IoV Internet of Vehicle

INTERN SEBASTIAN ARRAZATE MARTINEZ

Evolution of connected cars

Went through a number of phases that were categorized depending on who defined this categorization. Regardless of the source of these categories, different technologies and different improvements were included and new players and new business models were also introduced

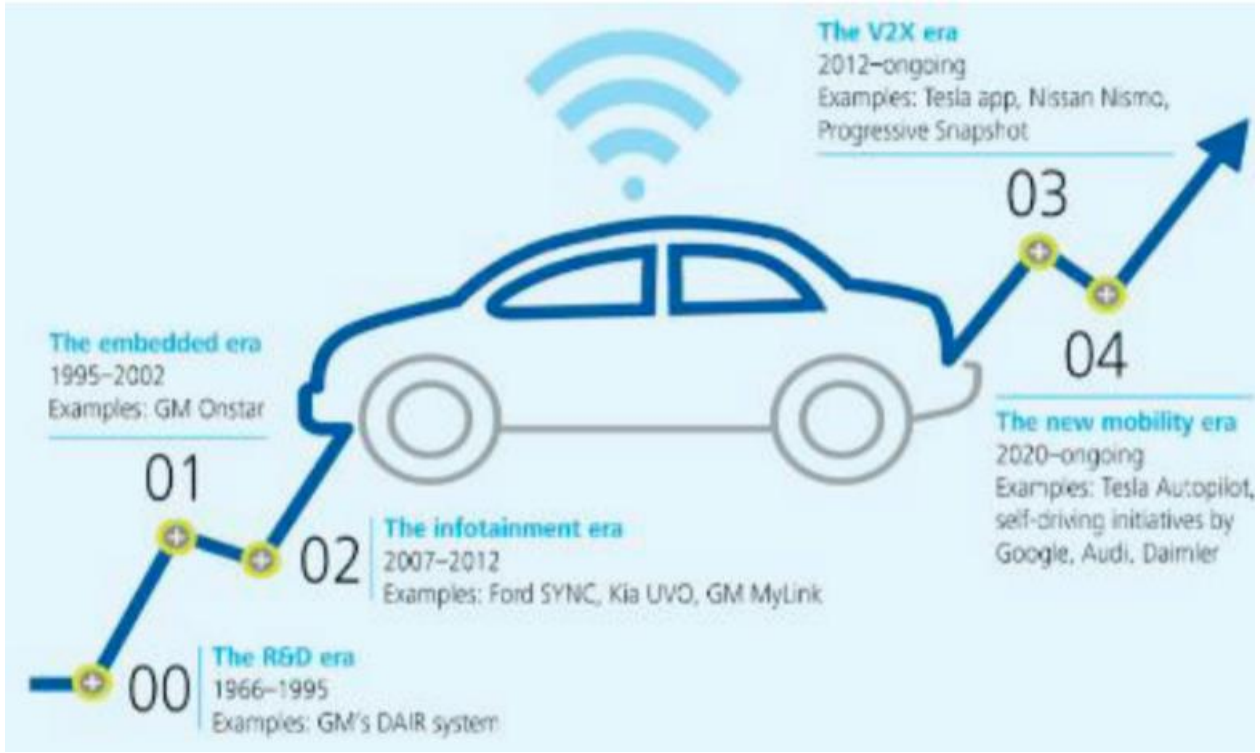
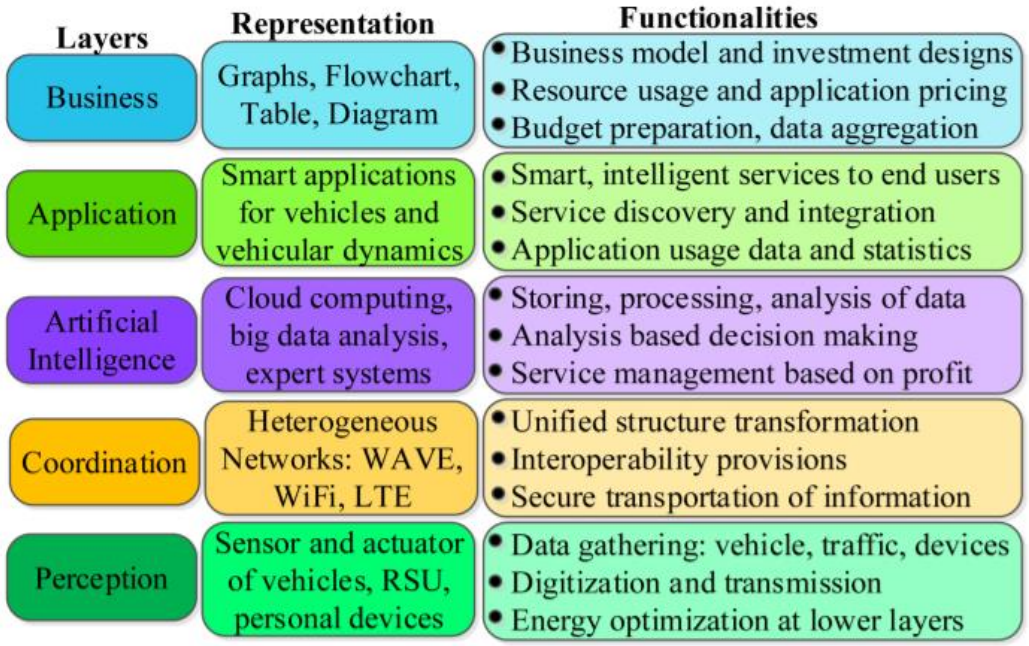


Figure shows phases that started back in 1960-s and goes beyond 2020.



