A Review on IoT in Automotive Sector

Chandrashekar C[1], Darshith Karthikeyan[2], Franklin P[3], Darshan B[4] and Abhishek C[5]

[1] Assistant professor, Department of ECE, BNMIT
[2]Department of ECE, BNMIT
[3]Department of ECE, BNMIT
[4]Department of ECE, BNMIT
[5]Department of ECE, BNMIT

Abstract

The Internet of Things (IoT) is a new Internet wave that is expected to change our lives. The Internet has connected people and now connects 'Things' to create seamless communication and intelligent integration. IoT is a disruptive technology that has great potential to change the world and change the way we live. It uses low-cost devices and sensors connected to the Internet that create new opportunities. Not so long ago, the IoT concept in the automotive sector was seen as a scientific concept of the future and today we are already seeing opportunities for connected vehicles, non-motorized vehicles and the use of IoT in the automotive system covering parking, environment, procurement and transport regulatory bodies. This paper discusses the emergence and development of the Internet of Things in the automotive sector to provide an overview of various areas such as Connected Car services / applications, Vehicle communications, IoT in Intelligent Transportation, IoT based Supply Chain Management in Automotive Industry and New Generation Vehicles, where progress is being made forward visible.

***Keywords*: Internet of things (IOT), Automotive industry, connected Cars.**

Introduction

Currently, with the rapid development of society, the concept of IoT has expanded to various industries, and gained acquired products and services to some extent. The concept of IoT will be introduced in automotive construction to achieve a higher level of automotive information, which is imminent, so the concept of "automotive manufacturing" has emerged. The automotive production of "IoT" is a crossroads in the field of the two largest IoT and smart cars in the emerging strategic industries. And it will be a new trend. Gathers the latest achievements in the field of procurement management and information management and RFID technology a unique ability to collect real-time data together, and in combination with other information technologies used throughout the automotive industry, its growth will play an important role in promoting the future of automotive, low cost , energy saving, environmental protection and efficient after-sales service. Manufacture of automotive IoT refers to the introduction of storage vehicles, attaching to each end point is an electronic tag, tracking and monitoring of a series of processes including car parts production, finished products, finished product, finished product safety and quality inspection, storage and packaging, and then use, after-service service and recycling. It recognizes the new automotive information system by collecting and complying with a different need for the question that appears in the process related to the continuous monitoring and treatment that operates on the information network platform. Automotive manufacturing "IoT" connected to a network of auto parts manufacturer, chip manufacturer, network hardware, system integration, software solution providers, etc.

Architecture of IOT

Internet of Things (IoT) includes a large number of smart devices connected to a wide Internet network with the help of various communication technologies. Most of these technologies are wireless in a way. This makes the composition very complex and difficult to manage. Therefore, the construction of buildings is necessary.

Composition is the structure of the network's and the organisation's specifications and functions, its terms and conditions of operation, and the data formats used in its operation.

IoT development depends on the technology used, the application areas, and the business features. There are various IoT structures available for IoT devices. However, "5 Layer Architecture is considered a well-planned IoT architecture".

Five layer IoT Structure: Perception layer: The comprehension layer is the basis of IoT, the visual interface between the global layer and the knowledge world. It uses radio frequency detection technology, bar code technology, sensor technology, placement technology, or other sample information technology to complete data collection, and with the help of visual control by the actuator, to use infection control between the visual field and the information area. Its main components include a two-sided code label, code-reader-writer, RFID tags and RFID-reader, cameras, and all kinds of sensors. Therefore, the IoT vision layer has the essential functions of seeing the data and collecting the actual data, the help needed to complete the bottom of the control object. Therefore, the main function of the IoT visual field is information and data collection, where necessary, to help complete visual control elements. ł Five-layer network access layer: The network access layer consists mainly of a base station node and a network access gateway, complete network control and data integration for each node in the visual layer, or complete data transfer from the above layers (network transfer or application layer). When the node layer nodes complete the connection, the node layer nodes need to load data, and send the data to the base station node. The base station node will receive the data, and complete the connection with the network transfer layer through the access gateway. When the application layer and network layer need to reduce data, the base station node sends data to each node in the view layer behind the network access gateway that receives data from the network transfer layer, and completes the data transfer and connection between layer detection and network transfer layer. Current access methods in the network access layer mainly include WIFI, Ad hoc, Mesh, ZIGBEE, industrial bus, detect data collection with various cognitive tools, or perform initial process and network access. Layer Five-layer network transfer layer: The network transfer layer is widely used to identify transfers and information exchanges, providing a network transfer with the basic needs and services required for many types, including satellite communication network, cellular fiber network and network and local network and network. and so on. It is a problem in the network layer that neutral access and seamless integration between different networks and communication systems, and how you can build transmission and exchange capabilities by end-point. Five-layer application support layer: With support for cloud computing technology, middleware technology, database technology, expert system etc. types of app sharing intelligently and interchangeably. Layer Five-layer application presentation layout: Application presentation layout function for the development of various Io-based applications in the processing of application support framework data, and utilizes multimedia technology, real-world, human interface to create an intuitive application interface between IOT , current use and use of all kinds of intelligent information.

