising, it becomes nearly impossible for a cloud-interested user to surf through that giant pool of models to comprehend their technology and suitability for his/her purpose, especially from cloud aspect of IoT. In this case, it is very likely that a user fails to hit the most pertinent model due to several reasons such as gradually eroded user patience, restricted time availability, etc.

In such scenario, to assists the user, we focus on the name of the cloud models and propose a novel first-level classification, called CNNC. The objective of this classification is to gauge the intuitiveness of the name of the cloud models.

The CNNC classification is believed to reduce the search time and consequent pain of the user to a greater degree. Only the cloud-powered data models are eligible for this classification. The scientific names of the cloud-assisted models are considered as the basis for classification, and are divided into two categories -- **C**louda and **NNC**louda.

CNNC = {**C**loud**a**, **NNC**loud**a**}, where NN- **N**o **N**ame, a- **a**ssisted

We further mature and test the proposed CNNC classification, by applying and explaining it with some prominent cloud-powered IoT- Big Data models. We believe, the discussion of this classification will invigorate the communities for more intuitive naming convention, where only the scientific name of a model itself is merely sufficient to gesticulate about underlying cloud technologies.

Section 3.1 and 3.2 should be about integration of Cloud and IoT. It can literature review, or our proposed architecture, or both.

The old Section 4 was removed. The new Section 4 – it can be paraphrased but later.

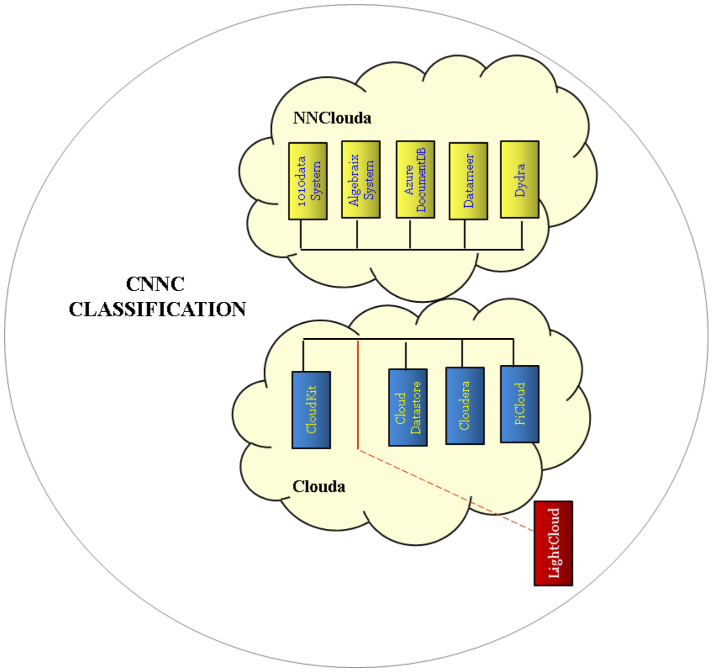

Figure 5. CNNC classification for emerging service models

4 Emerging as-a-Service and Analytics Models

IoT can be understood as a pervasive system that may have more than one mesh of embedded sensing devices. In coming years, the IoT paradigm is expected to encompass the scalable networks of billions of uniquely identified devices, also called things. The devices are highly capable for sensing, computing, communicating, uniquely identifying the other peer devices for communication and effuse humongous data streams; therefore, the IoT paradigm triggers the emission of amassed data, where swift inclusion of cloud-based services and analytics becomes indispensable in order to harness the full potential of the data and discover valuable knowledge, insight, and complex relationships between variables of the data. The functionally-rich cloud-based services and analytics help shifting the data engineering and computation burden from the end entity to the cloud environment and hide that complex details from the end users. This greatly eases the analysis process, especially for technically naive stakeholder, director, managers, or even for common users. Therefore, in recent years, the communities have focused on the development of the cloud-supported services and analytics to deliver the customizable outputs that suffice the needs of various types of users. In this section, we briefly illustrate some of the cloud-based emerging services and analytics, which may be highly useful in growing IoT paradigm.

1) **Business Integration-as-a-Service (BIaaS/BIaS)** enables the connections between numerous cloud-powered services and combines various other services and business activities to achieve a streamline process (Chang et al., 2012; Chang, 2013).

2) **Business Intelligence-as-a-Service (SaaS BI/BIaaS)** is an emerging cloud-supported service and analytics that efficiently facilitates the business intelligence exercise and provides the data retrieval through a web resource. SaaS BI/BIaaS is highly useful to stakeholders, managers, and tech-naïve common user and it completely hides the implementation details and presents the simple abstraction, thus elevate performance, to them (Sano, 2014; Chang, 2014).

3) **Business Framework-as-a-Service (BFaaS)** is a cloud assisted solution for business organizations to embrace the cloud-based services and practices. BFaaS is capable for providing the right strategies and business cases, accurately reviewing business performance in cloud, resolving the desktop to cloud migration issues and among heterogeneous clouds from several distinct providers, and smoothly synchronizing between

IaaS, PaaS, SaaS and business entities and between cloud-related disparate research methodologies (Chang et al., 2013).

4) **Cloud-Based Analytics-as-a-Service (CLAaaS)** delivers a data analytics, housed in the cloud as service to users. CLAaaS also facilitates on demand data storage and multifarious analytics using the customizable user interfaces. Also, for different user group, the interfaces can be customized differently or uniquely for query, decision management, and workflow design and service execution (Zulkernine et al., 2013).