The five layered architecture of IoV

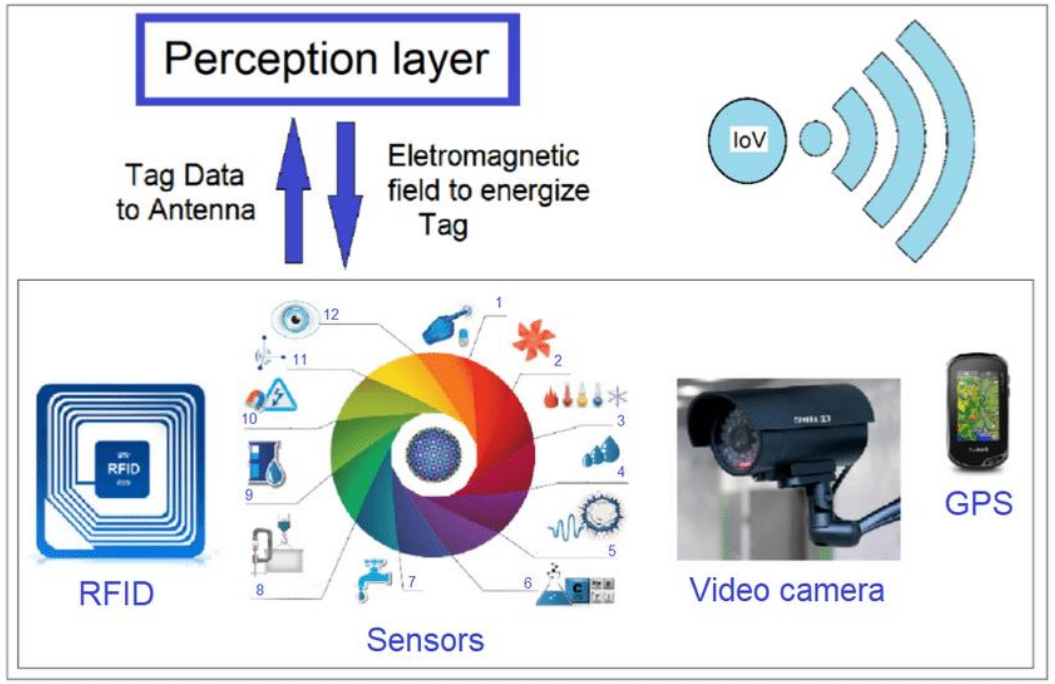
LAYERED ARCHITECTURE AND PROTOCOL STACK

The layered architecture design of a universal network which includes heterogeneous networks is a quite challenging task. It requires to identify and effectively group similar functionalities and representative elements of heterogeneous networks as a layer.

The representations and functionalities of each layer are described below in detail and a summarized

PERCEPTION LAYER

The primary responsibility of the layer is to gather information regarding vehicle, traffic environment and devices. The vast of information includes speed, direction, acceleration, position, engine condition and travel documents related to vehicle, on-road vehicle density and weather conditions related to traffic environment, and multimedia and infotainment records related to people. Architecture is represented by the different types of sensors and actuators attached to vehicles, RSUs, smartphones

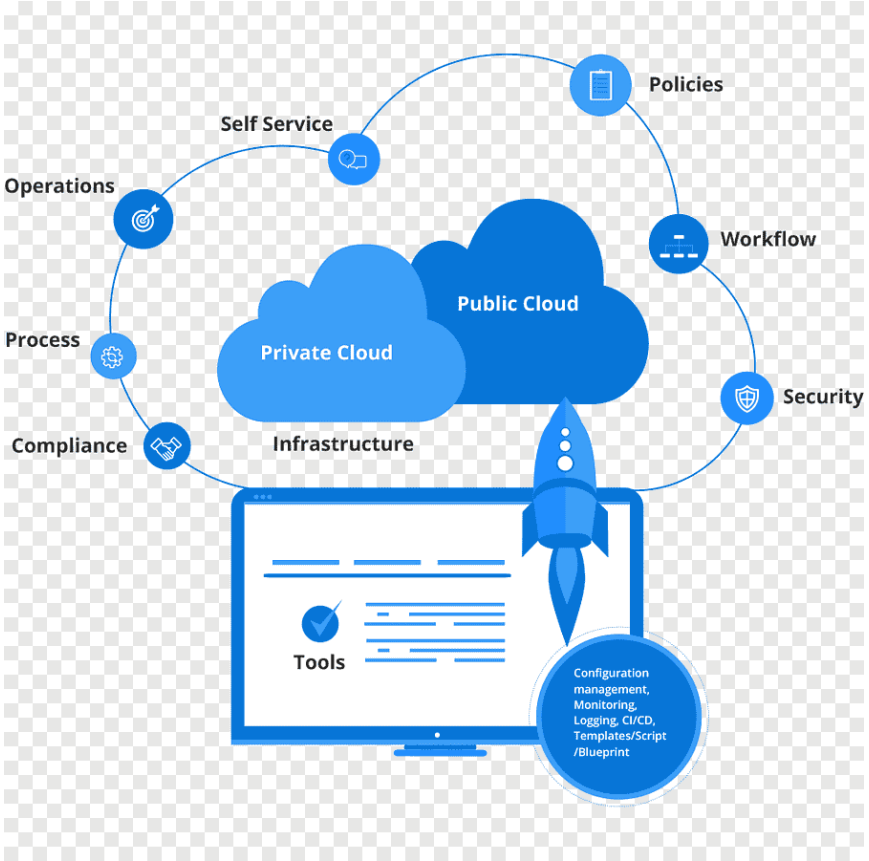


CO-ORDINATION LAYER

The second layer of the architecture is represented by a virtual universal network coordination module for heterogeneous networks involving WAVE, Wi-Fi, 4G/LTE and satellite networks, through which the perceived information from the lower layer is securely transferred to the artificial intelligence layer for processing. Due to the lack of standards, interoperability and cooperation among different types of networks is one of the main concerns in IoV for providing reliable network connectivity handled by this layer.

ARTIFICIAL INTELLIGENCE LAYER

It is the brain of IoV and responsible for storing, processing and analyzing the information received from lower layer and decision making based on the critical analysis. It works as information management center where computing and analysis techniques including Vehicular Cloud Computing (VCC) and Big Data Analysis (BDA), and Expert System are major operational components. Due to the number of services offered in cloud environment, service management is also one of the major concern in IoV where exclusive and dedicated services are the requirement of smart applications which are also handled by this layer.