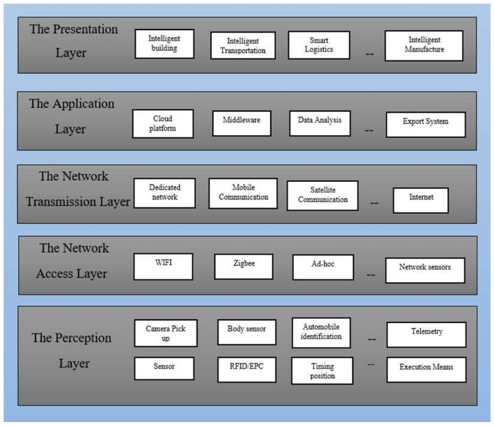

Figure 1: Five layer design of IoT

The IOT gateway hierarchy

The IOT gateway supports a variety of processes for communicating data types between different sensors, which can detect changes in the data format that communicates between a variety of sensors, to integrate uploaded data formats. At the same time, the acquisition or control command that accesses the visual network is designed to generate messages that meet specific device communication processes. The basic structure of the Io port as shown in Figure 2, including application layer, network layer, analysis layer (protocol modification and protocol process layer), visual layer

Application layer: Application layer will see the automatic management of the hearing device, as well as the management of each sub-network. (2) Network coverage: Network coverage provides a variety of visual interface for access network. With a portable environment or a fixed network environment, you can use a variety of access methods. With the nature of a particular network connection, it can be used in single access mode. Network coverage includes 197 different types of network communication with the Internet to build a network, which is the most common area of network communication, such as 2g, 3g, 4g network or Internet Internet, etc. (3) Analysis layer: The analysis layer will use standard protocol modification and data format analysis, including protocol adapter and compliance module. The protocol adapter module defines a standard access interface, which ensures that different access protocols can be a data-linked format. The protocol modification protocol will be integrated to integrate standard data downloaded from the protocol adapter, extracting data from the network layer to standard format. It also provided a modification of the protocol from recognition to the communication network, namely the implementation of the ZigBee protocol to the change of the TCP / IP protocol. (4) Sensitive access layer: An intuitive access layer will complete network control and physical access to notes, and be accompanied by multiple sensor network technologies to achieve separate access to the network recognition process.

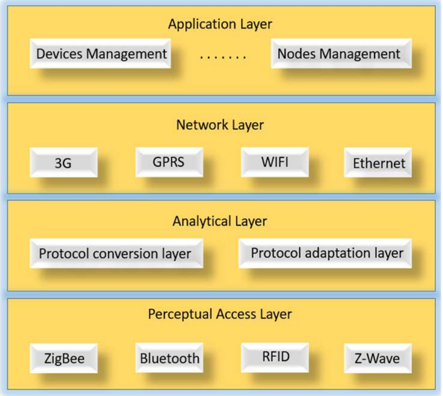

Figure 2: Gateway layers

The gateway hardware structure

IoT gateway is a bridge that connects the visual network and the access network, can support a variety of sensors (such as ZigBee, 6LoWPAN, RS485, CAN) and access method (such as cable, WLAN, GPRS, 3G), and provide a data format in Bumb. -middleware or application, in order to protect a separate sensor network and access network, make applications require attention only in the data processing application area. This paper adopts a modular design concept and embedded system technology to design an Io gate, IOT gate design is shown in Figure 3. The processor module is a basic gateway, which uses compliance, management, security and other data processing and storage features. The zigBee module detects visible or collective global data collection, be it a combination of sensor network nodes, RFID reader, video recording equipment, GPS, etc. With the network access module, the gateway will enter the WAN via a channel including cable (Ethernet, ADSL, FTT), wireless (WLAN, GPRS, 3G, satellite).