5) **Data-as-a-Service (DaaS)** is a cloud-based relatively new service that on demand delivers the data to consumers using the existing or new APIs. The use of DaaS helps avoid the typical need of - 1) storage and retrieval of behemoth data assets, and 2) exhaustive searching in that colossus data assets in order to derive the useful knowledge and statistics (Vu et al., 2012).

6) **Data Integrity-as-a-Service (DIaaS)** gauges the criticality of some data-oriented well-known issues; and therefore, to address them appropriately, it combines all the expertise essential for data integrity. Public verifiability and dynamic content are few such examples where DIaaS is highly useful. DIaaS shreds off the burdens of managing data integrity from a storage service as it manages the data integrity using a third party independent data integrity management service (IMS). Also, the inclusion of IMS helps reduce the security risk of the data stored in the storage services as now IMS checks the data integrity (Nepal et al., 2011).

7) **Data Mining-as-a-Service (DMAS/DMaaS)** offers the data owners to utilize the hardware and software solutions dispensed by DMAS/DMaaS providers and discourages them for the development of their own. DMAS/DMaaS is specially effective and useful for those consumers who govern mountainous amount of the data, but short in budget, allocated for data analysis. For such consumers, to outsource their data and data mining operations to a third-party service provider that always raises some security and monetarily concerns, but DMAS/DMaaS avoids the needs of any third-party service provider (Liu et al., 2012).

8) **Database-as-a-Service (DBaaS/DaaS)** is one of the most sought cloud-based emerging services in recent times to address the swiftly grown market needs due to the data inundation from IoT and other outlets. DBaaS/DaaS is highly effective in shifting much of the operational efforts such as provisioning, scaling, performance tuning, backup, and privacy to service providers in cloud from the localized database owners, administrations or users. Thereby, it guarantees lowering the overall expenditure as compared to the on-premises operational cost. Amazon RDS and Microsoft SQL Azure are the early providers of DBaaS (Curino, 2011).

9) **Ethernet-as-a-Service (EaaS)** is a cloud service that has high-bandwidth and fiber optic. It uses a two-way broadband shared infrastructure to successfully provide ubiquitous connectivity to remotely located devices (Zaslavsky et al., 2013).

10) **Failure-as-a-Service (FaaS)** is a cloud-based service that is useful in performing the routine large-scale failure drills in real deployments. FaaS is capable to regularly conduct the large-scale failures online. Thereby, it may further strengthen the ability to anticipate, mitigate, respond, or recover from failures at individual or organizational level (Gunawi et al., 2011).

11) **Forensics-as-a-Service (FRaaS)** provides a comprehensive cloud-powered forensics solution to develop a repeatable system. The system could be developed as a standard forensics operational model for the deployment in cloud irrespective of the client service lines or environments (Shende et al., 2012).

12) **Identity and Policy Management-as-a-Service (IPMaaS)** a cloud-supported service, dedicated for the policy management. It is conceived to deliver a unified control point the users, where they are capable to manage and access the policies and to control the access to their resources regardless the stored location of these assets (Takabi et al., 2012).

13) **Mobility-as-a-Service (MobiaaS)** is a cloud-enabled service that is highly useful in providing the required connectivity service continuity to the consumers. It also capable to deliver seamless handover for flows like voice as the consumers use a multitude of devices to communicate (Baliga et al., 2011).

14) **Object-as-a-Service (ObaaS)** is based upon the idea to dynamically build the service on each object as demanded and subsequently integrate that into the whole composition. ObaaS executes on the objects and exploits its sensing, actuating, and computing capabilities (Cherrier et al., 2014).

15) **Security-as-a-Service (SecuaaS/SaaS)** provides the cloud-based solution for data, host and application protection. SecuaaS/SaaS is capable to validate and ensure the security aspect over a geographically sparse scalable, multicloud and cloud federation infrastructure (Pawar et al., 2015).

16) **Sensing-as-a-Service (S2aaS)** is a cloud-powered sensing service that is offered through mobile phones. S2aaS has enormous scope to serve under IoT paradigm and also highly useful in environmental monitoring, social networking, healthcare, transportation and several other domains, where sensing is an important part. S2aaS is highly energy-efficient service and supports several sensing applications through various smartphone platforms (Sheng et al., 2013).

17) **Sensor-as-a-Service (SenaaS)** is a cloud-powered service that is delivered for ubiquitous management of the remote sensors. However, SenaaS has no role in any type of data collection or data dissemination mechanism for the sensor data (Zaslavsky et al., 2013). SenaaS is another qualified candidate that also has huge opportunities to serve in IoT paradigm.

18) **Sensing and Actuation-as-a-Service (SAaaS)** is to develop a cloud of sensors and actuators and deliver it as a service for sensing and actuation process. The inclusion of sensors and actuators initiates the creation of new, value added, quality services that eventually leads to pervasive cloud computing (Distefano et al., August 2012). Similar to SenaaS, SAaaS also has wide utility in IoT paradigm.

19) **Sensor Event-as-a-Service (SEaaS)** is a cloud-supported service for message and alert notification. The service is enabled and triggered at the sensor events. It also grants access privileges to the users on sensor data and measurements. SEaaS imparts capabilities for generation, subscription, and retrieval of the message and alert notifications. SEaaS allows users the dynamic registration of the sensors, which is followed by subsequent service notifications (Dash et al., 2010; Rao et al., 2012). Also, the role of SEaaS in IoT paradigm is expectedly highly promising.