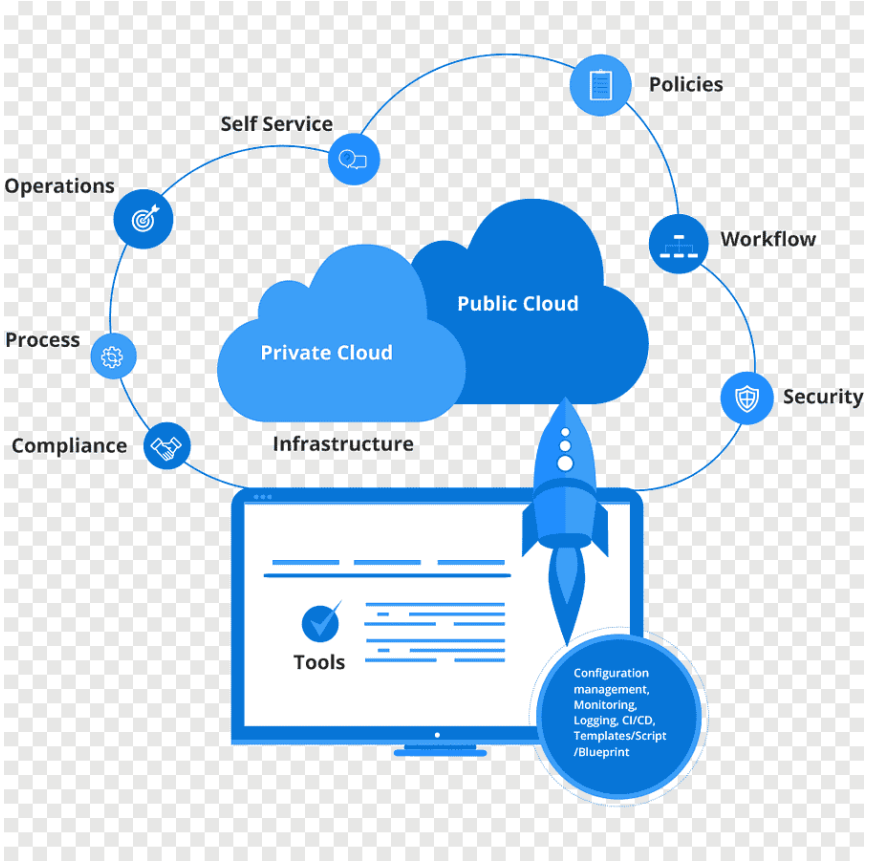


APPLICATION LAYER

The fourth layer of the architecture is represented by smart applications, ranging from traffic safety and efficiency to multimedia-based infotainment and web-based utility applications. The layer is responsible to provide smart services to end users which are based on intelligent and critical analysis of processed information by the AI layer. t also provides end user application usage data to the business layer.

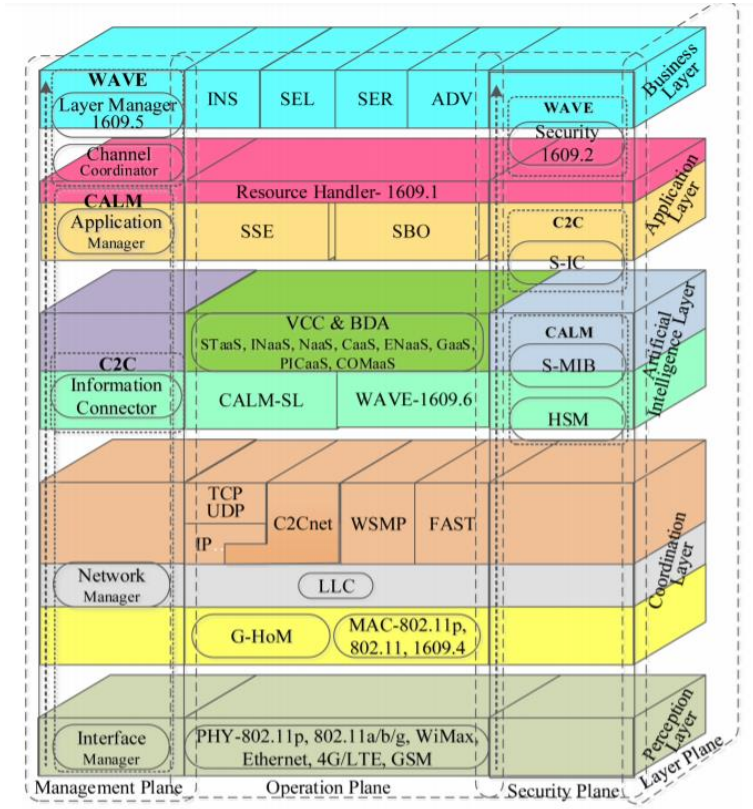
BUSINESS LAYER

The fifth layer of the architecture is represented by the operational management module of IoV. The major responsibility of the layer is to foresight strategies for the development of business models based on the application usage data and statistical analysis of the data. Different types of analysis tools including graphs, flowchart, comparison tables, use case diagram, etc., are the major part of the layer.



PROTOCOL STACK

The protocol stack has three planes including security, operation and management. The appropriate protocols are identified for different layers and planes of the architecture of IoV by quite efficiently managing most of the functional requirements using existing protocols.



The protocol stack for the five layered architecture of IoV

SECURITY PLANE

In this plane, security protocols including IEEE 1609.2, Security Information Connector (S-IC), Security Management Information Base (S-MIB) and Hardware Security Module (HSM) could be utilized which have been developed under WAVE, C2C and CALM projects; respectively. Security protocols for IoV is still an open research challenge due to the unavailability of clear definitions of layer wise security protocols which is being explored in some recent projects of IoT.

OPERATION PLANE

In perception layer, a few wireless access protocols could be considered in physical layer including 802.11p [38] of WAVE, 802.11a/b/g of Wireless Local Area Network (WLAN), Worldwide Interoperability for Microwave (WiMax), Ethernet, 4G/Long Term Evolution (LTE), Global System for Mobile communication (GSM) and satellite communications.

The coordination layer is divided into three sub-layers including lower, middle and upper:

1. The different MAC protocols could be utilized at lower sub-layer including IEEE 802.11p, 802.11 (a/b/g/n) and 1609.4 along with a Global Handoff Manager (GHM).
2. A Logical Link Control (LLC) protocol could be considered at middle sub-layer.
3. At upper sub-layers, three protocols including C2C network protocol (C2C-net), Short Message Protocol (WSMP) and Fast Application and Communication Enabler (FAST) could be considered for carrying out the operations of network and transport layers apart from traditional IP and UDP/TCP combinations.

