

REVIEW ARTICLE

Potential and Limitation of Internet of Things (IoT) Application in the Automotive Industry: An Overview

M.S. Beg^{1*}, I. M. Yusri^{1,2,*}, M.F. Jamlos³, W. H. Azmi³, N. H. Badrulhisam⁴ and Omar I. Awad⁵

¹Faculty of Mechanical and Automotive Engineering Technology, Universiti Malaysia Pahang, Pekan, 26600, Malaysia

²Centre for Automotive Engineering, Universiti Malaysia Pahang, Pekan, 26600, Malaysia

³Department of Mechanical Engineering, College of Engineering, Universiti Malaysia Pahang, Lebuhraya Tun Razak, 26300, Gambang, Kuantan, Pahang, Malaysia

⁴Center for Advances Engineering Design, Faculty of Engineering, Built Environment, and Information Technology, SEGi University, 47180 Selangor, Malaysia

⁵State Key Laboratory of Automotive Safety and Energy, Tsinghua University, Beijing 100084, China

ABSTRACT – With yearly output exceeding 70 million units, the automotive industry is one of the world's largest manufacturing industries. According to worldwide estimates, the car industry's global revenue was an astounding 3 trillion dollars equating to a combined global GDP of 3.65 percent. The emergence of IoT in the automobile sector has created new opportunities for automakers and purchasers worldwide. With industrial and commercial applications, IoT in the automobile industry has developed into a significant hotspot for a variety of multipurpose applications. From linked automobiles to automated transportation systems, Internet of Things applications have had a significant impact on the worldwide automotive business. The Internet of Things, along with other disruptive technologies, is reshaping the automobile sector as a whole. The evolution of this sector has resulted in the birth of ground-breaking advancements in automobiles, namely linked and autonomous vehicles. Different types of internet of things technology have significant qualities that make them viable candidates as a technology for use in automotive industry. This paper focuses on internet of things latest findings done by previous researcher and describes the operation of the technology. Moreover, this paper also provides insights into some countermeasures against internet of things.

ARTICLE HISTORY

Received: 4th April 2022

Revised: 29th Aug 2022

Accepted: 23rd Sept 2022

Published: 11th Oct 2022

KEYWORDS

Internet of things;

Automotive industry;

RFID;

Bluetooth;

Autonomous vehicles

INTRODUCTION

Currently, every corner of this earth is on the verge of moving towards industrial revolution 4.0. One of the key elements of industrial revolution 4.0 is the internet of things (IoT). Today access to the internet is limited via devices of desktops, tablets and smartphones. But with the emergence of IoT, practically all the appliances such as mobiles, refrigerators, watches, fire alarm systems, door locks, bicycles, medical sensors, fitness trackers, and smart security systems can be monitored remotely. The internet of things is a form of a smarter and more intelligent system that allow interconnections between human and objects. With this intelligent communication system, everyday activities will be analysed to provide valuable insight into human daily life [1].

The internet of things is an important area in the industrial revolution 4.0. According to JonathanTourmier the lens science from 1994 to 2020, the research and innovation on embedding the internet of things into the real-life application increased exponentially[2]. Although the world is currently in a crisis of pandemic Covid-19 recently, however, the trend does not show any signal of going down. The highest research and innovation is during the pandemic which is in the year 2020 as shown in Figure 1. The rate of the increasing trend is likely to rise even after 2020. Among the leading company that focuses on the development of application in the internet of things are International Business Machines (IBM), AT&T, CISCO, Microsoft, QUALCOMM, HUAWEI, ERICSSON, SIEMENS, Google and Intel.

A key advantage of the internet of things technology compared to other techniques is that the system is a design of diverse and various interconnected smart devices and applications with all the connections that must be linked via the internet to transmit all of the data. Through this connection, most human activities can be optimised to improve the efficiency of human daily life. Figure 2 indicates how the relation of service level expectation with the development of the internet of things level [3]. Apparently, it can be seen that enhancing the connection of the internet of things through data collection and analysis will discover new information, predict early detection, and makes decision over critical situation thus improving the quality of life [1], [2].

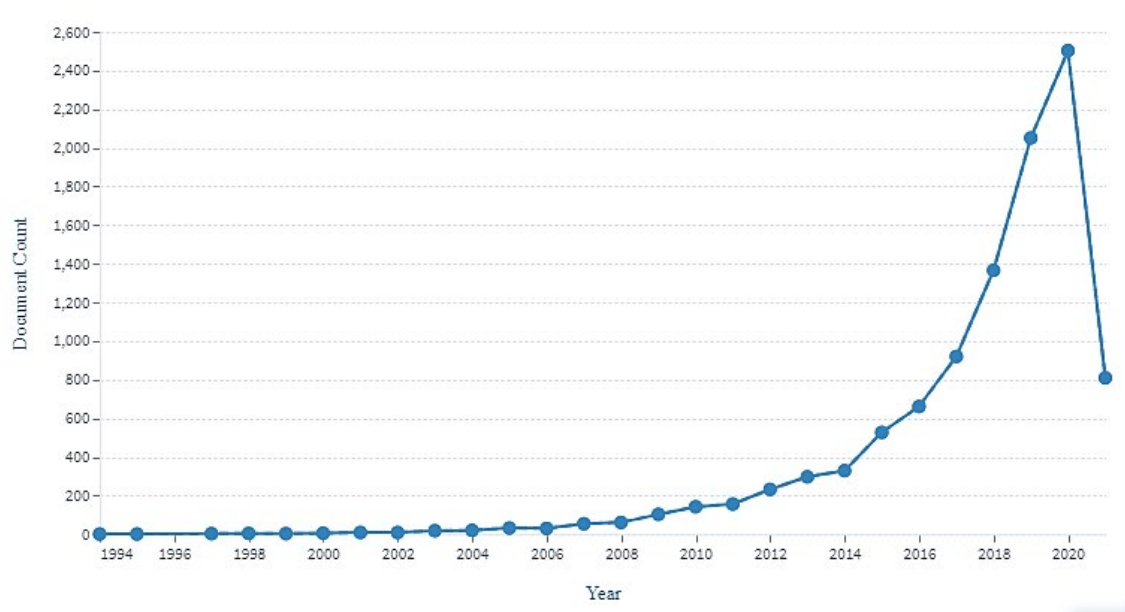


Figure 1. Research and innovation by leading company in the field of internet of things.