20) **Storage-as-a-Service (StaaS/SaaS)** is a cloud-based service to store the data in online storage space in cloud. StaaS/SaaS has robust cryptographic algorithms to address the user concerns about the data security and privacy. StaaS/SaaS also claims the lower computation cost, higher security and sensitivity based on data significance (Patel et al., 2012).

21) **Things-as-a-Service (ThiaaS)** allows the implementation of innovative and the value-added services in a cloud environment that is integrated with IoT paradigm. ThiaaS provides the mechanism to construct a cloud of things, where the multifarious resources are either aggregated or abstracted (Distefano et al., July 2012). Therefore, ThiaaS obviously is one of the most qualified and useful services in IoT evolution.

22) **Video Surveillance-as-a-Service (VSaaS)** is a cloud-enabled service for video surveillance and facilitates video recording, storage, remote viewing, and cyber threat and security management. For the on-premises installed surveillance devices, the VSaaS shifts the video processing, management and analysis in cloud environment unlike the conventional systems, where the computations are locally performed by the computing unit attached to the device itself (Prati et al., 2013), which add significant overheads that may dampen the performance.

4. An Emerging Service: Data analytics in autonomous vehicles

This section describes data analytics in autonomous vehicles as part of the emerging service. The in-depth case study also contributes to the theoretical contribution for our paper, as well as the privacy and ethical issues discussed in Section 7.

4.1 Current research on data analytics in autonomous vehicles

The history of autonomous vehicles using data analytics can be traced back to the 1980s when predicted that vehicles can control their own movements in the future (Mark *et al.*, 2010). According to the degree of self-controlled, the autonomous vehicles can be divided into five levels, see Fig. 6. Vehicles in level 1 (driver needs to have complete manual control of the vehicle while driving) and level 2 (driver needs to continuously monitor the operation of the vehicle and check the driving environment) are being mass production. In additional, some manufacturers have produced a level five test vehicles (vehicles can be completely autonomous under any circumstances while driving long distances) by using the technology of big data analytics (Hawes, 2015). Big data analytics collect data via autonomous vehicle sensor in real time and analyze big data with IoV. The most difference between data analytics and other analysis is that it effectively use and classify the massive data in real time (Xie *et al.*, 2013).

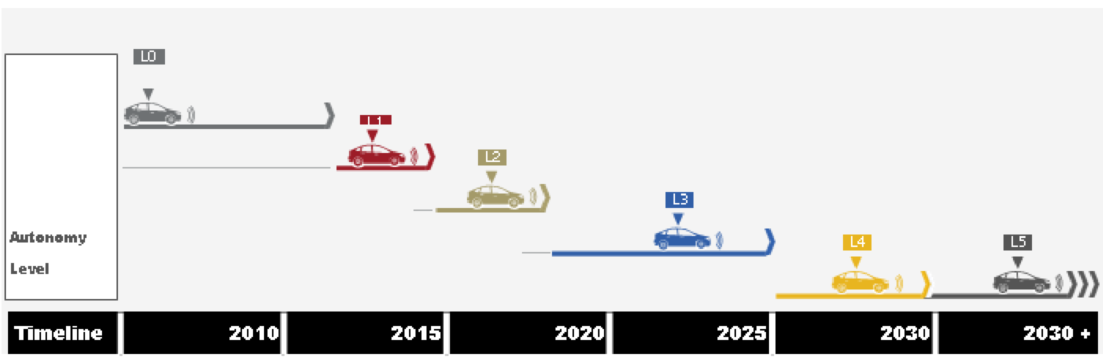

Figure 6. Connected and autonomous vehicle technology road map (Hawes, 2015)

4.2 The ethical issues of data analytics in autonomous vehicles
What is the significance of discussing the ethical concern on the new technology? O'Leary (2016) states that ethical concern can provide a signal that technology can be monitored at different stages of development. In addition, researching on ethical considerations in new areas of technology can reinforce the original code of ethics and discover the social nature of technological development when developing ethical norms (Kord, 2012). Therefore, ethical concern not only monitors technological developments but also implements the development of a new code of ethics. Finally, there is no way to fully anticipate what will happen in the future. People tend to solve various ethical issues until the technology is fully developed. Moreover, no recommendations and solutions were given to the ethical issues before maturity (Joy and Gerla, 2017). Therefore, setting up an ethical concern before a technology widely used helps to identify potential ethical issues in advance and it can provide enough time to come up with solutions (O'Leary, 2016).

Kord (2012) provides that there are four main ethical issues when big data in used in area of new industry including identity, privacy, ownership and reputation. He explains that different kinds of case to further explaining the importance of solving ethical issues. Also, Joy and Gerla (2017) state that when IoV, which is one of the common data analytics tool, being used in autonomous vehicles, there will arise privacy and secrity issues which can block the futrue development of autonomous vehicles hit into public. Therefore, it is nessary for autonomous vehicles to use data analytics within the scope of ethics.