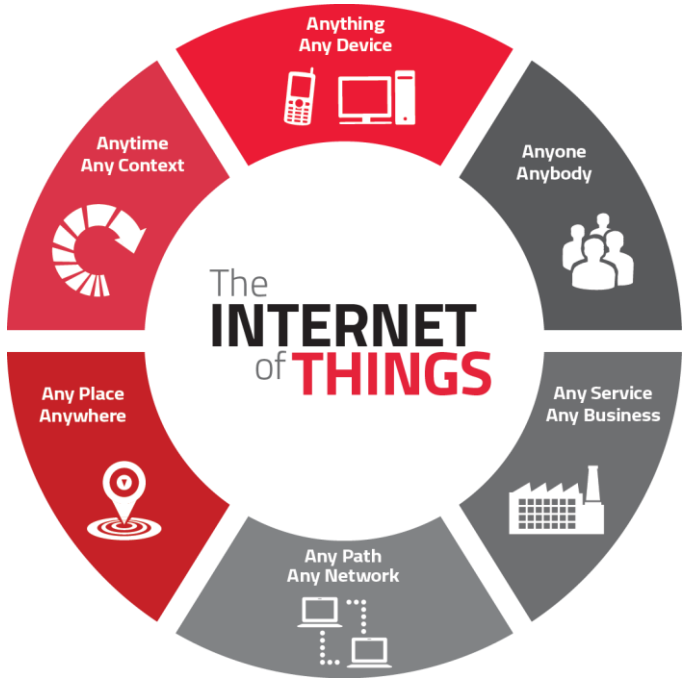
OPERATION PLANE

In Artificial Intelligence (AI) layer.

Protocols could be utilized at upper sub-layer including the cloud services Storage as a Service (STaaS), Infrastructure as a Service (INaaS), Network as a Service (NaaS), Cooperation as a Service (CaaS), Entertainment as a Service (ENaaS), Gateway as a Service (GaaS), Picture as a Service (PICaaS) and Computing as a Service (COMaaS).

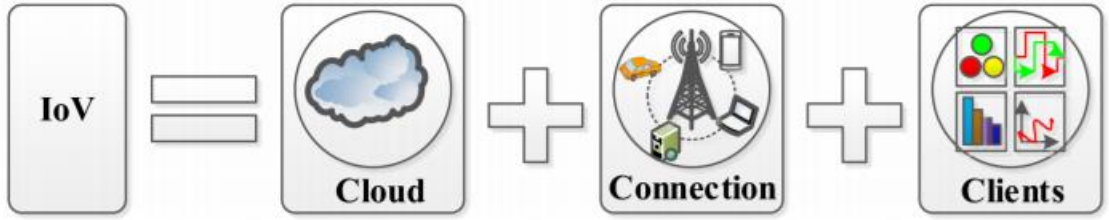
MANAGEMENT PLANE

In this plane, three protocol groups belonging to the management operations in WAVE, CALM and C2C could be considered. Layer manager IEEE 1609.5 and channel coordinator protocols are developed in WAVE. CALM has suggested three protocols for management purpose; namely, application, network and interface managers. Information connector protocol has been suggested in C2C for the same purpose.

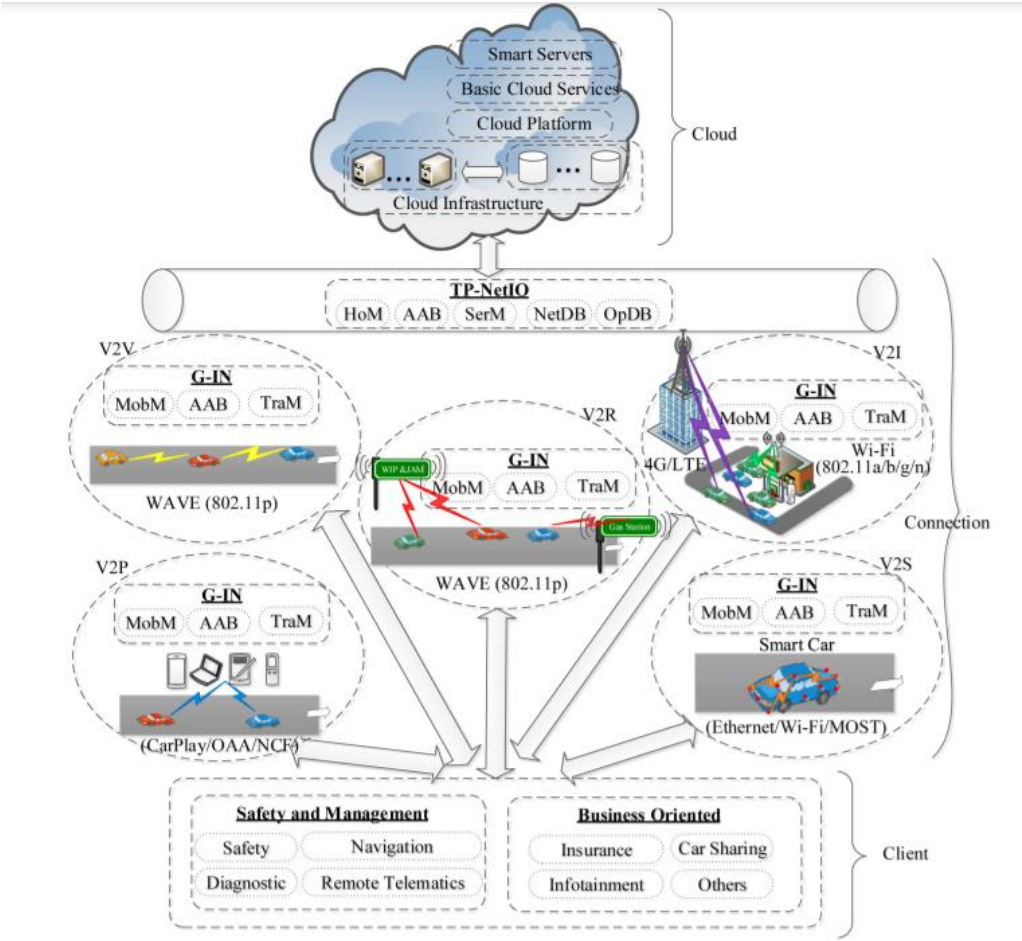


NETWORK MODEL

The building blocks of IoV in terms of network elements more effectively express the meaning and functionalities of IoV as a comprehensive heterogeneous network. The three major network elements of IoV are identified which include cloud, connection and client.