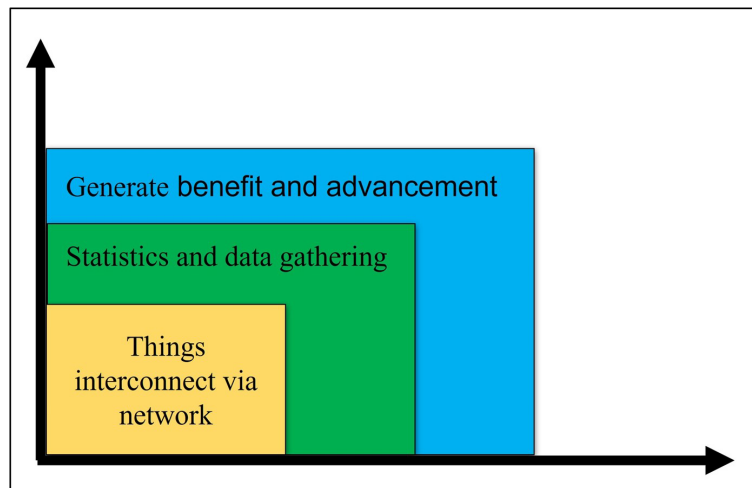


Figure 2. Service level vs level of internet of things development, adapted from [1].

However, it's important to keep in mind that the increase in the number of connected devices in the internet of things eco-system expands the range of possibilities for data breaches on personal information. Also, the connection is expanded far off beyond the scope of local networks, which requires strong authentication and authorisation protocols in a robust system since there are too many connected smart devices. The existing security-related solutions in many cases are not able to cope with all these requirements to their full extent and therefore more research in this area is required [2].

The automotive industry is one of the fastest-growing sectors for IoT development. In the automotive sector, the internet of things has drastically changed the way vehicles move today. The demand in the market today is not only focused on engine fuel efficiency solely. The industry also requires the manufacturer to design a vehicle that is very well equipped with sophisticated technology around the vehicle. Since the previous decade, market analysts have predicted that by the end of 2020, there would be 26 billion to 30.73 billion things connected to the internet as IoT-enabled devices, rising to 75.44 billion by 2025 [4].

People used fixed or mobile telecommunications during the pre-internet period, often known as the H2H or (Human-to-Human) period. Except that SMS services were one of the key means of communication [5]. When the internet first became available, it was utilised to transport information through a network between individuals [6]. The internet was then used as a service especially in E-Commerce and E-Business [7]. The internet of people was a period in which a person connected with one another through social media and a variety of other platforms such as Facebook, Orkut, Skype, and Youtube [8]. Until recently the technology is now focusing on Machine to machine communication (M2M). During this phase, the mechanism allows many devices to interface with one another, such as sensors, controllers, and wireless devices in a network without the need for human involvement [9]. The application of IoT is spreading faster among other products and innovations, future states of the automotive industry of today will need to adapt towards this internet of things technology, or be left behind by new entrants

The internal combustion engine had been one of the greatest achievements in human-designed technology. Among the historiography of human technology, perhaps the most well-known work is that of the diesel engine by German

inventor Rudolf Christian Karl Diesel. Ever since that great innovation, many more types of engine design such as inline, ‘V-shaped’, ‘W’ shaped, flat/horizontally opposed, opposed pistons and the radial engine had emerged. Apart from that various range of applications as they are used in vehicles, boats, ships, aeroplanes, and trains. This automotive industry has transformed the global landscape and changed the way people do business, expanded access to goods, created new services and many more. Before 1960, automotive technology had received the most attention on the engine solely. It is only from the mid-1960s until the present that the advancement of the internet of things has gained momentum in the automotive industry [10].

Internet of things applications in the automobile industry are rapidly becoming a necessary and commonly utilised technology for resolving several on-road issues, namely forward collision warning (FCW), blind-spot warning (BSW), lane departure warning (LDW), cross traffic warning (CTW) and pedestrian detection system (PDS). After conducting a study on the literature, it was believed that there is a lack of reviews that specifically address the aforementioned technology in relation to the internet of things in with all the types of collision avoidance. Due to the advantages of the internet of things, this study will conduct a systematic review of the application of the internet of things; the potential and limitations of the application of the internet of things (IoT) in the automotive industry.

PROGRESS IN AUTOMOTIVE TECHNOLOGY

Several global organisations have pushed decarbonisation measures in response to climate change problems to prevent exceeding the 1.5 or 2 degree Celsius safety threshold. In this sense, transport is responsible for an important part of greenhouse gas (GHG) emissions and the depletion of fossil fuels. In today’s world, transportation accounts for almost a quarter of total CO₂ emissions from fuel burning, with road transport accounting for a fifth (International Energy Agency 2019). In this regard, several governments are supporting the widespread use of electric vehicles (EVs), which might help the world reach its climate change targets. As a result of this, every industry is at least largely controlled by software, and the automobile sector is no exception in order to create a much more complex and efficient automobile that emits less CO₂. The worldwide automotive software industry is valued at about \$13 billion and rising at a rate of roughly \$100 million each year [11].

The automotive industry of today is currently moving through tremendous change [12], [13]. The change that the world can see now is a transmission from an analogue to a digital automotive vehicle. Going in this direction, it is expected that all parts of the latest vehicle will be equipped with a sensor to monitor the condition of the vehicle. In the history of automotive development, technology has been the key factor in its advancement. The automobile as we know it today was not invented in a single day by a single inventor. The chronological history of the major advancement in automotive technology can be seen in Figure 3.

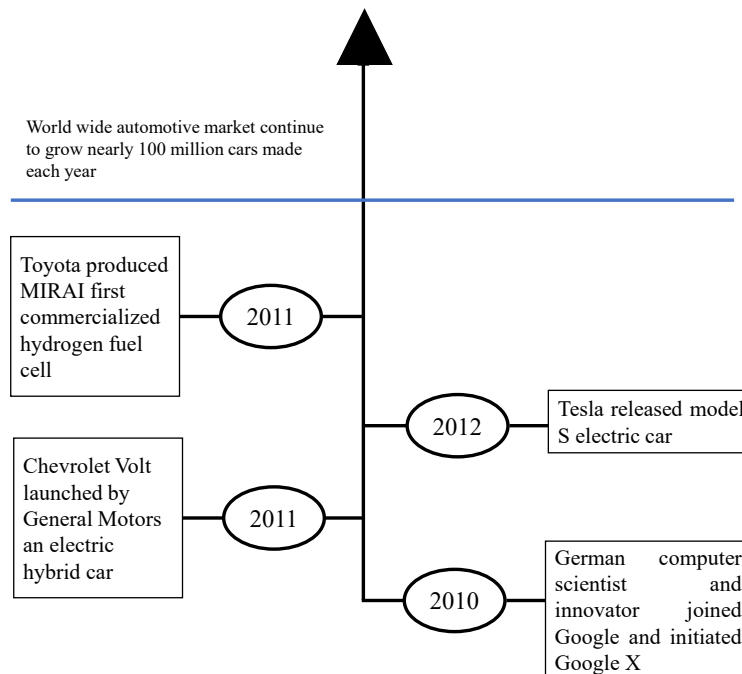


Figure 3. Major advancement in automotive technology.