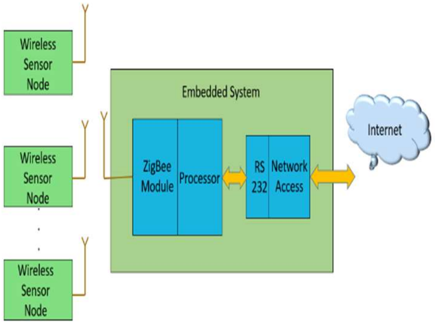

Figure 3: Gateway hardware

Classification of IoT

Sensible layout outlines what is happening in the IoT region and is integrated based on layer formation. An important design phase for IoT is the layer of information. It integrates data using sensors, which are IoT driving indicators. There are several categories of sensors used in collected IoT systems. The incomparable sensor available today is the phone. The real PDA has a variety of sensors included in it such as a circuit sensor, advanced sensors such as the accelerometer, whirligig, camera, light sensor, receiver, location sensor and magnetometer. This round is firmly entrenched in various IoT applications. Various types of sensors are now being used as sensors to monitor temperature, pressure, humidity, clinical parameters of the body, composite and chemical substances, and neural signals. Stable nerves are infrared nerves that start before cells. They are used extensively in a variety of IoT applications: IR cameras, enhancement areas, article closure testing, the presence of smoke and fumes, and as deterioration sensors. Such applications (or whatever so-called fog for app applications) usually transfer and review data before sending it to the association. Such units often have a small amount of temporary accumulation, minimal handling of the unit, and safety features. Various items pass over the organization using a different program of shows and standards. The most notable visual advances of short-term arrivals in low power shows are Radio Frequency Identification and Near Field Communication. For medium access, Bluetooth, ZigBee, and WiFi. Communication in the IoT world requires frameworks for exhibition frameworks and organizations.

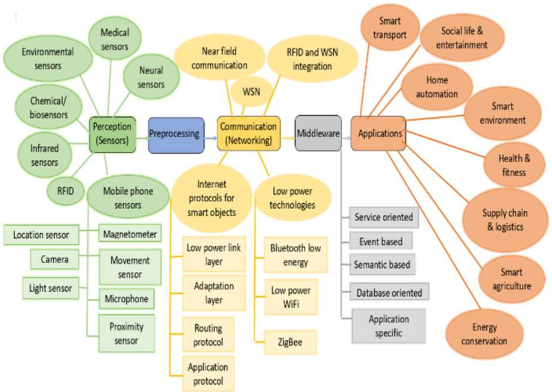

Figure 4: Classification of IoT

Literature Survey

There are many pages on the Internet of Things before. This paper looks at each layer in the IoT stack, which is why the show additionally ensures additional transitions. Part of the design similarly considers appropriate models for forward thinking, for example, mist management, which has not yet been considered. In addition, these audits effectively plan for progress based on the design layer they have with them. Other than that, I asked for an organizational layer and tried to integrate all the continuity used in IoT architecture. This framework is more complete, fragmented, and recognizable when it comes to various nearby research studies. This looks at different types of middleware development alike and considers a large collection of applications that combine smart homes, clinical considerations, connectivity, transportation, agriculture, environment, large city networks, and without compromising ecosystem power. There are no other tests in this space that create countless improvements and their application.

Sensors and Actuators

Currently, modern automotive designs can be made using a variety of sensors. This is programmed in the car engine to identify and solve potential problems such as repairs, support, etc. Sensors used in cars will check the performance of the car. The owner of the car does not know how many sensors are used in their cars. There are several major sensory organizations available worldwide, which can offer a new solution to customers. In modern cars, sensors are used to detect and respond to change conditions inside and outside a car. So that passengers can travel safely and safely. By using these sensory information we can increase comfort, efficiency, and safety.

Mass Air Flow Sensor

The MAF or Mass air sensor is one of the most important sensors used in automobiles. This sensor is used in a car engine. This sensor can be controlled by a computer and can detect air congestion in the engine. If the operation is stopped, the operation of the vehicle will be stopped. In addition, fuel consumption will be higher. These sensors are divided into two types namely vane meter and hot wire.

Engine Speed Sensor

The engine speed sensor in the car can be connected to the crankshaft. The main purpose of this sensor is to monitor the rotational speed of the crankshaft. For fuel injection and engine time control. There are various ways for a car engine to stop unexpectedly. So this sensor will stop that for motorists.

Coolant Sensor

Cooling sensor is the most important sensor used in cars. Because the computer depends on the input sensor to control all operations. For example, Turn on / off the EFE system (Early Fuel Evaporation), delay, refresh, EGR flow, and canister purge. Normally, this sensor can be connected to the board. If the sensor fails, then there will be some suspension indicators, such as poor gas mileage, etc. Therefore, the sensor condition should be checked for error. If it is damaged, then it will be a problem.

Manifold Absolute Pressure Sensor

The shortest time for maximum total compression is MAP. The primary function of this sensor in a car is to monitor engine load. Most importantly, it measures the difference between most pressures. This can be achieved by external pressure by the car to ensure that the car's engine is able to get fuel depending on the change within the pressure.