4.3 The Need and Benefit of Data Analytics in Autonomous Vehicles

4.3.1 Autonomous vehicles can use data analytics to ensure driving safety

Driving safety is the first problem to be improved when autonomous vehicles facing the public. Although the technologies applied to vehicles are getting more advanced, there are still a large number of deaths caused by traffic accidents in the world. In recent years, the number of deaths from traffic accidents in China has exceeded 100,000 each year (Xie *et al.*, 2013). With such a large number, we can conclude that traditional vehicles are not enough to ensure our safety. However, autonomous vehicles can use data analytics to design collision avoidance system, which has collision warning and driving assistance. By collecting and analyzing nearby vehicle data, road data and emergency braking data, the collision avoidance system eliminates accidents due to human error including distraction, inattention, high speed, etc. It greatly reduces the possibility of collisions by 20%, and the number of traffic accidents dropped 30% to 70%. In addition, when a car accident occurs, a distress signal can be sent out in time through specific buttons, and the exact position data of the vehicle can be collected by using global satellite positioning technology ('China Automotive,' 2017). The data analytics can save time for rescue work and minimize the owner's property loss. At the same time, the result of the accident data analytics is sent to the surrounding vehicles so that the surrounding vehicles can make timely evasive measures to prevent a wider range of accidents from occurring (Li *et al.*, 2017).

4.3.2 Autonomous vehicles can use data analytics to avoid traffic jams

According to the survey, Beijing's peak congestion delay index is 2.06 with an average speed of 22.61 km/h, which means that it need spend more than twice the time to reach the destination at the peak time. Nowadays, traffic congestion is not only appeared in first-tier cities, but also very common in second and third tier cities (Xie *et al.*, 2013). Autonomous vehicles can use data analytics to collect and analyze current traffic data, weather conditions, the previous results of the data analytics and so on to predict road congestion in the future, and choose one of the most convenient and time-saving road to optimize driver's driving decision. In addition, autonomous vehicle operators can collect and analyze data analytics results of autonomous vehicles once again to intelligently adjust the traffic light at the intersection, making autonomous vehicles to travel as smoothly as possible at intersection to increase vehicle throughput rate and reduce travel time (Li *et al.*, 2017).

4.3.3 Autonomous vehicles can use data analytics to improve the driver's driving experience

In long-term driving, the onboard social network can collect many driver's personal characteristics and driving style data, such as age, job, weight, and driving speed, turning time, etc. By analyzing these data, vehicle drivers or owners can interact well with the vehicle through the driving and entertainment information display, which displays GPS navigation routes, video playback, vehicle safety monitoring data and so on (Daziano *et al.*, 2017). According to the results of the data analytics, different decisions are made according to different driver characteristics to rescue the driver from stress, fatigue and tiredness, making the travel meaningful.

4.4 The Applications of Data Analytics in Autonomous Vehicles

Internet of Vehicles is an extension of the Internet of Things (IoT), and it is the most extensive and effective application of data analytics in the field of autonomous vehicles. IoV has three components: terminal system, management system and cloud system. The terminal system collects vehicles and roads data in real time via on-board equipment. The management system is managed by the telecom companies to organize and transfer the data uploaded by each terminal system. The cloud system is jointly established by various companies owning data to analyze and store big data and give real-time data analytics results. The results of these analytics are delivered through the network to the terminal system for autonomous driving. The following part will discuss each specific process of data analytics (Datta *et al.*, 2017).

Motion trajectories of vehicles are affected by various objects, including other vehicles, obstacles, pedestrians, etc. Although driving data is complex and diverse, it is not enough to be analyzed relying solely on the data of individual vehicles for autonomous driving. First of all, sensors installed on the vehicle can collect a lot of data, such as driver's driving status, the implementation of the road conditions and so on. As IoV is widely used, data collected by individuals can be integrated into big data for the entire driving environment, see Figure 7. IoV can collect data of different vehicles in different locations at different times by vehicle nodes, and the data will be stored by the big data center after transferring the data by sink nodes (Guo *et al.*, 2017).

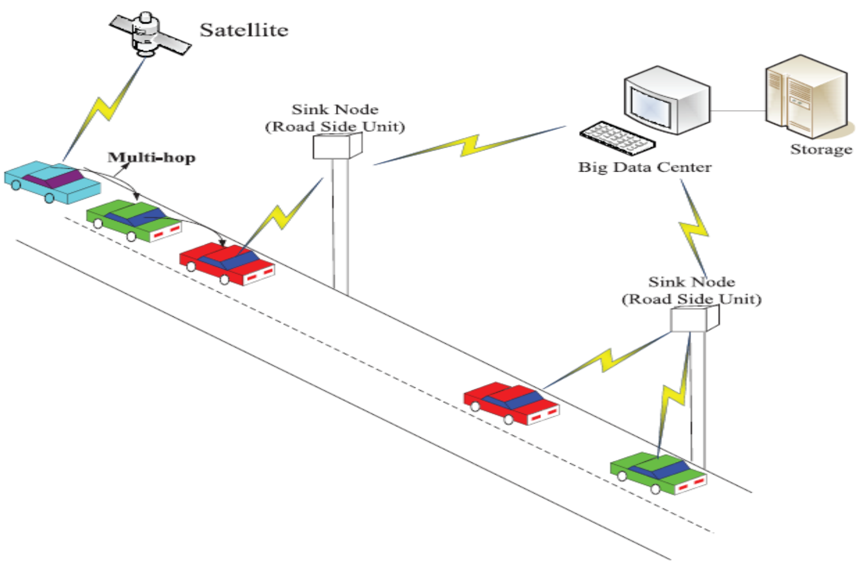

Figure 7. Basic architecture of data analytics in autonomous vehicle (Guo *et al.*, 2017)

With the wide application of data analytics technology in the field of autonomous vehicles, the collected data not only relate to personal privacy, such as the real-time location of the vehicle, but also include some important data, including vehicle operating parameters closely related to traffic safety. Some unscrupulous people use the data to send fraudulent claims that infringe on privacy and endanger the transportation system or charge for their own benefit. Therefore, how to avoid an ethical problem of large-scale driving data acquisition needs further study.