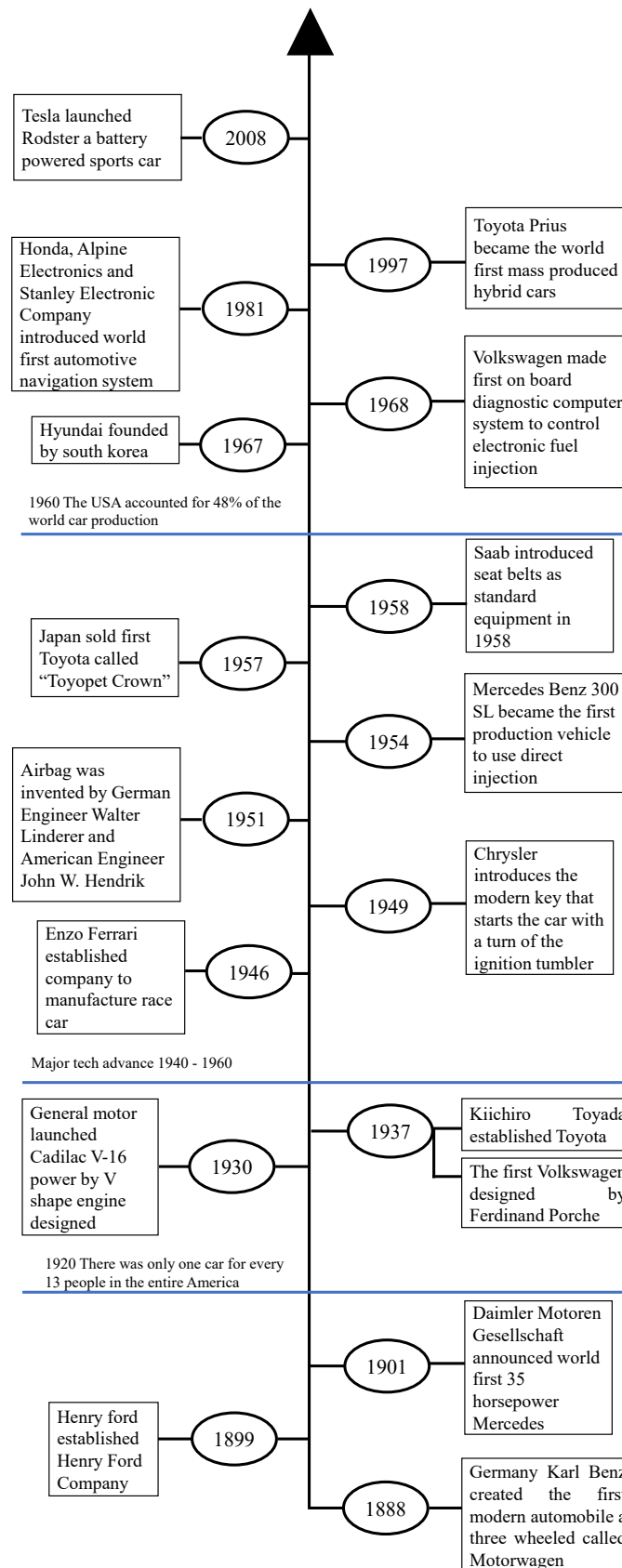


Figure 3. Major advancement in automotive technology (cont.).

Many people or teams of people are credited with inventing the car. The early day of development of the automotive industry all began in the late of 18 century in 1885. A German engineer named Karl Benz had developed a road-going vehicle 3-wheel motor powered with gasoline fuel. The world's first road-going vehicle was then patented and the name "Benz Patent Motorwagen" [14]. Henry Ford in 1899 then established the Henry Ford Company and started the world's first mass production of automotive cars [15]. At the beginning of the 19th century, Daimler-Motoren-Gesellschaft created the first automobile that was able to drive up to 55 mph with 35 horsepower of engine capability. During that time, this

automobile was designed by Wilhelm Maybach, the brilliant head design engineer is regarded as the first modern car in the world [16]. After that, there are a series of newly designed automobiles that appeared in the market such as General Motors which introduced the Cadillac equipped with 16 engine cylinders and powered through a V-shaped engine design.

Apart from that, a Japanese automobile company started to enter the market. It's really an eye-opening history because nobody aspect that an Asia country could compete with Europe and America. By 1930, Kiichiro Toyoda formed the Toyota company and started to design a sedan car [17]. Between the period of 1940 to 1960, Enzo Ferrari established a company that manufactured a race car. One of the main reasons for the success of the company is that he is a racing car driver [18]. During that period as well Chrysler invented the modern key in 1949, which allowed the automobile to be started by turning the ignition tumbler [19]. The airbag, together with seat belts, is one of the most important innovations in the field of driver and passenger safety. In 1953, Hetrick, a former industrial engineering specialist, was granted a patent for a safety cushion assembly for automobile vehicles [20]. In 1954 Mercedes-Benz produced the world-first four-cylinder, four strokes direct injection gasoline engine known as 300 SL. After that, Mercedes keeps on moving forward to lead in direct injection technology [21]. Then in 1957, Toyota first sold the first sedan car in America. It was first introduced in Japan as the Toyopet Crown in 1955 and has since served as Toyota's flagship sedan in Japan [22]. The Swedish manufacturer (SAAB) later in 1958 implemented seat belts as standard equipment in vehicles to protect the driver or a passenger from potentially dangerous movement caused by an accident [23]. In 1968, the Hyundai Motor Company began producing automobiles, assembling imported components and sets for the Ford Motor Company. To do so, the Hyundai Motor Company took use of government incentives to get licenced technology from other nations, mostly Japanese technologies, and picked Mitsubishi Motors as its primary parts and component supplier [24].