The three network elements of IoV.



The network model of IoV with the three network elements

Cloud

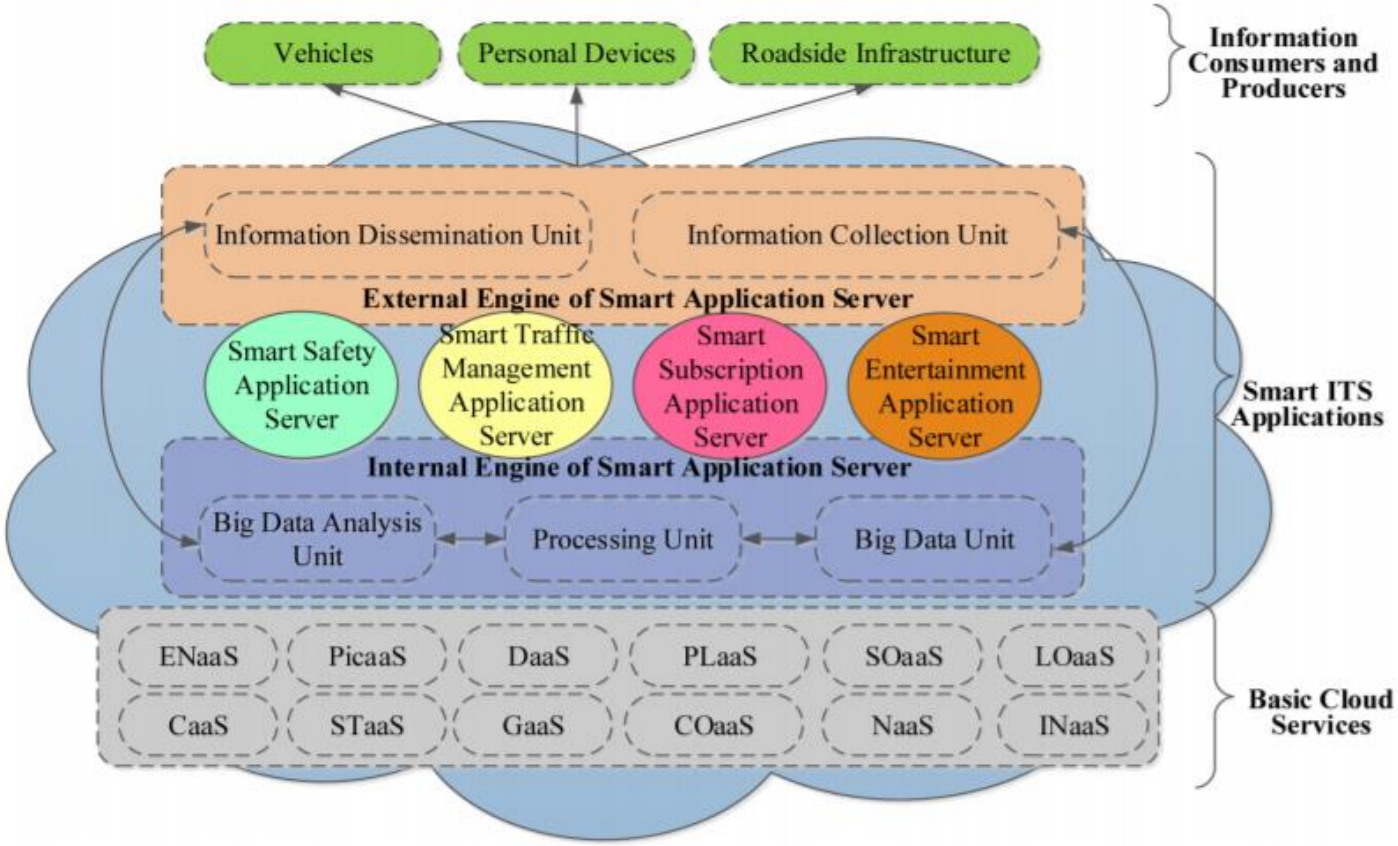
The first element of IoV, are accessed using a reliable ‘connection’ which is the second element of IoV.

The different types of connections are utilized by smart ‘client’ applications which is the third element of IoV. Each client application has service requirements which might be different from other clients. The service requirements of a client are defined in terms of characteristics of a wireless access technology. Therefore, a prioritized preference of wireless access technologies are used by client applications.

Cloud

The first element of IoV, are accessed using a reliable 'connection' which is the second element of IoV.

The different types of connections are utilized by smart 'client' applications which is the third element of IoV. Each client application has service requirements which might be different from other clients. The service requirements of a client are defined in terms of characteristics of a wireless access technology. Therefore, a prioritized preference of wireless access technologies are used by client applications.



The role of cloud computing as three operation levels.

THE CLOUD

A framework is proposed to highlight the role of cloud computing as an element in IoV by utilizing the concept of cloud-based application servers. The framework has three major operation levels including basic cloud services, smart application servers and information consumers and producers.

BASIC CLOUD SERVICES

The basic cloud services include the services offered to smart traffic application servers including Co-operation as a Service (CaaS), Storage as a Service (STaaS), Gateway as a Service (GaaS), Computing as a Service (COaaS), Network as a Service (NaaS), Data as a Service (DaaS). Smart ITS application servers are developed and deployed on a cloud platform which provides basic cloud services to the applications for IoV.

SMART ITS APPLICATION SERVERS

Smart application servers of IoV are divided into four categories including traffic safety, traffic management, service subscription and entertainment. Two processing engines; namely, internal and external engines are considered for smart servers. The internal engine includes big data unit, processing unit for big data and analysis unit of processed big data. All the operations of these three units are performed using the basic cloud services offered at cloud platform. The external engine includes information dissemination unit responsible for end-to-end delivery of services to client applications and information collection unit responsible for in-source data gathering.