Throttle Position Sensor

Automotive sensor mainly uses carburetion & electronic fuel injection (EFI) response. Informs the computer about the opening rate of the powder and the location of the related throttle. This sensor has flexible resistance elements, which are used to change resistance as the pinch opens.

Vehicle Speed Sensor

As the name suggests, this VSS sensor has the ability to verify the speed of car wheels. It is a type of tachometer. This sensor is mounted inside an anti braking system known as ABS. In addition, the sensor output is also used by the odometer to read the speed of the car to control the gears according to the speed of the car.

Communication

Bluetooth

Essential IoT communication protocols / essential technologies. Bluetooth, which is very important in the computer and in many consumer product markets. Expected to be the key to wearable products in particular, it also connects to IoT even with a smartphone in most cases. The new Bluetooth Low-Energy (BLE) -

or Bluetooth Smart, as it is now branded - is an effective alternative to IoT applications. Importantly, while providing the same distance as Bluetooth it is designed to offer significantly reduced power consumption.

Zigbee

ZigBee is similar to Bluetooth and is widely used in industrial settings. It has some important advantages in complex systems that offer low power performance, high security, durability and height and are well-suited for the optimal use of wireless control and sensory networks in IoT.

Z-Wave

Z-Wave is a powerful low-power RF IoT communication technology designed for home automation of products such as light and sensor controls among many other devices.
Z-Wave uses a simpler rule than others, which can allow for faster and easier development, but the only chip maker is Sigma Designs compared to many other wireless technology sources like ZigBee and others.

Wi-Fi

WiFi connectivity is one of the most popular IoT communication protocols, often a clear choice for many developers, especially when providing WiFi access within the home environment within LANs.
There is a wide range of infrastructure available as well as offering fast data transfer and the ability to handle very high quality data.
Currently, the most common standard of WiFi used in many homes and businesses is 802.11n, which offers hundreds of megabytes per second, which is suitable for file transfers but can be very powerful for most IoT systems.

Cellular

Any IoT system that needs to be operated over long distances can use the power of GSM / 3G / 4G mobile connectivity. While mobile phones are obviously capable of sending very high-quality data, especially 4G, the cost and power consumption will be much higher for most applications. But it would be great for low-bandwidth data projects that will send the lowest data over the Internet.

NFC

NFC (Near Field Communication) IoT technology. It enables easy and secure communication between electronic devices, and especially smartphones, allowing consumers to make transactions where the unwanted person is physically present.
It helps the user to access digital content and connect electronic devices. It basically expands the capabilities of the card communication technology and enables devices to share information at a distance of less than 4cm.

LoRaWAN

LoRaWAN is one of the most popular IoT Technology applications, aimed at broadband (WAN) applications. LoRaWAN's design for providing low-power WANs with features that are specifically needed to support low-cost secure communications in IoT, smart city, and industrial applications.
Specifically it meets the requirements of low power consumption and supports large networks with millions of devices, data rates range from 0.3 kbps to 50 kbps.

Middleware

Middleware works as an agent between service providers (IoT devices) and service buyers (business applications). A layer of software that stays between apps and objects. It is a mediator interface that enables communication between the Internet and 'objects'. It hides the differences between devices, components and IoT system technology. Middleware provides solutions to the problems they face on a regular basis, such as collaboration, security and trust. The following are the key features of middleware, which improve device performance.

Flexibility

This feature helps to establish better-quality connectivity, which improves the communication between applications and things. There are different kinds of flexibility (e.g., response time, faster to evolve and change).

Transparency

Middleware hides many difficulties and architectural information details from both the application and the object sides, so that the two can communicate with minimum knowledge of either side.

Interoperability

Allows two sets of applications on interconnected networks to exchange data and services meaningfully with different assumptions on protocols, data models, and configurations.

Platform portability

An IoT platform should be capable to communicate from everywhere, anytime with any device. Middleware runs on the user side and can provide independence from network protocols, programming languages, OSs and others.

Re-usability

This feature makes designing and developing easier by modifying system components and assets for specific requirements, which results in cost efficiency.

Maintainability

Maintainability has a fault tolerance approximation. Middleware performs maintainability efficiently and extends the network.

Security

Middleware should provide different security measures for ubiquitous applications and pervasive environments. Authentication, authorisation and access control helps in verification and accountability.

Characteristics of open source IoT middleware.

An open source IoT platform should be error-tolerant and widely available. It has the following features: No vendor access, and comes with a strong integration of a wide range of business tools, applications, products and programs built and delivered by various organizations and vendors. Marketing time, reduces risk and increases quality The acceptance of openware middleware improves interoperability with other business applications due to the ability to reuse recommended software stacks, libraries and specific items.