In 1968 Volkswagens in their fuel-injected type, 3 vehicles offer the first on-board computer system with scanning capabilities. On-board diagnostic is a system used in the automotive industry to describe a vehicle's capacity to self-diagnose and report [25]. The first automatic car navigation system was created in 1981. Honda, Alpine, and Stanley Electric collaborated to create the Gyro-Cator system. This system is capable of determining the position of the vehicle by a built-in helium gyroscope that detects vehicle location [26]. The Prius was introduced in Japan in 1997 and became the first mass produced hybrid car in the world. With a redesign of the batteries by the year 2000. In 2004, the second-generation, reworked Prius entered the market. The Prius was updated as a midsize hatchback in 2004 and received the Advanced Technology Partial Zero-Emissions Vehicle certification (AT-PZEV). Between the Corolla and the Camry lies the third generation of the Prius HEV. Prius has earned multiple awards, including car of the year in the region of Europe, Japan, and North America [27]. In 2008, Tesla Motors unveiled The Roadster, their first electric vehicle. On a single charge, the Roadster covered 245 miles (394 kilometres). Through December 2012, Tesla has sold roughly 2,450 Roadsters in over 30 countries since 2008. Tesla ran into several issues while introducing the first electric vehicle, not just with the product but also with its marketing [28].

POTENTIAL OF IOT TECHNOLOGY IN THE AUTOMOTIVE INDUSTRY

Software is responsible for a lot of innovation in the automobile industry. Electronics and software were responsible for almost 90% of vehicle advancements in 2012. More software developments will be possible as a result of new automobile technology [29]. First, sensors provide a vast amount of data that may be utilised to enhance future cars or offer after-market services, for example. Second, increased processing power and communication capabilities will enable the storage, transmission, and analysis of vehicle data, as well as the use of a broader variety of infotainment apps. Emerging all of these software and hardware technologies will also enable the development of applications that make travel safer, more efficient, and more pleasant [30]. This section summarises the IoT architecture. It is a grouping of devices having sensors, actuators, and processors that work together to reach a specific goal.

Radio Frequency Identification

RFID (radio-frequency identification) is a method of automatically identifying and tracking tags affixed to items using electromagnetic fields. A radio transponder, a radio receiver, and a transmitter comprise an RFID system. The tag sends digital data, generally an identifying inventory number, back to the reader when it is activated by an electromagnetic interrogation pulse from a nearby RFID reader device. This number may be used to keep track of stock items. Figure 4. illustrates how the RFID application works in the facility; RFID is used widely in the company facility to allow only company person to enter the facility. The RFID reader is a network-connected device that may be either portable or fixed. It transmits impulses that activate the tag via radio waves. When the tag is turned on, it transmits a wave back to the antenna, which is converted into data. The RFID tag contains the transponder. The literature on RFID has highlighted different situations as well. Qin et al. [31] developed RFID systems on roads (RSR), which have recently been put forward to localise not only manned vehicles but also autonomous vehicles. Their study presents an adaptive mobile tag reading algorithm that may effectively prevent reader collisions and enhance tag reading efficiency for accurate vehicle location in a variety of traffic circumstances. The feasibility and efficacy of our suggested strategy have been confirmed via extensive modelling and testing. Field testing shows that, with moderate vehicle density and sparsely placed tags, our proposed method can meet the tag reading criteria given by the upper-layer localisation system with a probability of up to 0.976. In another research study, Chen et al. [32] proposed an RFID-based vehicle localisation system in GPS-less situations. In order to confirm the practicality of the suggested method, they conducted a series of tests in their test region. In terms of practical implementation, they use single antenna multi-frequency-based range estimation and multi-range-based localisation, where a closed-form robust CRT algorithm solves the integer ambiguity issue, and this technique is

used to determine the vehicle location from estimated ranges. Experiments reveal that the suggested technique can accomplish precise vehicle localisation with a precision of less than 33 cm with a 90% probability.

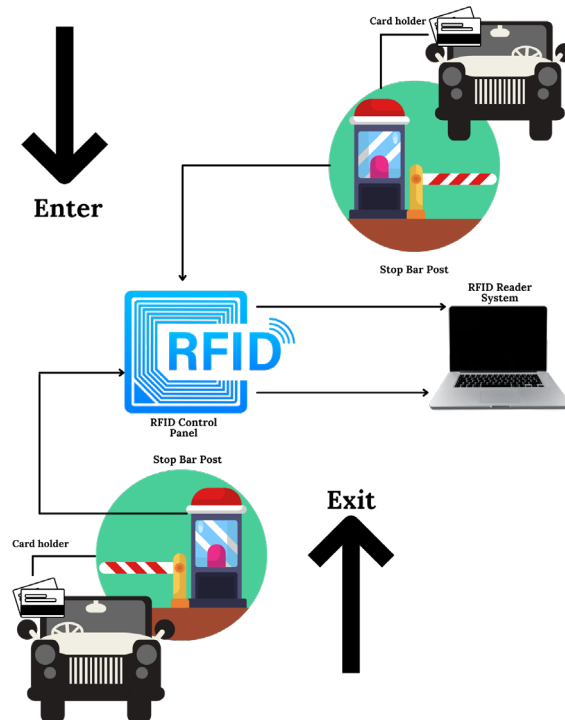


Figure 4. Use of RFID as entering and exit situation in a facility.

Bluetooth and Wi-Fi

Bluetooth is a short-range wireless technology standard for transmitting data over short distances between fixed and mobile devices. Figure 5 depicts the Bluetooth connections between all of the devices. Wireless technology based on the IEEE 802.15.1 standard is used in this gadget. It's used to transfer data between fixed and mobile wireless devices over short distances and to create WPANs (Wireless Personal Area Networks). Ericsson, a telecommunications company, first proposed it in 1994 as a wireless replacement for RS-232 wires. Automotive manufacturers have been paying close attention to connectivity services in recent years. Advanced entertainment systems with large displays are no longer exclusive to high-end automobiles. Integrated services are predicted to be the most popular by 2025 as a result of increased client demand. Individuals are getting more connected to their mobile phones and the services they offer as their functionality improves and grows. This implies that having the same platform and Apps in a person's car is crucial. Car makers can help reduce the number of accidents caused by texting and driving by offering such platforms [33]. In Mourad et al. [34], the effect of adjacent networks on an on-board WLAN network was evaluated during test drives. In a metropolitan context with a large number of public or private APs, measurements found that the interference impact is particularly strong. In comparison to freeway environments, there is a significant difference. Inter-vehicular communication using Bluetooth low energy (BLE) was examined [35]. The results demonstrate that communication is possible up to 100 metres but that a reliable link can only be established up to 50 metres. WLAN interference, in particular, has a significant impact on performance, particularly when all three non-overlapping WLAN channels are utilised. The testbed findings in [19] showed that Bluetooth performance deterioration is dependent on the distance of the Bluetooth connection, the distance to the interferer, the orientation of the antennas, and the traffic load [36].