INFORMATION CONSUMER AND PRODUCER

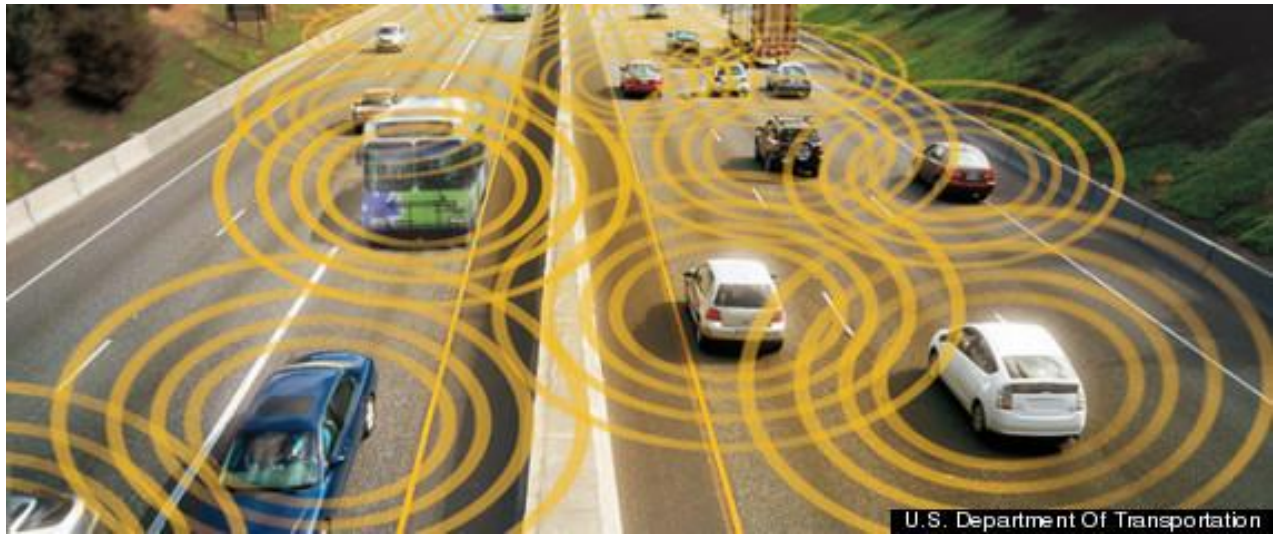
The role of cloud computing makes the 'cloud' one of the important elements in the design and development of IoV. The services offered by the four smart application servers including smart safety, Smart Traffic Management, Smart Entertainment and Smart Subscription are the basis of smartness in IoV.

The primary responsibility of the cloud servers is to process and apply artificial intelligence in real time big traffic data to make intelligent decisions for smart client applications. It would require a Real Time Operating Systems (RTOS) for the activation of IoV services. Google's effort to develop Android-based RTOS for IoV with the help of Open Automobile Alliance (OAA) is one of the good candidates.

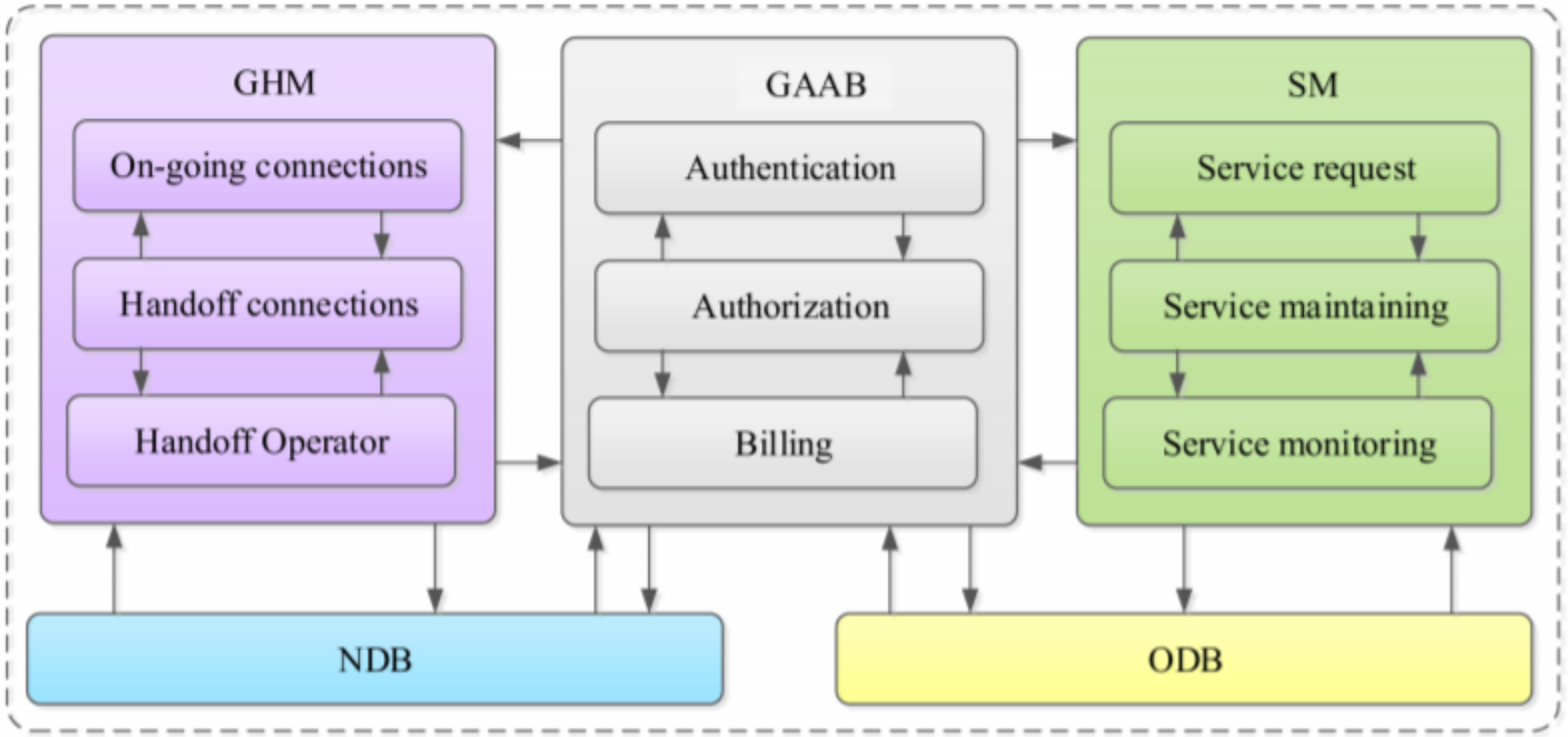
THE CONNECTION

Due to the consideration of different types of networks including VANETs, Wi-Fi, 3G/LTE, and satellite, inter connection among these networks is significantly challenging.