IoT middleware platforms should support open APIs, cloud deployment models, and are widely available.

It should support open data formats such as RestAPI, JSON, XML and Java, and be freely available

The IoT middleware platform should support multiple and diverse devices, and be compatible with hardware data recognition.

Moving to any new platform or program should be seamless. It should be possible to accept or combine any solution.

The data model must be distributed and expanded, providing the availability and scalability of the system.

The IoT middleware platform should support major communication protocols such as MQTT, CoAP, HTTP, WebSockets, etc.

The IoT middleware platform should support various security features such as encryption, authentication, authentication and auditing.

It should support technologies such as M2M applications, real-time statistics, machine learning, artificial intelligence, statistics, visibility and event reporting.

IoT middleware architecture

The middleware mediates between IoT data producers and the consumers. APIs for interactions with the middleware are based on standard application protocols. API endpoints for accessing the data and services should be searchable via an open catalogue, and should contain linked metadata about the resources.

The device manager communicates messages to the devices. The database needs to access and deliver messages to the devices with minimum latency.

Data processing involves data translation, aggregation and data filtering on the incoming data, which enables real-time decision making at the edge. The database needs to support high-speed reads and writes with sub-millisecond latency. It helps in performing complex analytical computations on the data.

The IoT data stream normalises the data to a common format and sends it to enterprise systems. The database needs to perform the data transformation operations efficiently.

Middleware supports the authentication of users, organisations, applications and devices. It supports functionalities like certificates, password credentials, API keys, tokens, etc. It should also support single sign-on, time based credentials, application authentication (via signatures) and device authentication (via certificates).

Logging is necessary for both system debugging as well as auditing. Middleware manages the logging of system debugging and auditing details. It helps to track the status of the various services, APIs, etc, and administers them.

Key open source IoT middleware platforms

Holistically, an IoT implementation covers data collection and insertion through sensors as well as giving control back to devices. The different types of IoT middleware are categorised as:

Application-centric (application and data management)

Platform-centric (application enablement, device management and connectivity management)

Industry-specific (manufacturing, healthcare, energy and utilities, transportation and logistics, agriculture, etc)

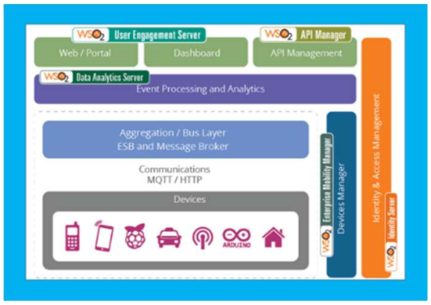

Figure 5: Reference model for IoT platform modules

Key challenges and Problems

Although IoT plays an important role in various aspects of life, there are few issues and challenges to be addressed. This research paper addresses the most common issues such as an increase in the number of connected devices, different environments, increased data retention, privacy and security. Various challenges related to standardization, architecture, increased security and safety are discussed in the paper.

A. Standardization is one of the most important and major challenges in the field of IoT application and is the backbone of IoT development. The most important bodies for making policies such as ETSI, ITU, IETF, IEEE, etc. It is involved in the IoT development framework. A different configuration function is different to provide open and seamless work. There are some problems with integration with different standards so that they do not change. All of these challenges need to be considered in the future to be integrated into different types of IoT technologies.

B. Architecture In the IoT System IoT structures have played an important role in making the integration of different technologies. It is used to support service continuity. The most important and major challenge for the IoT system is to implement integrated integrated system construction. The basic requirement for this is to build equality, openness, and honesty in all forms of nature. It should enable shortcuts, easy and awesome integration and automation on IoT. IoT architecture includes a variety of group types such as hardware, software, network, and general.

C. Decreased balance in IoT refers to the addition of new devices and services to existing applications. It supports a large number of devices with various problems. Installing a scalability mechanism must be structured and structured. The biggest problem in separation is installing the device and new features in the IoT.

D. Security is embedded in most IoT devices to connect devices and objects. There are many types of attacks that can disable our network, data attacks and access to personal information. It is difficult to provide security with current technology.

Applications of IOT.

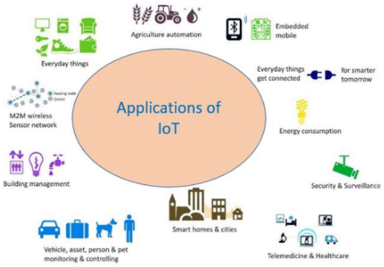

Figure 6: Applications of IoT

The IoT plays an important and diversified role in all areas of everyday life. Major IoT application domain includes smart energy, city, health, smart transport, agriculture, etc.