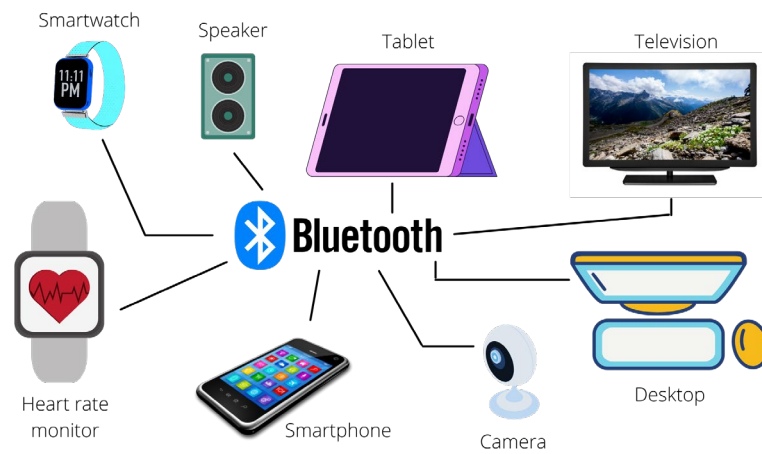


Figure 5. Bluetooth and Wi-Fi in daily life.

V2V and V2X

Vehicle-to-vehicle (V2V) communications is a wireless network in which cars transmit messages with information about their activities [37]. This information would include speed, position, travel direction, braking, and loss of stability. Every node (vehicle, smart traffic light, etc.) in the V2V network would be able to send, collect, and retransmit signals as shown in Figure 6. There are several vehicular communication networks available to protect the safety and security of passengers, delivering traffic information, warning the driver about vehicle conditions and positioning, contributing to traffic management as well as minimising accidents. The most used vehicular communication paradigms are V2V, V2I, vehicular ad-hoc networks (VANETs), and so forth [38]–[40]. The network's five to ten hops would collect traffic conditions a mile ahead. Even the most inattentive driver will be able to lift his foot off the pedal in that amount of time. V2V warnings may appear to the driver as an alert, such as a red light flashing in the control module or an amber then red alert indicating growing difficulties in early automobiles. It might indicate the threat's direction. All of this is subject to change for the time being since V2V is still a concept with thousands of operational prototypes or converted test vehicles. However, the V2V communication system enables necessary information to be shared between vehicles in order to avoid accidents, traffic congestion, and emergency braking. On the other hand, V2I systems utilise internet connectivity to collect and share data between vehicles and roadside infrastructure units (RSUs). Additionally, both vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) are part of vehicle-to-everything (V2X) because they leverage emerging IoT technology for sharing information from anywhere to anything [41], [42]. One of the recent studies combined both different types of methods which are the infrastructure to vehicle (I2V) and V2V. This integration is done collaboratively to increase the efficiency with which data is delivered [43].

Lu Wei [44] proposed a method for securing V2V and V2I connections in VANETs concurrently. The purpose of this work was to develop a shared session key for verified vehicles and RSUs and to demonstrate how the established key, in conjunction with existing message authentication and encryption techniques, may be used to secure both V2V and V2I communications concurrently. The protocol's key components may be classified into two categories; developing a tree-based, lightweight, secure, and practical method for the key agreement that takes into account. The security analysis showed that the suggested approach was secure. In Dey et al. [45], the authors showed the potential of V2V and V2I in a Het-Net environment with Wi-Fi, DSRC, and LTE that ensures efficient exploitation of existing communication choices while minimising backhaul communication infrastructure needs for connected vehicle applications. Existing CVT architectures, such as CVRIA, indicate that flawless V2V and V2I communication are necessary to exploit the potential of CVT applications fully. The performance of a CVT application employing Het-Net is contingent upon the availability of several wireless connectivity choices, acceptable communication latency, data security, and message delivery dependability. A feasible communication option for a wide variety of CVT applications (e.g., safety, mobility, and environmental) should comprise V2V and V2I capable of effectively leveraging a Het-Net without losing connection while switching from one communication network to another. It will need a successful handoff between two wireless networks in a Het-Net scenario. However, these disparate networks were not built to allow for smooth message exchange between them when nodes/vehicles are moved.

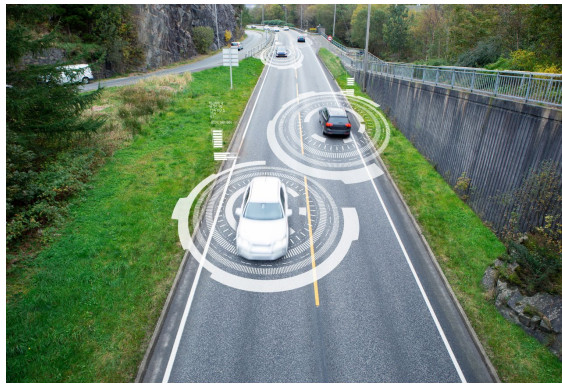


Figure 6. Vehicle-to-vehicle (V2V) communications to transmits information about the activities of their vehicles, such as speed, position, travel direction, braking, and loss of stability.

Automotive Ethernet

Ethernet protocol was developed in 1980 by Robert Metcalfe, and it has been regularly improved since then. Numerous research initiatives on new communication infrastructures are ongoing for vehicles. In 2007, the BMW automobile company unveiled a Demonstration of an IP-based car prototype on a technological level. They collaborated with the Technical University of Munich, and CAR@TUM was created as a result of this [46]. Higher-data-rate bus systems, such as CAN FD (Controller Area Network with Flexible Data Rate) [47] and 100BASE-T1 Automotive Ethernet [48], enable the integration of additional functionalities in automobiles, all the way up to autonomous driving. Data transmission demands a high level of dependability, which necessitates a high level of protection against electromagnetic interference.

Long Term Evolutions (LTE)

Long Term Evolutions (LTE) is a wireless mobile telecommunications service created by the Third Generation Partnership Project (3GPP) [49]. This technology is based on the IEEE 802.11 wireless LAN protocol [50]. The Core Network, Radio Access Network (RAN), Backhaul Network, and Device Equipment are the four primary components of LTE. The brain network is the Core Network. It is made up of gateways that regulate access, QoS, and network regulations. The user will be able to access the internet and multimedia services via the core. The radio access network (RAN) is made up of cell towers that include transceivers and antennas that offer wireless coverage. The fibres and microwave links that were installed below and under the sea make up the backhaul network. It establishes a link between the RAN and the Core Network. The Device Equipment is the end user. This is the cell phone, router, or microprocessor that is directly linked to the RAN and has internet access.

