Implementation of internet of vehicles (IoV) technology on traffic management

Tan Yong Keat
School of Computing
Asia Pacific University of Technology & Innovation (APU)
Kuala Lumpur, Malaysia
TP59755@mail.apu.edu.my

Chandra Reka Ramachandran
School of Computing
Asia Pacific University of Technology & Innovation (APU)
Kuala Lumpur, Malaysia
Chandra.reka@staffmail.apu.edu.my

Dr. Vazeerudeen Abdul Hameed
School of Computing
Asia Pacific University of Technology & Innovation (APU)
Kuala Lumpur, Malaysia
vazeer@staffemail.apu.edu.my

***Abstract*—Following the emergence of the Internet of Things (IoT) technology, researches across the world have begin to research a way to combine such a technology with the traffic system in an attempt to revolutionize the way the traffic is managed in order to minimize the probability of the many unwanted occurrences in traffic, including accidents, casualties, road congestions and many more. Thus began the extensive research on the concept of the Internet of Vehicles (IoV) technology as well as different ways to implement and enhance its efficiency, security, and reliability. This research covers only the general concept of the Internet of Vehicle's implementation on traffic management, its existing challenges, and a few potential solutions to improve upon the structure of the Internet of Vehicles.**

Keywords—Internet of Vehicles (IoV), network, traffic management, trust management, fog computing, communication, offloading, blockchain.

I. INTRODUCTION

In most of the smart city applications, Internet of Things (IoT) devices are being employed for automatic monitoring systems [1-4]. As the influence of the Internet of Things (IoT) grows over time, the concept of Internet of Vehicles (IoV) began to emerge. The current form of transportation and traffic bears the risk of accidents and the potential inconvenience from traffic congestions. This is due to the fact that the current traffic system relies heavily on the drivers' adaptability to react to occurrences of various unpredictable situations on the road, as well as their capability to drive in a synchronous manner to avoid traffic congestion. However, such a feat is nigh impossible due to the sheer individuality and carelessness of each driver. The communication between drivers are disconnected and limited only to simple gestures and signal lights.

Thus, the logical solution to traffic problems is to remove the uncertain elements created from the human individuality, to remove human control over the traffic flow. With the interconnection and interoperability of intelligent devices made possible through the IoT technology, the Internet of Vehicles shows a promising potential in resolving traffic congestions, road safety issues and improving the overall travelling experience for both drivers and passengers [11].

The Internet of Vehicles (IoV), unlike the Internet of Things (IoT), does not simply connect specific objects through data awareness. Instead, the Internet of Vehicles serves as a network that integrates the behavior between human and vehicle, and interconnects them with their surroundings through mobile devices, intelligent devices, and sensors. Through this, the Internet of Vehicles allows the driver, the vehicle, and the surrounding environment itself to perform information exchange, which can be used to automate driving as a means to manage the fluidity of the traffic, and ensure the safety of the drivers, passengers and nearby pedestrians [12].

Currently, there are several main concerns regarding the implementation of the Internet of Vehicles. Each of these concerns correspond to the essential, intended capabilities of the Internet of Vehicles. Firstly, as with most network systems, data privacy remains to be the main concern for most users. However, standard network protection does not apply to the network used by vehicles. Needless to say, the security of the traffic system is to be taken as the utmost priority to ensure the traffic stays in order. Secondly, in the case of delayed communication, it is of the utmost importance that it is measured in milliseconds as not doing so will result in potentially fatal accidents should a network issue occur. Thirdly, the automation of the vehicles must be perfectly accurate as they are expected to have improved velocity as compared to traditional car-driving in order to realize the objective to improve the flow of the traffic [13].

II. TRAFFIC MANAGEMENT

First and foremost, in order to better comprehend the viability and significance of the potential future implementations for the Internet of Vehicles, it is of the utmost importance that the very idea and concept of the Internet of Vehicles, as well as the merits and flaws it presents should be explored and clarified. The core concept of the Internet of Vehicles is based on the exchange of information. In other words, communication. The Internet of Vehicles is a network of communications that allows vehicles to exchange information with one another, as well as the surrounding environments and pedestrians, enabling a great degree of traffic management, ensuring unity in automated movement and providing insight on the surrounding environment.