Smart city

IoT plays an important part to expand the smartness of the city that contains submissions to monitor the parking space obtainability in the cities, monitor the sensitive area, monitoring of vehicles, weather monitoring system, detection of waste container, intelligent highway warning message and unexpected events like accident and traffic jam. Smart city application includes smart parking, urban maps, smart lighting. This uses an RFID, wireless sensor network and single sensors as the IoT element then the bandwidth of the application starts from insignificant to huge.

Smart agriculture and smart water

IoT is helping to monitor and improve the strength of the work in agriculture by measuring the soil dampness and bole diameter to manage and sustain the vitamins of the agriculture product. It controls the climate condition to exploit the creation of the fruits, vegetables and the quality of it. It is used to study the condition of the weather to forecast the ice information, rain, snow or wind. is also used in water management to monitor water appropriateness in the rivers, water quality (drinkable/non drinkable) and water level in the various rivers and dams.

Retail and Logistic

Retail and supply chain use IoT to monitor the storage conditions with the supply chain. The tracking of the product and payment is done based on RFID and WSN applications in the IoT. In the IoT, logistics includes the shipment quality, item location, and tracking, etc. The element of the IoT used the RFID, sensors and single sensor.

Healthcare

In the healthcare industries, IoT is used for tracking the objects, identity, sensing, and authentication of the people. The process of tracking is used for the identification of the person or object in motion. This is used to monitor the flow of the patient and authenticate the patient in the hospital to reduce the medical record maintenance and prevent mismatching. In this, the application includes the various types of telemedicine solutions with a prescription. In the current trend, the elements of the IoT healthcare domain are RFID, NFC, WSN, Wi-fi, bluetooth, etc. It is used to improve the monitoring methods of the function like temperature, heart rate, and glucose.

Security

IoT plays an important role in security domain. Security is a most important aspect of the IoT application which is used in the all layers of IoT protocol. Few parameters are like limited access control, liquid presence, radio activity and explosive, etc. Limited access control is used to block unauthorized access to restricted areas. Liquid detection in the data center and warehouse uses the liquid presence. The application of radiation is used to measure the radiation of nuclear and monitor the environment.

Conclusion

The purpose of this review paper was to gain knowledge about the IoT architecture, middleware, device management, data management, sensors used in automobiles, communication protocols and applications of IoT in automobiles to develop an IoT system that can be merged with the infotainment system of automobile as an important add on feature for further betterment and enhancement in the field of automotive industry.

References

[1] S. A. Al-Qaseemi, H. A. Almulhim, M. F. Almulhim and S. R. Chaudhry, "IoT architecture challenges and issues: Lack of standardization," 2016 Future Technologies Conference (FTC), 2016, pp. 731-738, doi: 10.1109/FTC.2016.7821686.

[2] T. Yashiro, S. Kobayashi, N. Koshizuka and K. Sakamura, "An Internet of Things (IoT) architecture for embedded appliances," 2013 IEEE Region 10 Humanitarian Technology Conference, 2013, pp. 314-319, doi: 10.1109/R10-HTC.2013.6669062.

[3] S. Krčo, B. Pokrić and F. Carrez, "Designing IoT architecture(s): A European perspective," 2014 IEEE World Forum on Internet of Things (WF-IoT), 2014, pp. 79-84, doi: 10.1109/WF-IoT.2014.6803124.

[4] C. Zhong, Z. Zhu and R. Huang, "Study on the IOT Architecture and Gateway Technology," 2015 14th International Symposium on Distributed Computing and Applications for Business Engineering and Science (DCABES), 2015, pp. 196-199, doi: 10.1109/DCABES.2015.56.

[5] J. Ren, H. Guo, C. Xu and Y. Zhang, "Serving at the Edge: A Scalable IoT Architecture Based on Transparent Computing," in IEEE Network, vol. 31, no. 5, pp. 96-105, 2017, doi: 10.1109/MNET.2017.1700030.

[6] A. H. Ngu, M. Gutierrez, V. Metsis, S. Nepal and Q. Z. Sheng, "IoT Middleware: A Survey on Issues and Enabling Technologies," in IEEE Internet of Things Journal, vol. 4, no. 1, pp. 1-20, Feb. 2017, doi: 10.1109/JIOT.2016.2615180.

[7] M. A. A. da Cruz, J. J. P. C. Rodrigues, J. Al-Muhtadi, V. V. Korotaev and V. H. C. de Albuquerque, "A Reference Model for Internet of Things Middleware," in IEEE Internet of Things Journal, vol. 5, no. 2, pp. 871-883, April 2018, doi: 10.1109/JIOT.2018.2796561.