LTE technology has evolved from 1G up to 4G and 5G is yet to achieve its maturity soon. It lies between a frequency of 700MHz and 2.7GHz [51]. OFSDMA, MIMO, and MU-MIMO are all 4G characteristics. The Orthogonal Frequency Division Multiple Access (OFDMA) procedure achieves great spectral efficiency to enable a channel allocation strategy that allows mobile terminals to receive downlink transmission signals from the base station. This is the technique of splitting the transmitted data into orthogonal narrowband carriers based on its frequency. To boost the performance of the physical layer and data link layers, the OFDM transmitter separates the information into several simultaneous sub-streams and sends it to the sub-carrier. Numerous Inputs and Multiple Outputs (MIMO) is a technique that uses multipath transmission to allow multiple radio connections to broadcast and receive data at the same time.

LIMITATIONS OF IOT IN THE AUTOMOTIVE INDUSTRY

The IoT is a very sophisticated system comprised of several components that work together to accomplish a shared purpose [52], [53]. A large number of devices connected to the same network compete for limited radio and network transmission resources. Without suitable design, this sophisticated system may also be subject to a single point of failure, resulting in system failure [54]. Well-trained and accomplished workers are required to operate IoT in an automobile vehicle, but it's difficult to find. Due to the diverse nature of automotive IoT applications and capabilities, the number of vehicle customers and automakers industries interested in this technology, as well as the need for IoT professionals, continues to grow proportionately [55].

For operators who are skilled and well-trained to integrate IoT in a vehicle, which is not possible to get their services everywhere. Because of the wide range of applications and facilities for automotive IoT, car owners and manufacturers are interested in this technology, and the demand for IoT experts grows with it. There is a lot of evidence that qualified staff can handle the challenges that are coming up better than new staff can [56]. Again, for the IoT to work, the system needs to get permission from the people who own the cars and other things that communicate with them. They might not want to share their information with other cars and things. This is important because there is a strong chance that personal information will be misused, which is a very personal thing [57]. Because there are more devices, having IoT raises the costs of the car and the maintenance costs of the roadside infrastructure. From the manufacturer's point of view, to run an IoT-enabled industrial plant, you need digitally skilled specialists and operators, which costs more money.

Within vehicles, in-vehicle communication occurs through the use of automotive bus systems, which enable message transmission between vehicle ECUs; infotainment and telematics systems, which provide entertainment capabilities and

vehicle system information to passengers; and vehicle ports, which allow vehicles to connect to diagnostic devices, import media, and charge their batteries. These in-vehicle communication settings are protected by the security measures discussed in this section.

On-Board Diagnostics (OBD) systems monitor different emission control and engine components/subsystems and are capable of lighting the check engine light Malfunction Indicator Lamp (MIL). The initial generation of OBD standards focused on electrical failure detection and lacked standardised Diagnostic Trouble Codes (DTC), communication protocols, and connection locations. In 1996, the United States government enforced the use of the second-generation OBD, dubbed OBD-II. Along with electrical failures, the second-generation OBD monitored emission-related systems and ensured interoperability across manufacturers. OBD systems use OBD-II ports, which are often located behind the steering column of a vehicle. Threats to OBD-II ports are subject to cyber attacks on the in-vehicle network and dongle exploitation. In-vehicle network access attack: An attacker gains access to the in-vehicle network by inserting an external device into the OBD-II port. OBD-II ports are weak places in vehicular security because they allow the collection of diagnostic data, access to the in-vehicle network, and the installation of malware [58]. In Miller and Valasek [59], with an ECOM cable and improvised connections to connect to the OBD-II port, they were able to send and receive signals through CAN. Dongle exploitation attack: Dongles connected to the OBD-II port may be remotely manipulated and are easily decrypted [60]. One such dongle was the Bosch Drive-log connection, which kept track of vehicle maintenance and directed the vehicle operator to the most relevant service places. This dongle, which links to the OBD-II port of a car, was executed as a brute-force assault that allowed them to connect to the dongle through Bluetooth and transmit malicious communications via the controller area network. These transmissions finally resulted in a moving vehicle's engine failing. This one connection was the Bosch Drive-log connection, which kept track of vehicle maintenance and directed the vehicle operator to the most relevant service places. This dongle, which links to the OBD-II port of a car, was compromised when the Argus Cybersecurity company executed a brute-force assault that allowed them to connect to the dongle through Bluetooth and transmit malicious communications via the Controller Area Network. These transmissions finally resulted in a moving vehicle's engine failing [61].

Raya and Hubaux [62] describe threats on V2V to damage the network's operation. An active hacker is capable of creating and sending malicious packets across the network. Local attackers have a restricted reach and can conduct assaults solely inside that range, while extended attackers have a broader reach spread over the network. V2V communicates using a mesh topology based on the vehicular ad-hoc network (VANET), allowing any node in the network to broadcast and receive signals.

CONCLUSION

With its benefits over other technologies utilised in a modern automotive vehicle, the IoT technology has the potential to benefit the automotive sector significantly. Indeed, the IoT technology is geared toward a higher reliability/latency-sensitive use case, which will eventually meet the demands of industrial automation, crucial information broadcasting, and self-driving automobiles. Given that, the implementation of the IoT over the next decade will result in new architectures, technologies, and hardware that automatically give the additional functionality and capabilities required to enable true full internet of things vehicles on a global scale. We shall examine the possible advantages of the internet of things.

ACKNOWLEDGEMENT

The authors would like to thank the Ministry of Higher Education for providing financial support under Fundamental Research Grant Scheme (FRGS) No. FRGS/1/2021/TK02/UMP/02/1 (University reference RDU210153) and Universiti Malaysia Pahang for laboratory facilities as well as additional financial support under Internal Research grant RDU1903101.