The Internet of Vehicles mainly consists of 4 forms of communication. The first form of communication involves the communication between the vehicle and its respective owner. With this, the driver will be able to obtain information on the status of the vehicle such as the vehicle's fuel level, tire pressure, car lock, and speed. If an onboard processor is installed, the owner can receive security and damage alerts even when away from the vehicle [10]. The second form of communication involves the communication between vehicles. This includes information on the vehicles' speed and

proximity to ensure the vehicles are travelling in a safe pace and distance. One vehicle can also notify another of their damages such as a punctured tire, so that the vehicle may drive at a relatively safer speed. The third form of communication involves the communication between the vehicle and a centralized server. This enables the centralized server to observe the vehicle's lock, fuel level, tire pressure, speed, and the components of the exhaust gases' in order to manage the traffic with greater accuracy. The fourth form of communication involves the communication between the server and specific third parties such as police patrols, fire engines, ambulances, and pollution control. Through an onboard processor, whenever a vehicle suffers from sudden temperature spikes, heavy collisions, or even theft, the data is reported to the server. In turn, the server will forward the data to the appropriate corresponding third parties. This ensures appropriate help will be provided by the third party in a more timely manner.

There are numerous advantages when implementing the Internet of Vehicles for traffic management. By sending data from the onboard processors to the traffic signal, the Internet of Vehicles will determine the pace of each lane as well as the amount of time allocated for a traffic light's green signal. Also, by detecting the body temperature of surrounding pedestrians through onboard proximity sensors, IoV vehicles can respond immediately towards a pedestrian in close proximity, and reduce its speed or perform an emergency break to avoid life threatening situations. IoV vehicles can also detect if another vehicle is having abnormalities such as punctured tires, in order to create awareness of potential dangers from said vehicle. In conjunction with the aforementioned forms of communication within the Internet of Vehicles, it is also possible for the IoV vehicles to monitor its own components' status, prevent the theft of the vehicle, minimizing the probability of road accidents and potentially save lives [10].

Unfortunately, while the Internet of Vehicles shows great potential in performing traffic management, there are several challenges to be accounted for before such technology may be implemented. Due to the Internet of Vehicles' reliance on wireless networks, it may be vulnerable to malicious exploitations from hackers. As there are countless vehicles to be found around the roads, the central server will receive data from immense amounts of interconnected nodes. Thus, any malicious actions towards any of the core components of the system such as the central server, router, or the IoV vehicle's processor, bears a risk of causing a system crash, potentially causing catastrophic damage unto the traffic, which will undoubtedly threaten the lives of many [10].

Evidently, it is imperative for sensors and processors to be installed in every vehicle within the traffic in order for the Internet of Vehicles to serve its purpose. However, it is not an impossibility that some vehicle owners will refuse to install said compartments out of fear of personal information leakage, which may potentially lead to legal issues. Moreover, even if all vehicles were to have the aforementioned compartments installed without issues, if the processes and servers are unable to handle the data with consistent efficiency, the IoV system will lose its reliability completely, and thus will be unable to fulfill its purpose and rendered useless. In addition, even the management of the IoV system is a challenge in itself, as it requires equipment with great compatibility with the internet, as well as an organized infrastructure to work in a synchronized fashion [6].

III. TRUST MANAGEMENT

Another major core element of the Internet of Vehicles involves wireless communications between vehicles, or between the vehicle and its surrounding environments such as roadside units, sensors, and even people [8]. However, just as scams, phishing and false information are widely spread around the Internet, the Internet of Vehicles also face several security risks as well as privacy risks. The very existence of potential malicious or dishonest individuals pose a great concern for the Internet of Vehicles, as even a simple false information in road traffic may cause a consecutive series of problematic occurrences, which could potentially be life threatening. Naturally, it is not possible for Internet of Vehicles to be implemented in the future as long as lives at stake.