5 Discussions on Emerging Services and Analytics

As, the new data-related challenges are surfacing due to the evolution of IoT, the scientific communities are developing new services and analytics tools at the same pace to efficiently address them. Pachube (Haque, 2004) is believed to be one of the few providers, which begin the online data-related services, especially facilitates the attachment of sensor data to Web. Today, it delivers an IoT-enabled platform for cloud-based real-time data management. Nimbits (Nimbits Inc., 2015) is IoT-supported, cloud-powered, open-sourced, freely available social platform that assists in sensor data collection, storage, and sharing through cloud services. iDigi (Digi International

Inc., 2015) is a rich PaaS framework, quipped with all the required tools & techniques for the secure, cost-effective, and scalable connectivity, integration and communication management of enterprise applications with remotely located sensing devices, independent of network and location. ThingSpeak (2014) is another an IoT-enabled open-sourced SaaS platform, with rich set of APIs for data storage and communication from sensing devices. Madria et al. (2014) consider geographical area and propose a platform - Sensor cloud. It is a cloud-powered framework to virtualize the wireless sensors based on the covered geographical area. Sensor cloud can accommodate the on-demand multi-user networks connection simultaneously over a large geographical area. In IoT age, Sensor cloud, a multi-user environment, is being considered as a potential substitute of resource-constrained physical traditional wireless sensors.

Each one of the cloud-based emerging services, described in section 5 is highly robust in the dedicated job execution for which it is designed and developed. CLAaaS is an effective service for IoT-enabled applications, where each device generates lots of data that can be transmitted from one device to another device. It also supports the multi-faceted analyses of big data, on demand storage of data and other services through the customized user interfaces. It is one of the most reliable data-oriented services that leads on easy tailoring the client's requirements. In cloud environment, DaaS is considered as the most effective service for swift storage and management of Big Data, generated from various kinds of connected things such as sensors, circuits, actuators, etc. This data is aggregated from multiple machines or vehicles and stored in the cloud or storage devices. The integrity of IoT data among the sensor-embedded, wireless-enabled things is maintained through the services (DIaaS) that must use the upper edges of highly secure cryptographic hashing algorithms. It ensures that the data is not changed during transmission. The mining operations on IoT data are supported for both small and large volume in cloud environment, therefore, are suitable for small scale as well as large scale clients. In cloud, the mining services (DMaaS) are especially required for those clients, which have large volume of data, but comparatively limited budget for data analysis. In practice, the nature of IoT data can vary from little to extraordinarily large. The security and privacy protection of the device generated Big Data require the essential security measures in place. The security threats between sensor-actuator and networks are an eavesdropper listening on data or commands that can reveal information about the operations of the infrastructure. A fake device in IoT network may inject fake measurements that can cause the failure occurrences, managed through FaaS; it can disrupt the control processes, resolved most effectively through IPMaaS and can also react inappropriately or dangerously. Also, it can be used to mask physical attacks and in between network and server. The maintenance of security services (SecuaaS/SaaS) in IoT is extremely hard, resource-exhaustive and high-priced; the sustenance of such services requires the expert resources. The sensing services (SaaS/SenaaS) in IoT support the data acquisition from the ubiquitous sensing systems, actuators or other devices that extract the system logs or operating on the data, gathered from other machines or vehicles and transmit wirelessly. The sensors or actuators in IoT exploit the sensing services (SaaS) through various handheld devices. In the cloud environment, such energy-efficient IoT services have the ability to support various sensing applications on different platforms. The commodity things in IoT are highly likely to communicate the message and alert notifications. The message and alert related services are supported through SEaaS. VSaaS outperforms the other cloud services of same nature when it comes to surveillance related services. It is a highly-ranked, trustworthy, robustly secured efficient service. In surveillance systems, the IoT-enabled objects/devices/things generate the vast amount of video data such as recording, remote viewing etc.; the cloud coordination for the device-generated data management though VSaaS delivers additional robustness to the comprehensive surveillance systems. Chang and Wills (2015) analyze the effective methodologies and metrics for fair performance comparison between cloud and non-cloud storage systems to for efficiency and performance improvements. Chang, Kuo and Ramachandran (2015) build a cloud framework-Cloud Computing Adoption Framework (CCAF) and to address the recent real-time security concerns for cloud data of petabytes range, CCAF is tailored to provide robust security to the clouded data. Also, discussed are the overview, rationale and components in the CCAF.

6 Impacts and Benefits to Businesses

This section illustrates some of the transformative and sustainable impacts and benefits of Big Data, IoT, cloud-based the emerging services and analytics to the business domain. Over the last few years, the advancements in data science has transformed the business domains. The availability of multidimensional, heterogeneous and voluminous datasets and functionally-rich data engineering and analytics models have greatly impacted the businesses and the robust analyses of the data through various dimensions have delivered uncountable benefits that have enormously contributed in sustainable growth of the businesses. As, the services and analytics are capable to illuminate the complex relationships of the variables of the data and hidden patterns, the business entities now take the best advantages of emerging services and analytics in uncovering the dubious market trends, variations in customer preferences, etc. The findings through analytics can lead to several efficacious improvements to the present state of the entities in a related domain. For example, for a business domain, the unraveled information can help in ameliorating the marketing strategies, enhancing revenue generation, delivering more effective customer related services, ensuring upgraded operations etc. The use of the recommendation systems is widely and popularly witnessed in almost of kinds of businesses to improve their sale, which intelligently and dynamically analyze the previous purchasing trends of the buyer and consequently recommend new products to them on their return. Therefore, the emerging services and analytics have impacted the businesses in effective ways for better informed decision making process.