[8] Ji, Z., Ganchev, I., O'Droma, M., Zhao, L., & Zhang, X. (2014). A Cloud-Based Car Parking Middleware for IoT-Based Smart Cities: Design and Implementation. Sensors, 14(12), 22372–22393. Doi: 10.3390/s141222372.

[9] R. T. Tiburski, L. A. Amaral, E. De Matos and F. Hessel, "The importance of a standard security architecture for SOA-based Iot middleware," in IEEE Communications Magazine, vol. 53, no. 12, pp. 20-26, Dec. 2015, doi: 10.1109/MCOM.2015.7355580.

[10] M. A. Razzaque, M. Milojevic-Jevric, A. Palade and S. Clarke, "Middleware for Internet of Things: A Survey," in IEEE Internet of Things Journal, vol. 3, no. 1, pp. 70-95, Feb. 2016, doi: 10.1109/JIOT.2015.2498900.

[11] Huo Y, Tu W., Sheng, Z., & Leung, V. C. M. (2015). A survey of in-vehicle communications: Requirements, solutions and opportunities in IoT. 2015 IEEE 2nd World Forum on Internet of Things (WF-IoT).

[12] Ma D, Lan G., Hassan, M., Hu, W., & Das, S. K. (2019). Sensing, Computing, and Communications for Energy Harvesting IoTs: A Survey. IEEE Communications Surveys & Tutorials, 1–1.

[13] Abdur Rahim, M., Arafatur Rahman, M., Rahman, M. M., Taufiq Asyhari, A., Zakirul Alam Bhuiyan, M., & Ramasamy, D. (2020). Evolution of IoT-enabled connectivity and applications in automotive industry: A review. Vehicular Communications, 100285.

[14] Rasheed, I., & Hu, F. (2020). Intelligent super-fast Vehicle-to-Everything 5G communications with predictive switching between mmWave and THz links. Vehicular Communications, 100303.

[15] Keertikumar M., Shubham M., & Banakar, R. M. (2015). Evolution of IoT in smart vehicles: An overview. 2015 International Conference on Green Computing and Internet of Things (ICGCIoT).

[16] International Journal of Advanced Research in Computer and Communication Engineering Vol. 1, Issue 7, September 2012.

[17] Jonathan Hui, PhD, Arch Rock Corporation David Culler, PhD, University of California, Berkeley Samita Chakrabarti, IP Infusion January 2009.

[18] Frank, R., Bronzi, W., Castignani, G., & Engel, T. (2014). Bluetooth Low Energy: An alternative technology for VANET applications. 2014 11th Annual Conference on Wireless on-Demand Network Systems and Services (WONS).

[19] Naik, D. R., Das, L. B., & Bindiya, T. S. (2018). Wireless Sensor networks with ZigBee and WiFi for Environment Monitoring, Traffic Management and Vehicle Monitoring in Smart Cities. 2018 IEEE 3rd International Conference on Computing, Communication and Security (ICCCS).

[20] Klaina, H., Picallo, I., Lopez-Iturri, P., Astrain, J. J., Azpilicueta, L., Aghzout, O, Falcone F. (2020). Aggregator to Electric Vehicle LoRaWAN based.

[21] A. Mavromatis, C. Colman-Meixner, A. P. Silva, X. Vasilakos, R. Nejabati and D. Simeonidou, "A Software-Defined IoT Device Management Framework for Edge and Cloud Computing," in IEEE Internet of Things Journal, vol. 7, no. 3, pp. 1718-1735, March 2020, doi: 10.1109/JIOT.2019.2949629.

[22] Y. -B. Lin et al., "EasyConnect: A Management System for IoT Devices and Its Applications for Interactive Design and Art," in IEEE Internet of Things Journal, vol. 2, no. 6, pp. 551-561, Dec. 2015, doi: 10.1109/JIOT.2015.2423286.

[23] J. D. C. Silva, J. J. P. C. Rodrigues, K. Saleem, S. A. Kozlov and R. A. L. Rabêlo, "M4DN.IoT-A Networks and Devices Management Platform for Internet of Things" in IEEE Access, vol. 7, pp. 53305-53313, 2019, doi: 10.1109/ACCESS.2019.2909436.

[24] L. Bracciale, P. Loreti, A. Detti, R. Paolillo and N. B. Melazzi, "Lightweight Named Object: An ICN-Based Abstraction for IoT Device Programming and Management," in IEEE Internet of Things Journal, vol. 6, no. 3, pp. 5029-5039, June 2019, doi: 10.1109/JIOT.2019.2894969.

[25] F. A. Kraemer, D. Palma, A. E. Braten and D. Ammar, "Operationalizing Solar Energy Predictions for Sustainable, Autonomous IoT Device Management," in IEEE Internet of Things Journal, vol. 7, no. 12, pp. 11803-11814, Dec. 2020, doi: 10.1109/JIOT.2020.3002330.