REFERENCES

- [1] H. Elazhary, "Internet of Things (IoT), mobile cloud, cloudlet, mobile IoT, IoT cloud, fog, mobile edge, and edge emerging computing paradigms: Disambiguation and research directions," *J. Netw. Comput. Appl.*, vol. 128, pp. 105–140, Feb. 2019, doi: 10.1016/J.JNCA.2018.10.021.
- [2] J. Tournier *et al.*, "A survey of IoT protocols and their security issues through the lens of a generic IoT stack," *Internet of Things (Netherlands)*, vol. 16, p.100264, 2021, doi: 10.1016/j.iot.2020.100264.
- [3] D. Koo, K. Piratla, and C. J. Matthews, "Towards sustainable water supply: schematic development of big data collection using internet of things (IoT)," *Procedia Eng.*, vol. 118, pp. 489–497, 2015.
- [4] S. Oza *et al.*, "IoT: The future for quality of services," *Lecture Notes in Electrical Engineering*, vol. 570, pp. 291–301, 2019.
- [5] K. Alieyan *et al.*, "Botnet and Internet of Things (IoTs): A definition, taxonomy, challenges, and future directions," in *Research Anthology on Combating Denial-of-Service Attacks*, IGI Global, 2021, pp. 138–150.
- [6] R. Maru, J. Pitroda, and A. D. Raval, "Feasibility study of Internet of Things (IoT) in construction industry: A review," *Studies in Indian Place Names*, vol.40, no. 50, pp.4948-4958, 2020.
- [7] K. Sharma, D. Anand, M. Sabharwal, P. K. Tiwari, O. Cheikhrouhou, and T. Frikha, "A Disaster Management Framework Using Internet of Things-Based Interconnected Devices," *Math Probl Eng.*, vol. 2021, p. 9916440, 2021.
- [8] A. Khanna and S. Kaur, "Internet of Things (IoT), applications and challenges: A comprehensive review," *Wirel. Pers. Commun.*, vol. 114, pp. 1687–1762, 2020.

- [9] V. Dehalwar, A. Kalam, M. L. Kolhe, and A. Zayegh, "Review of machine to machine communication in smart grid," In 2016 International Conference on Smart Grid and Clean Energy Technologies (ICSGCE), 2016, pp. 134–139.
- [10] M. A. Rahim *et al.*, "Evolution of IoT-enabled connectivity and applications in automotive industry: A review," *Vehicular Communications*, vol. 27, p. 100285, 2020.
- [11] O. A. Jefferson *et al.*, "Mapping the global influence of published research on industry and innovation.," *Nat. Biotechnol.*, vol. 36, no. 1, pp. 31–39, Jan. 2018, doi: 10.1038/nbt.4049.
- [12] M. De Gennaro *et al.*, "Designing, prototyping and testing of a ferrite permanent magnet assisted synchronous reluctance machine for hybrid and electric vehicles applications," *Sustain. Energy Technol. Assess.*, vol. 31, pp. 86–101, 2019.
- [13] M. De Gennaro, E. Paffumi, and G. Martini, "Customer-driven design of the recharge infrastructure and Vehicle-to-Grid in urban areas: A large-scale application for electric vehicles deployment," *Energy*, vol. 82, pp. 294–311, 2015.
- [14] H. Inoue, "Perspective for Advanced Vehicle Technology into CASE Era," *NTN Technical Review*, vol. 87, pp. 2–10, Nov. 2019.
- [15] F. Alizon, S. B. Shooter, and T. W. Simpson, "Henry Ford and the Model T: lessons for product platforming and mass customisation," In International Design Engineering Technical Conferences and Computers and Information in Engineering Conference, 2008, pp. 59–66.
- [16] E. Lepoutre, P. Roman, and S. Tom Georges, "Used car market and heterogeneous environmental standards, from developed to developing countries," M.Sc thesis, Université catholique de Louvain, Belgium, 2019.
- [17] K. Wada, "The foundation of the Japanese automobile manufacturing industry: Attempts to adopt Ford's production system," in *The Evolution of the Toyota Production System*, Singapore: Springer, 2020, pp. 37–69.
- [18] B. Yates, *Enzo Ferrari: The Man and the Machine*. London: Penguin UK, 2019.
- [19] B. Webb, "Steering column locks and motor vehicle theft: Evaluations from three countries," *Crime prevention studies*, vol. 2, pp. 71–89, 1994.
- [20] H. Sasaki and I. Sakata, "Identifying potential technological spin-offs using hierarchical information in international patent classification," *Technovation*, vol. 100, p. 102192, 2021.
- [21] Y. Takagi, "A new era in spark-ignition engines featuring high-pressure direct injection," In Symposium (international) on Combustion, 1998, pp. 2055–2068.
- [22] J. Gertner, "From 0 to 60 to world domination," *New York Times*, 18 Feb. 2007.
- [23] G. Sinnapolu and S. Alawneh, "Intelligent wearable heart rate sensor implementation for in-vehicle infotainment and assistance," *Internet of Things*, vol. 12, p. 100277, 2020.
- [24] F. Nunes, G. L. R. Vaccaro, and J. A. V. A. Júnior, "The development of the Hyundai production system: The historical evolution," *J Manuf Syst*, vol. 43, pp. 47–57, 2017.
- [25] A. Sumorek and M. Buczaj, "Problems of searching for failures and interpretation of error codes (DTCs) in modern vehicles," *ECONTECHMOD: An International Quarterly Journal on Economics of Technology and Modelling Processes*, vol. 5, pp. 27–34, 2016.
- [26] W. Wang, M. Uehara, and H. Ozaki, "Proposal of navigation system based on system optimal traffic assignment," in *Conference on Complex, Intelligent, and Software Intensive Systems*, 2018, pp. 184–195.
- [27] C. C. Chan, "The state of the art of electric, hybrid, and fuel cell vehicles," *Proceedings of the IEEE*, vol. 95, no. 4, pp. 704–718, 2007.
- [28] S. Bhardwaj *et al.*, "Problems faced by automobile industries: Case study on Tesla," *International journal of Tourism and hospitality in Asia Pasific (IJTHAP)*, vol. 3, no. 2, pp. 78–88, 2020.
- [29] D. Mohr *et al.*, "The road to 2020 and beyond: What's driving the global automotive industry," *McKinsey & Company*, vol. 28, no. 3, p. 2014, 2013.
- [30] M. Alam, "The software defined car: Convergence of automotive and Internet of Things," in *Wireless World in 2050 and Beyond: A Window into the Future!*, Springer, 2016, pp. 83–92.
- [31] H. Qin, W. Chen, W. Chen, N. Li, M. Zeng, and Y. Peng, "A collision-aware mobile tag reading algorithm for RFID-based vehicle localisation," *Computer Networks*, vol. 199, p. 108422, 2021.
- [32] R. Chen, X. Huang, W. Liu, and Y. Zhou, "RFID-Based Vehicle Localisation Scheme in GPS-Less Environments," In IEEE INFOCOM 2020-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), 2020, pp. 1237–1241.
- [33] A. Mourad *et al.*, "On the performance of WLAN and Bluetooth for in-car infotainment systems," *Vehicular Communications*, vol. 10, pp. 1–12, 2017.
- [34] A. Mourad, F. Heigl, and P. A. Hoehner, "Performance evaluation of concurrent IEEE 802.11 systems in the automotive domain," In 2016 IEEE 41st Conference on Local Computer Networks (LCN), 2016, pp. 655–661.
- [35] M. O. Al Kalaa, W. Balid, N. Bitar, and H. H. Refai, "Evaluating bluetooth low energy in realistic wireless environments," In 2016 IEEE Wireless Communications and Networking Conference, 2016, pp. 1–6.
- [36] K. Matheus and S. Zurbes, "Co-existence of Bluetooth and IEEE 802.11 b WLANs: Results from a radio network testbed," In The 13th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, 2002, pp. 151–155.
- [37] Y. Ren, M. Yan, X. Xu, and H. Yu, "Traffic dynamic model for attacked information propagation under V2V communication networks," In 21st COTA International Conference of Transportation, 2021, pp. 475–485.
- [38] S. Sharma and B. Kaushik, "A survey on internet of vehicles: Applications, security issues & solutions," *Vehicular Communications*, vol. 20, p. 100182, 2019.
- [39] J. Wan, C. Zou, K. Zhou, R. Lu, and D. Li, "IoT sensing framework with inter-cloud computing capability in vehicular networking," *Electronic Commerce Research*, vol. 14, no. 3, pp. 389–416, 2014.
- [40] A. R. Khan *et al.*, "DSRC Technology in Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) IoT System for Intelligent Transportation System (ITS): A Review," *Recent Trends in Mechatronics Towards Industry 4.0*, pp. 97–106, 2022.
- [41] S. Zhang, J. Chen, F. Lyu, N. Cheng, W. Shi, and X. Shen, "Vehicular communication networks in the automated driving era," *IEEE Communications Magazine*, vol. 56, no. 9, pp. 26–32, 2018.
- [42] N. Cheng *et al.*, "Air-ground integrated mobile edge networks: Architecture, challenges, and opportunities," *IEEE Communications Magazine*, vol. 56, no. 8, pp. 26–32, 2018.