The footprints of the impacts and benefits of emerging IoT in businesses are not yet fully expanded, but early traces have begun visible. The businesses believe to have innovative impacts, especially organizational and institutional as the aura of IoT grows and transforms the traditional business performance and procedures. The IoT-led huge data generation as a result of normal daily operations or chores is seemingly to offer enormous opportunities to draw benefits to the businesses. However, the generation of invaluable or unnecessary data, may be in small quantities, is susceptible to adversely impact the businesses instead as such data is more vulnerable to misuse that may proceed to invalid or untrue conclusions. Some of the obvious benefits, the IoT is expected to deliver to businesses and also to communities are energy conservation, reduced costs and public safety. However, the data privacy and protection in IoT will have critical influence from the public behavior and opinions. Also, the data privacy and protection will be impacted by the extent the behavior-related private information of people are allowed to be public, where certain behavior events trigger the harvesting and trading of the information. As, IoT is increasingly integrating the technological systems at large-scale, in near future, the businesses may be greatly benefitted with the IoT-enabled automation that will favorably impact the business quality, reliability, and sustainability.

The inclusion of cloud-supported computing environment has witnessed tangible impacts and quantifiable improvements in business domain. The SaaS model helps the businesses to maintain the most up-to-date version of their software applications, required for successful run of the business, and to make is globally available with zero down-time. The improved features as new enhancements in typically frequently new releases are made available for public use in no time; this leads to highly positive impact on the businesses and helps enhance the business productivity and sustainability. The highly affordable cloud-environment, equipped with the rich set of extremely secured robust services has inspired the almost all the businesses to partially or fully migrate their large, expansive, exceptionally protected and secured data centers. This in its entirety helps reduce significantly (a substantial part of business budget) the IT-related operational cost of the businesses and upwardly impacts them with improved IT capabilities. The cloud-housed applications are good candidates for collaboration that through shared storage, easily share the dispersed but relevant information in real time; the subsequent analyses of such information may help improve the product development and customer service; this also will lead to reduction in time-to-market. The businesses take best advantages of the flexible nature of cloud computing technology, where, on demand, the additional capacity to the provisioned resource can be quickly provided during a sales promotion to successfully accommodate the sudden increase in customer traffic and to avoid any slowness in response time, hence to avoid losing sales; once, the promotion is over, the previous capacity is requested back and thus operate back on the reduced cost after comparatively a short-lived spike. The worldwide cloud adaptation in businesses has substantially reduced the number of energy-hungry data centers and is aiding the energy efficient operations. In sum, the cloud environment and the cloud-based emerging services are enforcing the reduction of the carbon footprints, promoting the healthy and green environment and encouraging the businesses for enhancing the green credentials (West and Goldenberg, 2012).

7 The Ethical Issues of Data Analytics in Autonomous Vehicles

7.1 Privacy issues in data collection, storage and extraction

With the extensive use of various data collection facilities, the autonomous system can not only identify the driver through physiological characteristics such as fingerprints and heartbeats, but also automatically adjust the vehicle speed, the temperature in the car and the music according to the preference of different people. The autonomous system can even determine whether the driver is healthy and gives driving advice through sleep time, exercise conditions, dietary habits and physical characteristics (Joy and Gerla, 2017). However, the use of these autonomous technologies means that autonomous systems have a great deal of personal information and are even more selfaware than themselves. Sometimes data collection is not authorized by the owners of the vehicles. Privacy violations can arise if certain private information is collected illegally for commercial purposes without permission (Kord, 2012).

Due to the generally high computing power of autonomous driving systems, cloud computing has been configured as the main architecture in many autonomous vehicles. Many autonomous vehicle data telecommunication companies and government agencies on road safety are beginning to store data on the cloud because cloud computing technology is easy-to-use with a low-cost, and allocate data resources according to demand based on a share-data-pool. After storing the privacy information on the road to the cloud, the information is vulnerable to various threats and attacks. When the database is attacked or sold to a third party, it created a ethical issue of privacy disclosure (Guo *et al.*, 2017).

The extraction of driving knowledge from driving data is an important ability of autonomous vehicles. Driving knowledge extraction tools are becoming more powerful, numerous seemingly unrelated pieces of driving data may be integrated together to identify individual driving behavior characteristics and even driving style features. For example, by combining driving history, parking locations, driving speeds, and other types of recorded data, a driver's driving trajectory can be sketched. Personal driving preferences and driving habits can be analyzed to further predict driver's potential demand, which can be used by automotive, insurance and other related suppliers to provide drivers with the necessary information, products or services in advance (David *et al.*, 2016). However, these personalized customization processes are accompanied by the discovery and exposure of personal privacy. The fragment data collected with permission can be extracted the sensitive personal information, which the users do not want to disclose.