Thus, in order to overcome this problem, it is imperative for the Internet of Vehicles to establish trust even within a large societal community consisting of many upstanding individuals, as well as malicious and dishonest individuals. There are many aspects of a mechanism to be considered in order to establish trust [8]. Like most network communication services, the service quality must be stable at all times. The vehicle owners should also be given the basic options to freely revoke prior commands as well as to verify certain information or commands with ease. The Internet of Vehicles must always provide or make use of quality information gained through network communication at all times with the utmost consistency. The Internet of Vehicles must also be accessible at all times while being able to handle its tasks with the utmost efficiency with minimal waste. Finally, the Internet of Vehicles must possess a high degree of robustness to ensure its reliability, as well as effective security measures for privacy of information.

In accordance to the observations from [8], it is proposed that blockchain technology possess the potential to instill the trust in the Internet of Things unto the masses as it is observed to have attained a favorable reputation and achieved significant feats including its implementation on recent technologies such as smart contracts, as well as cryptocurrencies. In essence, the blockchain technology enables an approach to information in a reliable, secure, and decentralized manner as a distributed ledger system. In addition, transaction sharing performed between stakeholders through the blockchain technology does not require any form of centralized authority serving as an intermediary [9].

In terms of trust management, a Global Unique Identifier (GUID) and an address can be assigned to IoV vehicles as well as various Internet of Things devices (with global accessibility) within a smart vehicle through the help of blockchain technology. In terms of data integrity and security, as long as the true sender is in possession of a corresponding Global Unique Identifier as well as a unique public key, the blockchain network ensures that data transmissions between IoV vehicles are proofed and signed through cryptography. Through the Ethereum blockchain, smart contracts provide greater access control, governance, management and tracking of smart vehicles. With the Ethereum blockchain, the data from smart vehicles are also kept within the InterPlanetary File System (IPFS) or cloud in a open, trusted and decentralized methodology. These aspects of the Ethereum

blockchain enables the Internet of Vehicles to store shared data regarding road events, damages or routes [5].

IV. FOG COMPUTING

As the main goal of the implementation of Internet of Vehicles is to improve the flow of traffic and to minimize the risks of traffic accidents, the logical approach to said problem is to improve the overall accuracy of the vehicles' responses in real time. However, as the name implies, the Internet of Vehicles is heavily reliant on the stability and accuracy of the server and network systems. A delay in transmission can prove to be fatal. Thus, it is imperative to lighten the loads on a traffic management server. In order to ensure the average time required for the internet of vehicles to respond to the occurrences surrounding the vehicles is shortened to the utmost limit, it is stated that fog computing is a viable option to accomplish such a goal [9].

The main role of fog computing in the Internet of Vehicles, is to perform migrations of computational resources to network edges. This is achieved by offloading tasks to fog nodes in accordance to a proposed efficient predictive scheme (through predictive or direct relay transmission mode) [9]. By scheduling available free resources in vehicles, the rate of the computational resource consumption can be reduced as a countermeasure to avoid overloading the cloud. This will, in turn, improve the transmission within the vehicular networks significantly.

The transition from manually driven vehicles to a fog-enabled Internet of Vehicles are bound to have challenges that come with its benefits. In addition to offloading tasks, the Internet of Vehicles also requires a decentralized system model that enables urban area traffic management in order to reduce the response delay further by reducing the load on traffic management servers. While the aforementioned solution of offloading tasks for the traffic management server via fog computing possess great potential in resolving the response delay issue, the costs for such an attempt will certainly be heavy, as it requires a large number of fog nodes to be installed and placed, which may drastically increase network costs in large sums. It is also imperative to ensure that the traffic loads for fog nodes are balanced and scheduled accordingly.

In order to ensure applications in massive vehicular networks run in real time with minimal requirement for latency and computational resources, it is crucial to research a method to optimize the offloading of network traffic tasks [1]. There are instances when the driver requires certain information when travelling with a vehicle, such as the condition or events on the travel route, including pavements or crowds. This however, is a challenge in itself as finding a desired information amongst a massive accumulation of environmental data stored in automated vehicles is a difficult task, even for fog enabled networking services [10].