- [43] K. Liu, J. K. Y. Ng, V. C. S. Lee, S. H. Son, and I. Stojmenovic, "Cooperative data scheduling in hybrid vehicular ad hoc networks: VANET as a software defined network," *IEEE/ACM Transactions on Networking*, vol. 24, no. 3, pp. 1759–1773, 2015.
- [44] L. Wei, J. Cui, H. Zhong, Y. Xu, and L. Liu, "Proven secure tree-based authenticated key agreement for securing V2V and V2I communications in VANETs," *IEEE Trans Mob Comput*, 2021.
- [45] K. C. Dey, A. Rayamajhi, M. Chowdhury, P. Bhavsar, and J. Martin, "Vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication in a heterogeneous wireless network—Performance evaluation," *Transp. Res. Part C Emerg. Technol.*, vol. 68, pp. 168–184, 2016.
- [46] T.-C. Nichiștea and M.-G. Unguritu, "Automotive ethernet applications using scalable service-oriented middleware over IP: service discovery," In 2019 24th International Conference on Methods and Models in Automation and Robotics (MMAR), 2019, pp. 576–581.
- [47] R. Isermann, "Electrical and electronic architectures of automobiles," in *Automotive Control*, Berlin: Springer, 2022, pp. 15–34.
- [48] B. Ma *et al.*, "An authentication and secure communication scheme for in-vehicle networks based on SOME/IP," *Sensors*, vol. 22, no. 2, p. 647, 2022.
- [49] G. S. Mahalakshmi, K. Koquilamballe, and S. Sendhilkumar, "Influential detection in twitter using tweet quality analysis," In 2017 second international conference on recent trends and challenges in computational models (ICRTCCM), 2017, pp. 315–319.
- [50] K. Ikkelä, M. Myllynen, J. Heinanen, and O. Martikainen, "4G Mobile Network Architecture," in *Emerging Personal Wireless Communications*, Springer, 2002, pp. 183–195.
- [51] M. Almarashli and S. Lindenmeier, "Evaluation of vehicular 4G/5G-MIMO antennas via data-rate measurement in an emulated urban test drive," in *2018 48th European Microwave Conference (EuMC)*, 2018, pp. 300–303.
- [52] S. Latif *et al.*, "An Efficient Pareto Optimal Resource Allocation Scheme in Cognitive Radio-Based Internet of Things Networks," *Sensors*, vol. 22, no. 2, p. 451, 2022.
- [53] B. B. Sinha and R. Dhanalakshmi, "Recent advancements and challenges of Internet of Things in smart agriculture: A survey," *Future Generation Computer Systems*, vol. 126, pp. 169–184, 2022.
- [54] T. Mufti, S. S. Sohail, B. Gupta, and P. Agarwal, "Sustainable Approach for Cloud-Based Framework Using IoT in Healthcare," in *Smart Technologies for Energy and Environmental Sustainability*, Cham: Springer, 2022, pp. 231–244.
- [55] A. E. Omolara *et al.*, "The internet of things security: A survey encompassing unexplored areas and new insights," *Comput Secur*, vol. 112, p. 102494, 2022.
- [56] P. Brous, M. Janssen, and P. Herder, "The dual effects of the Internet of Things (IoT): A systematic review of the benefits and risks of IoT adoption by organisations," *Int. J. Inf. Manage.*, vol. 51, p. 101952, 2020.
- [57] Z. El-Rewini, K. Sadatsharan, D. F. Selvaraj, S. J. Plathottam, and P. Ranganathan, "Cybersecurity challenges in vehicular communications," *Vehicular Communications*, vol. 23, p. 100214, 2020.
- [58] P. Carsten, T. R. Andel, M. Yampolskiy, and J. T. McDonald, "In-vehicle networks: Attacks, vulnerabilities, and proposed solutions," In Proceedings of the 10th Annual Cyber and Information Security Research Conference, 2015, pp. 1–8.
- [59] C. Miller and C. Valasek, "Adventures in automotive networks and control units," *Def Con*, vol. 21, no. 260–264, pp. 15–31, 2013.
- [60] M. H. Eiza and Q. Ni, "Driving with sharks: Rethinking connected vehicles with vehicle cybersecurity," *IEEE Vehicular Technology Magazine*, vol. 12, no. 2, pp. 45–51, 2017.
- [61] A. Kovelman, "A remote attack on the bosch drivelog connector dongle," *von Argus Cyber Security*, 2017.
- [62] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," *J. Comput. Secur.*, vol. 15, no. 1, pp. 39–68, 2007.