7.2 Security issues in data analysis protection and governance

Autonomous vehicles use data analysis to replace many drivers' decision-making behaviors. However, autonomous vehicles can still cause traffic accidents due to the complex road environment. People have their own ethical codes when an accident occurring, while autonomous vehicles also need to comply with the rules of human society when making decisions. For example, assuming three pedestrians on the sidewalk in front of an autonomous vehicle which cannot be braked in time, whether the autonomous system choose to hit these three pedestrians or to a pedestrian who turns into a roadside? The application of autonomous vehicle technology is regularizing some of the ethical issues in life. If it is not combined with social ethical constraints in the research, develop and design of the system, it is possible to follow the logic different from that of humans in decision-making, which may lead to serious security issues (Applin, 2017).

Some autonomous vehicle companies or telecom operators tore autonomous vehicle data in the cloud system in order to provide vehicle owners through the mobile terminal remote control vehicles or provide cloud services. So far, there is no clear cloud data protection standards because autonomous vehicles are not put in mass production all over the world. Without an effective system of protection, hackers can find, unlock, and fire startup features in the cloud with a simple laptop, and even commands that run from the cloud can override those who operating in the car. This means that once the loophole is mastered and exploited by the extremists, even if he is not in the scene, it is easy to create a traffic accident at a designated road site (Ring, 2015). The situation is very serious at high speed or traffic-intensive roads or at major event sites of. In 2013, Chris Miller and Chris Valase successfully used their laptops to gain access to the vehicle data storage system, which led to the successful control of smart vehicles (Greenberg, 2016) .

In addition, the government is more concerned with public safety than car makers and car owners. Poor regulation of data poses a threat to public safety. Research on autonomous vehicles requires a lot of experimentation on highway and urban roads. At present, some national governments have allowed some smart car companies to experiment on the road. For example, the United Kingdom allows Mercedes-Benz and Audi autonomous vehicles to carry out drone experiments at speeds below 60km/h. In California, USA, the current law requires autonomous cars to have driver supervision on their side while conducting experiments, including Tesla, Google, etc. The data collected by autonomous vehicles include the user's body characteristic data and driving trajectories collected from the real environment. If the information is obtained by terrorists, they can use the data to design terrorist attacks where the vehicle is often jammed. If the government is lack of monitoring of these data, resulting in abuse of data stored in the cloud or car prices, will pose a great threat to public security (Crayton and Meier, 2017).

7.3 Recommendations for security issues

7.3.1 Development of ethical guidelines for analysis

When autonomous vehicles make decisions and take actions, people want their behavior to conform to the ethical rules of human society that should be taken into consideration and embedded in autonomous vehicle systems during system design and development. Therefore, it is necessary to establish ethical guidelines for the research and development of autonomous vehicles, which can guide designers and manufacturers on how to make an ethical hazard assessment of a vehicle and to form a complete research and develop specification of autonomous technologies (Applin, 2017).

7.3.2 **High safety standards for autonomous vehicles**

Data analytics cannot solve the ethical dilemma of who should be given priority in accidents. In order to minimize the possibility of data analytics encountered in the field of autonomous vehicles such a dilemma, it can focus on improving the effectiveness of data analytics and leaving enough time for the reaction of the vehicle. In addition, autonomous vehicles should have enough data protection measures to ensure the data would not be hacked by criminals. Reliable autonomous vehicles should have strong safety performance and be able to adapt to different road conditions, effectively handle all kinds of deliberate attacks and avoid accidents caused by abnormal malicious operations (Fleetwood, 2017). On the one hand, it is necessary to improve the safety standards for the development of autonomous vehicles and technically improve the security and robustness of autonomous systems. For example, improve the safety of chip design standards to ensure the advanced nature of the algorithm and timely updates. On the other hand, it is necessary to implement autonomous system safety certification, strictly test autonomous vehicles, enhance public trust and ensure the healthy development of autonomous vehicles (Xie *et al.*, 2013).

7.3.3 Strong supervision for data usage

The data of autonomous vehicles are owned by individual autonomous vehicle companies or operators, government does not have enough energy to supervise all driving data. This does not mean that the government should allow casual use of data. The government can prompt large smart car companies to jointly establish a cloud platform that can share resources (Datta *et al.*, 2017). Vehicle companies and operators stored the data in the cloud platform, other people or organizations can also use the resources. In this way, the regulation of the data is to supervise the cloud platform. In addition, it is suggested that a set of open and transparent autonomous vehicle supervision system should be set up at the national level to realize the full supervision of autonomous driving algorithm design, product development, data collection and product application. Furthermore, government needs to increase the punishment for violations, urging autonomous vehicle industry and corporate self-regulation.

8 Conclusions and Future Work

This work provides a comprehensive illustration about the cloud-based emerging service and analytics. The selection of the services of interests is majorly influenced by their utility and applicability in IoT paradigm. Additionally, other important and useful emerging services are also briefly explained, especially for the business domain. The management and mining of large volume of data amassed, especially from the sensing systems are posing sturdy challenges to the traditional techniques. This is where, the quest for new emerging services and functionally-rich multifarious analytics begins; today, the concept of cloud computing has emerged as the most sought destination that promises to effectively address the data triggered challenges. In this paper, we further understand the broader concept of cloud environment that imbibes the emerging services and analytics also and has revolutionized the perspective of management and sharing of IT resources and services. The applications with complex data-intensive computations are the best candidates to qualify for cloud computing advantages. The next generation emerging service developments are bridging the gap and helping the cloud computing to gradually accommodate the IoT challenges completely and providing the abundant analytics tools to the end users.