[26] H. Zhang, M. Babar, M. U. Tariq, M. A. Jan, V. G. Menon and X. Li, "SafeCity: Toward Safe and Secured Data Management Design for IoT-Enabled Smart City Planning," in IEEE Access, vol. 8, pp. 145256-145267, 2020, doi: 10.1109/ACCESS.2020.3014622.

[27] S. Wang, J. Yuan, X. Li, Z. Qian, F. Arena and I. You, "Active Data Replica Recovery for Quality-Assurance Big Data Analysis in IC-IoT," in IEEE Access, vol. 7, pp. 106997-107005, 2019, doi: 10.1109/ACCESS.2019.2932259.

[28] Q. Doan, A. S. M. Kayes, W. Rahayu and K. Nguyen, "Integration of IoT Streaming Data With Efficient Indexing and Storage Optimization," in IEEE Access, vol. 8, pp. 47456-47467, 2020, doi: 10.1109/ACCESS.2020.2980006.

[29] S. Valtolina, L. Ferrari and M. Mesiti, "Ontology-Based Consistent Specification of Sensor Data Acquisition Plans in Cross-Domain IoT Platforms," in IEEE Access, vol. 7, pp. 176141-176169, 2019, doi: 10.1109/ACCESS.2019.2957855.

[30] Y. Kang, I. Park, J. Rhee and Y. Lee, "MongoDB-Based Repository Design for IoT-Generated RFID/Sensor Big Data," in IEEE Sensors Journal, vol. 16, no. 2, pp. 485-497, Jan.15, 2016, doi: 10.1109/JSEN.2015.2483499.

[31] Ahmed, A. I. Bhatti and M. Iqbal, "Virtual Sensors for Automotive Engine Sensors Fault Diagnosis in Second-Order Sliding Modes," in IEEE Sensors Journal, vol. 11, no. 9, pp. 1832-1840, Sept. 2011, doi: 10.1109/JSEN.2011.2105471.

[32] W. J. Fleming, "New Automotive Sensors—A Review," in IEEE Sensors Journal, vol. 8, no. 11, pp. 1900-1921, Nov. 2008, doi: 10.1109/JSEN.2008.2006452.

[33] R. Lovas, A. C. Marosi, M. Emödi, Á. Kisari, E. Simonyi and P. Gáspár, "PaaS-Oriented IoT Platform with Connected Cars Use Cases," 2018 International Conference on Sensor Networks and Signal Processing (SNSP), 2018, pp. 409-420, doi: 10.1109/SNSP.2018.00085.

[34] D. Gota, A. Fanca, A. Puscasiu, H. Valean and L. Miclea, "Driving Evaluation Based on Acceleration, Speed and Road Signs," 2019 23rd International Conference on System Theory, Control and Computing (ICSTCC), 2019, pp. 554-559, doi: 10.1109/ICSTCC.2019.8885678.

[35] K. Weide-Zaage, "New-Automotive -Autonomous Driving Challenges for the Microelectronic Components," 2019 Pan Pacific Microelectronics Symposium (Pan Pacific), 2019, pp. 1-6, doi: 10.23919/PanPacific.2019.8696273.

[36] V. Chinnalagi, R. Murugeswari, T. Priyadharshni, K. Rajalakshmi and J. Vijitha Ananthi, "Dynamic performance of smart sensor network using IoT," 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 2017, pp. 49-53, doi: 10.1109/I-SMAC.2017.8058396.

[37] J. Kim, S. Yu and J. Lee, "Short paper: Wireless sensor network management for sustainable Internet of Things," 2014 IEEE World Forum on Internet of Things (WF-IoT), 2014, pp. 177-178, doi: 10.1109/WF-IoT.2014.6803147.

[38] Wen-Tsai Sung, Jui-Ho Chen and Ming-Han Tsai, "Applications of wireless sensor network for monitoring system based on IOT," 2016 IEEE International Conference on Systems, Man, and Cybernetics (SMC), 2016, pp. 000613-000617, doi: 10.1109/SMC.2016.7844308.

[39] T. N. Nguyen, C. V. Ho and T. T. T. Le, "A Topology Control Algorithm in Wireless Sensor Networks for IoT-based Applications," 2019 International Symposium on Electrical and Electronics Engineering (ISEE), 2019, pp. 141-145, doi: 10.1109/ISEE2.2019.8921357.

[40] R. Saxena, V. Rishiwal and O. Singh, "Performance Evaluation of Routing Protocols in Wireless Sensor Networks," 2018 3rd International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU), 2018, pp. 1-6, doi: 10.1109/IoT-SIU.2018.8519933.