V. CONCLUSION

It is without a doubt that the Internet of Vehicles, or at least, the concept behind its idea holds great potential of revolutionizing the management of traffic, as it is a massive transition from manually driven cars to automated cars, interconnected across the network not just with one another, but also with the environment surrounding them. However, there are several challenges to overcome, the three most prominent ones being the need for extreme levels of security, the reliability required to build enough trust with the drivers and the necessary efficiency in the handling of data. As long as any of the prior issues are unresolved, the Internet of Vehicles cannot be implemented by any means. Fortunately, as shown in the previous sections, various ideas for solutions have emerged and researches and experiments are currently being conducted by other researchers extensively, including existing technologies such as fog computing and blockchain as potential solutions to the aforementioned problems. Evidently, there are many other possible solutions available and are currently being researched. There are much of Internet of Vehicles and its many challenges and respective solutions are not yet covered in this research, alternatives that have yet to be considered. Thus, more extensive research are required to discover ways of improving the IoV's energy efficiency, suitable combinations of applications and devices, safety features, the most suitable network architecture, as well as security protocals in much detail, in order to realized the future that is the Internet of Vehicles.

REFERENCES

[1] T. Eldemerdash, et al., "IoT Based Smart Helmet for Mining Industry Application," *International Journal of Advanced Science and Technology*, vol. 29, no. 1, pp. 373-387, 2020.

[2] H. Singh, R. Abdulla, S. K. Selvaperumal., "Carbon Monoxide Detection Based IoT," *Journal of Applied Technology and Innovation*, vol. 5, no. 3, 2021.

[3] W. M. Rasheed, R. Abdulla, L. Y. San., "Manhole cover monitoring system over IOT," *Journal of Applied Technology and Innovation*, vol. 5, no. 3, 2021.

[4] A. M. Samson, R. Dhakshyani, R. Abdulla., "IOT Based Sustainable Wallet Tracking System," International Journal of Advanced Science and Technology, 29(1), pp. 1301 – 1310, 2020.

[5] X. Wang, Z. Ning and L. Wang, "Offloading in Internet of Vehicles: A Fog-Enabled Real-Time Traffic Management System," in *IEEE Transactions on Industrial Informatics*, vol. 14, no. 10, pp. 4568-4578, Oct. 2018.

[6] E. K. Lee, M. Gerla, G. Pau, U. Lee, and J. H. Lim, ''Internet of Vehicles: From intelligent grid to autonomous cars and vehicular fogs,'' Int. J. Distrib. Sensor Netw., vol. 12, no. 9, pp. 1–14, 2016.

[7] Z. Ning, J. Huang, X. Wang, J. J. P. C. Rodrigues, and L. Guo, ''Mobile edge computing-enabled Internet of vehicles: Toward energy-efficient scheduling,'' IEEE Netw., vol. 33, no. 5, pp. 198–205, Sep. 2019.

[8] P. K. Singh, R. Singh, S. K. Nandi, K. Z. Ghafoor, D. B. Rawat and S. Nandi, "Blockchain-based adaptive trust management in internet of vehicles using smart contract," IEEE Trans. Intell. Transp. Syst., early access, Jul. 16, 2020

[9] R. Iqbal, T. A. Butt, M. Afzaal, and K. Salah, ''Trust management in social Internet of vehicles: Factors, challenges, blockchain, and fog solutions,'' Int. J. Distrib. Sensor Netw., vol. 15, no. 1, 2019,

[10] T. T. Dandala, V. Krishnamurth, and R. A. Alwan, ''Internet of Vehicles (10 V) for traffic management,'' in Proc. IEEE Int. Conf. Comput., Commun. Signal Process., Chennai, India, Jan. 2017.

[11] J. Contreras, S. Zeadally, and J. A. Guerrero-Ibanez, ''Internet of vehicles: Architecture, protocols, and security,'' IEEE Internet Things J., Apr. 2017.

[12] F. Yang, S. Wang, J. Li, Z. Liu, and Q. Sun,"An overview of internet of vehicles,"China Communications, vol. 11, no. 10, pp. 1−15, 2014.

[13] M. Chen, Y. Tian, G. Fortino, J. Zhang, and I. Humar, ''Cognitive Internet of vehicles,'' Comput. Commun., vol. 120, pp. 58–70, May 2018.

[14] T. S. J. Darwish and K. A. Bakar, ''Fog based intelligent transportation big data analytics in the Internet of vehicles environment: Motivations, architecture, challenges, and critical issues,'' IEEE Access, vol. 6, pp. 15679–15701, 2018.