We also present a n-depth emerging service, data analytics in autonomous vehicles including the functions and current status. This paper focuses on two ethical issues: privacy and security. Data analytic requires the big data to solve problems, but people pay more and more attention to the protection of their privacy data. Without appropriate legal and technical measures to solve this problem, users may no longer be willing to provide their own data to the car or other departments (Claus et al., 2017). Security is also an ethical issue that needs attention. It not only includes driving safety of vehicle users, but also road safety and public safety. By reviewing the data analytics of ethical issues and solutions in many areas, this article provides some recommendations from multiple perspectives. Some are already on the scene. For example, the Chinese government has started to step up monitoring cloud data of major operators, like Ali Cloud System. The others are still stuck in the theoretical aspects worth further proof to practice. In summary, it is necessary to have ethical concerns for data analytics in autonomous vehicles.

The core contribution of this study was to explore the cloud-based emerging services that helps in comprehensive data analytics for even technical naïve end users such as stakeholder, director, manager, etc. We briefly overviewed the concept of cloud computing and explored some emerging services, may be useful in IoT. It was discerned that the number of data management systems had grown swiftly in last few years and was still expanding. Each data model claimed to outperform others with its unique storage technology and computing mechanism. For a cloud-interested user, to find the most suitable cloud-enabled model, it became too difficult to examine the underlying technology through the big pool of available models. Therefore, we presented a novel classification, called CNNC {Clouda, NNClouda}; the basis of the classification was the scientific name of the models and intended to harness their intuitiveness to better assist the users. Hypotheses were used to validate the proposed classification and some of the available models of each class were investigated to test the correctness. The investigation revealed, a cloud-powered model was correctly classified as either Clouda or NNClouda, but certainly fallen under CNNC classification. However, in one instance, interestingly a model (LightCloud) was found qualified for Clouda subclass, but was not cloud-powered at least yet. This basis helped inferred that Clouda class not necessarily had all the models as cloud-supported. The CNNC classification was further strengthen through some related case studies. Additionally, being cognizant of IoT scope, some important emerging services and analytics were also explored. Future work includes the further expansion of the discussion on the emerging services and analytics from the perspective of integration of the emerging technologies in various domains.

Additional references

Applin, S. (2017) 'Autonomous Vehicle Ethics: Stock or custom?', *IEEE Consumer Electronics Magazine, Consumer Electronics Magazine, IEEE, IEEE Consumer Electron. Mag.*, (3),pp. 108.

'China Automotive', (2017) *Acquisdata Industry SnapShot: China - Automotive*, (7614),pp. 1.

Claus, S., Silk, N. and Wiltshire, C. (2017) 'Potential impacts of autonomous vehicles on the UK insurance sector', Bank of England Quarterly Bulletin, 57(1),pp. 40-48.

Crayton, T. J. and Meier, B. M. (2017) 'Autonomous vehicles: Developing a public health research agenda to frame the future of transportation policy', *Journal of Transport & Health*, 6,pp. 245-252.

Datta, S. K., Haerri, J., Bonnet, C. and Ferreira Da Costa, R. (2017) 'Vehicles as Connected Resources: Opportunities and Challenges for the Future', *IEEE Vehicular Technology Magazine*, 12(2),pp. 26.

David, S., Kenneth. and Sun, Z. (2016) 'Meta-analysis of big data security and privacy: Scholarly literature gaps', *IEEE Consumer Electronics Magazine, Consumer Electronics Magazine, IEEE, IEEE Consumer Electron. Mag.*,pp. 4035.

Fleetwood, J. (2017) 'Public health, ethics, and autonomous vehicles', *The American Journal of Public Health*, (4),pp. 532.

Greenberg, A. (2016) 'Hackers Remotely Kill a Jeep on the Highway—with me in it', [online], available:http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/[accessed on March 2, 2018.].

Guo, L., Li, Q., Ye, T., Wu, J., Li, J., Dong, M. and Ota, K. (2017) 'A Secure Mechanism for Big Data Collection in Large Scale Internet of Vehicle', *IEEE INTERNET OF THINGS JOURNAL*, 4(2),pp. 10.

Hawes, M. (2015) 'Connected and autonomous vehicles- the UK economoic opportunity', [online], available: http://www.smmt.co.uk/wp%E2%80%93-The-UK-Economic-Opportu...1.pdf [accessed 28/March./2016.].

Joy, J. and Gerla, M. (2017) 'Internet of Vehicles and Autonomous Connected Car - Privacy and Security Issues', in *ICCCN*, Vancouver, IEEE.

Kord, D. (2012) *Ethics of Big Data*, Beijing: O'Rilly Media, Inc.

Mark, C., Magnus, E., Jonathan, P. H. and Richard, M. M. (2010) 'Autonomous driving in urban environments: approaches, lessons and challenges', *Philosophical Transactions: Mathematical, Physical and Engineering Sciences*, (1928),pp. 4649.

O'Leary, D. E. (2016) 'Ethics for Big Data and Analytics', *IEEE Intelligent Systems IEEE Intell*,pp. 81-84.

Ring, T. (2015) 'Feature: Connected cars – the next targe tfor hackers', *Network Security*, 2015,pp. 11-16.

Xie, B., Li, K., Wang, J. and Zhao, S. (2013) 'Vehicle networking concept and its automotive industry applications based on'triple network convergence'', *JOURNAL OF AUTOMOTIVE SAFETY AND ENGERGY*, (4),pp. 348.