There are two major components of a connection; namely, Third Party Network Inter Operator (TPNIO) and Gateway of Internetworking (GIN). TPNIO is responsible for management of the connection whereas GIN represents the connection.



Both components and a prioritized preference of Wireless Access Technologies (WAT) for connection are described in detail in following.



The logical relationship of the components of TPNIO.

THIRD PARTY NETWORK INTER OPERATOR (TPNIO)

The need of direct Service Level Agreement (SLA) between the operators of the networks is reduced in IoV due to the consideration of TPNIO. The direct SLA is a challenging constraint for any heterogeneous networks. TPNIO enables seamless roaming without compromising the quality and security of the services of network operators.

Global Handoff Manager (GHM)

- The global handoff manager is responsible for performing seamless transfer of on-going communications between any pair of operators of the networks in IoV.

Global Authentication Authorization and Billings (GAAB)

- The GAAB is responsible for verifying vehicle's credentials and granting permissions to access network services. The usage-based pricing of network services is also handled by GAAB.

Service Management (SM)

- SM is responsible for providing and monitoring quality of service offered to vehicles. It helps to deliver guaranteed services to vehicles using service quality agreement.

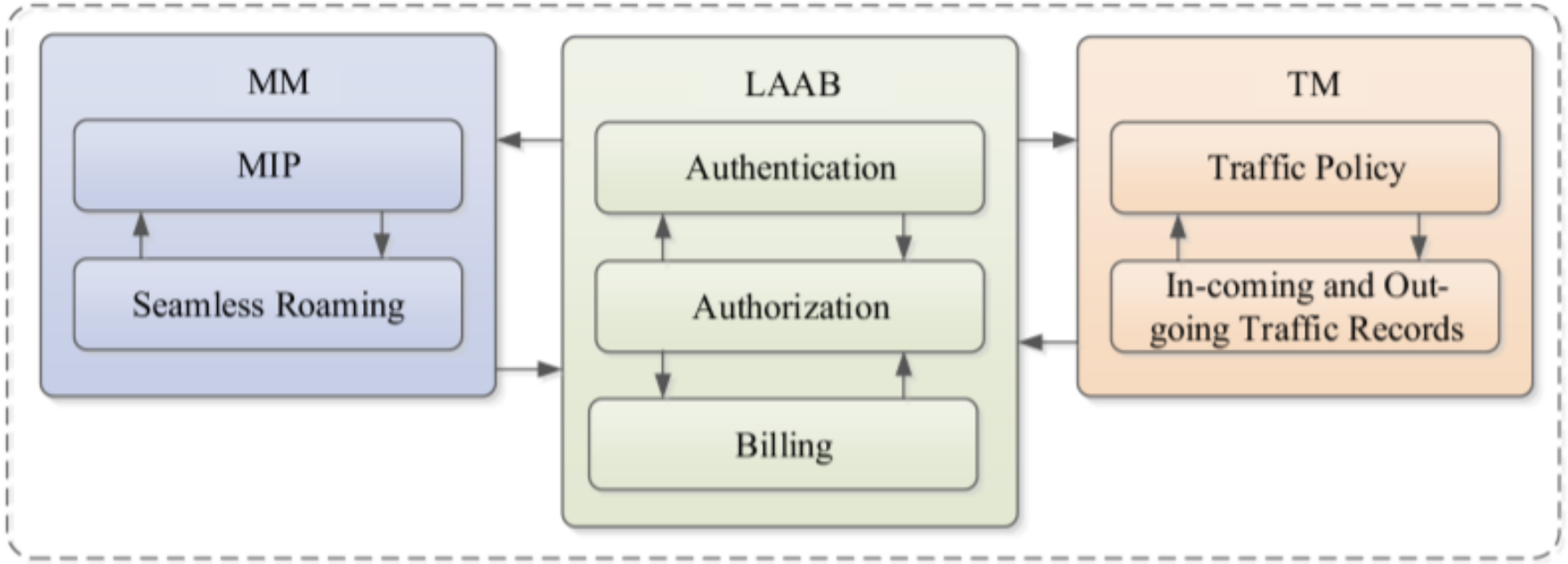
Network Database (NDB)

- NDB is a databased of the registered networks with their technologies and protocols in IoV. The database is utilized to identify a network while establishing communications between the operators of different types of networks.

Operator Database (ODB)

- ODB is a database of the registered operators of the different types of networks in IoV. These operators have SLA with TPNIO due to which the need for direct SLA between operators is not required. The database is utilized to identify operators and their SLAs to provide guaranteed quality of service.

The logical relationship of the components of GIN



GATEWAY OF INTERNETWORKING (GIN)

Due to the heterogeneous network environments in IoV, different wireless access technologies are utilized to establish connections. There are five types of vehicular networks in IoV including V2V, V2R, V2I, V2P, and V2S.

The V2V and V2R networks represents vehicular communications through WAVE. The V2I network represents vehicular communications through Wi-Fi or 4G/LTE [56]. The V2P network represents vehicular personal device communications using CarPlay of Apple or Android system of OAA or Near Field Communication (NFC). The V2S network represents in-vehicle sensor communications through Ethernet, Wi-Fi or Media Oriented System Transport (MOST).

These networks are utilized by client applications to access the services of smart based servers with the help of Gateway of Internetworking (GIN). Each vehicular network has its GIN which coordinates with the TPNIO to establish and maintain a connection.

Mobility Management (MM)

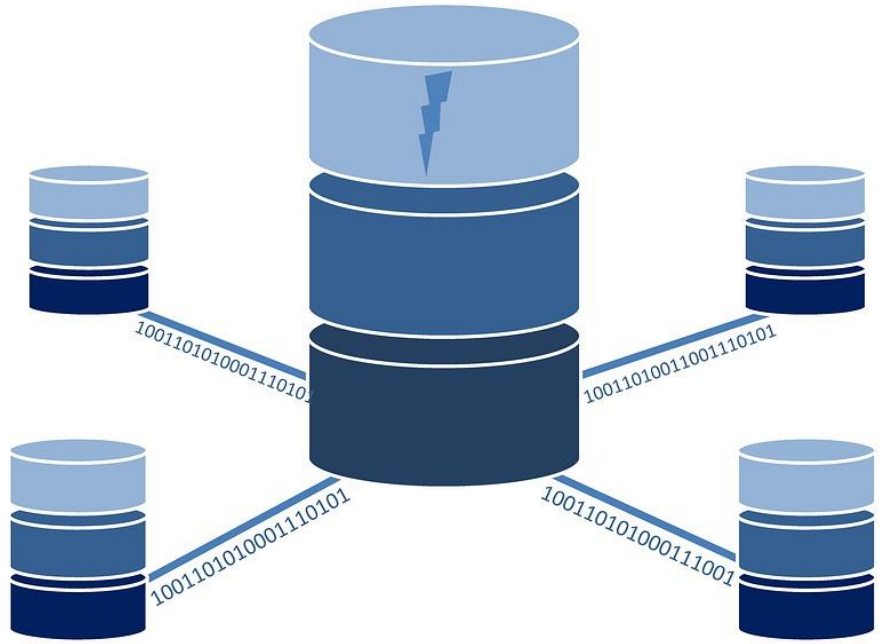
MM is responsible to provide the functionalities related to Mobile IP (MIP). The concepts of Foreign Agent Vehicle (FAV) and Home Agent Vehicle (HAV) are utilized to implement MIP. In IoV, a vehicle registered with a network operator is considered HAV for the operator and FAV for the other operators of the network. The seamless roaming module communicates with GHM to perform roaming operation. The concept of tunneling could be utilized for the conversion of IP versions to avoid the restrictions of using a particular version of IPv4 or IPv6.

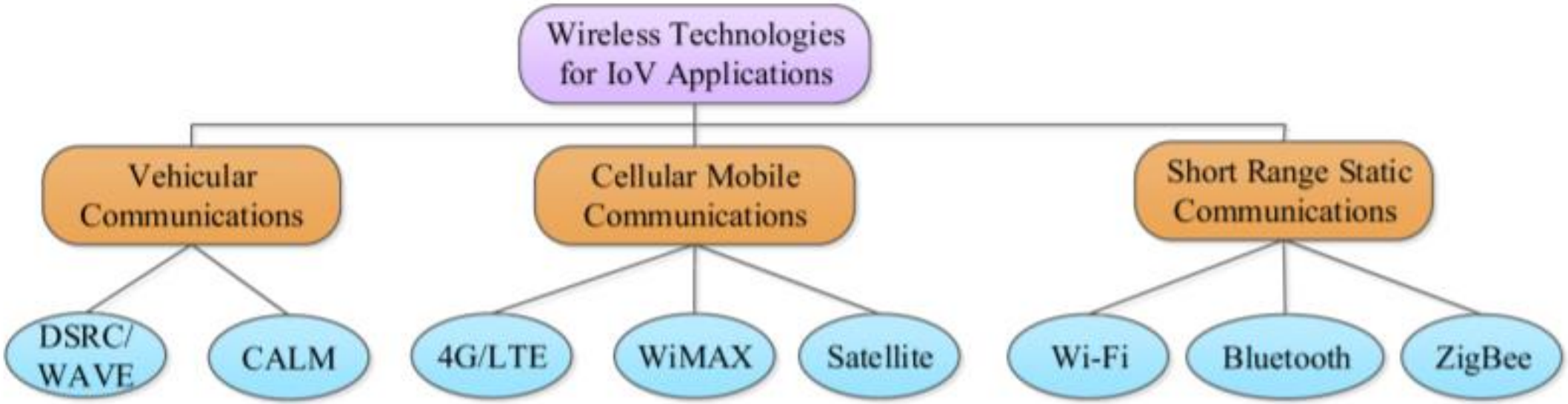
Local Authentication Authorization and Billing (LAAB)

LAAB is responsible to provide authentication, authorization and billing services to HAV which are local users of the networks. It also helps the Global AAB (GAAB) of TPNIO for providing the same services to FAV.

Traffic Management (TM)

TM is responsible to provide network traffic monitoring services by implementing the policies of the network. The policies may differ from network to network. The monitoring helps the network operators to provide quality of services to the client applications. The monitoring is based on the analysis of usage of traffic data as well as the live traffic data of connections.





The classification of WAT for the applications of IoV.

PRIORITIZED PREFERENCE OF WIRELESS TECHNOLOGIES

The WAT are divided into three categories; namely, vehicular, cellular mobile and small range static communications based on the communication network where WAT are utilized. These technologies have been developed for different types of communication networks.

A prioritized preference of wireless technologies is derived in Table based on the six parameters which effectively characterize these technologies. The six significant parameters of WAT include data rate, communication range, mobility support, communication delay, security support and scalability.

Property	**Prioritized Preference based on the Property** *High* → *Low*
Data Rate	Wi-Fi(a/b/g/n) → 4G/LTE → WiMAX → DSRC/WAVE → CALM → Bluetooth → ZigBee
Communication Range	WiMAX → 4G/LTE → DSRC/WAVE → CALM → Wi-Fi(a/b/g/n) → ZigBee → Bluetooth
Mobility Support	DSRC/WAVE → CALM → WiMAX → 4G/LTE → Wi-Fi (a/b/g/n) → ZigBee → Bluetooth
Communication Delay	DSRC/WAVE → CALM → 4G/LTE → ZigBee → Wi-Fi (a/b/g/n) → Bluetooth → WiMAX
Security Support	4G/LTE → WiMAX → Wi-Fi (a/b/g/n) → ZigBee → Bluetooth → CALM → DSRC/WAVE
Scalability	WiMAX → 4G/LTE → DSRC/WAVE → CALM → Wi-Fi (a/b/g/n)→ ZigBee → Bluetooth

CLIENT

The services of smart cloud-based servers are utilized by the ‘client’ applications of vehicles with the help of a network connection. The client applications or clients in IoV can be broadly divided into two categories; namely, safety and management oriented, and business oriented.

The taxonomy of client applications of IoV