# The Internet-of-Vehicle Traffic Condition System Developed by Artificial Intelligence of Things

**Hsin-Te Wu** ( hsinte@niu.edu.tw )
National I-Lan University https://orcid.org/0000-0002-3221-9037

**Research Article**

**Keywords:** Artificial Intelligence of Things, Internet of Vehicle, Federated Learning, Faster R-CNN, 6G Network

**Posted Date:** November 7th, 2022

**DOI:** https://doi.org/10.21203/rs.3.rs-315715/v1

# The Internet-of-Vehicle Traffic Condition System Developed by Artificial Intelligence of Things

**Hsin-Te Wu**

Received: date / Accepted: date

**Abstract** An Internet-of-Vehicle (IoV) system primary transmits traffic information and various kinds of emergency notices through Vehicle-to-Vehicle (V2V) or Vehicle-to-Infrastructure (V2I); however, the transmission of multimedia enables drivers to control route conditions better, such as road obstacles and the range of a construction site. Additionally, car accidents usually require relevant video records of the scene for investigation; surrounding cars could transfer the accident scene videos to help the police restore the detailed situation. Meanwhile, the multimedia messages of IoV need to go through security verification and privacy protection for the system to deliver push notifications and multimedia messages to social groups instantly.

The study aims to construct an IoV traffic condition system developed by Artificial Intelligence of Things (AIoT); the data transmitting method of this research is via the 6th Generation Network (6G Network), which has advantages of high transmission speed and Quality of Service (QoS) guarantee. Furthermore, the suggested system employs federated learning to ensure message security and privacy. The features of the researched system are: 1. Use Faster Region-based Convolutional Neural Networks (R-CNN) to recognize the objects in cameras and judge if there are road obstacles and any constructions; 2. Capture car accident videos through federated learning, and send the encrypted evidence to relevant legal units; 3. Use push notifications to send multimedia messages to social groups instantly, marking the locations and the road conditions to help drivers control the conditions with the surroundings. This study expects to delivering videos and Global Positioning System (GPS) data for road condition recognition, improving driving safety.

**Keywords** Artificial Intelligence of Things · Internet of Vehicle · Federated Learning · Faster R-CNN · 6G Network

Hsin-Te Wu
Department of Computer Science and Information Engineering,
National Ilan University, Yilan City, Taiwan
E-mail: hsinte@niu.edu.tw

## 1 Introduction

In recent years, the concepts of Smart City and Internet of Vehicle (IoV) have gradually become a part of the Internet of Things (IoT) development in the new generation. Intelligent transport systems have been developing for years, aiming to smoothen traffic and help drivers control road conditions through IoV. Currently, traffic messages are mainly texts; yet, words sometimes might be difficult for drivers to understand actual road conditions and the range of influence. Additionally, although there are surveillance cameras at several important junctions and roads to monitor traffic congestion, the equipment is not universal. Meanwhile, many road conditions require videos to record relevant conditions, support responsible units to handle situations, such as accidents and the ranges of obstacles; if there are more cars to provide relevant videos, they could help clarify road conditions and offer evidence. Drivers cannot operate on-board devices to send messages or observe road conditions constantly while driving; therefore, it is essential for on-board devices to be more intelligent in judging road conditions, sending abnormal situations to the sever and legal units, and providing only essential road information to drivers instead of offering other unnecessary messages to distract users.

There are two types of data communication in IoV, Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I). The government needs to install massive wireless equipment to be the repeater stations for V2I communication, which may have higher installation cost; while in V2V communication, data packets may be lost when vehicles move at high speeds, failing to deliver the data to assigned destinations. Moreover, both V2V and V2I transmit over IEEE 802.11p that only deliver between short distances, causing relevant issues like handoff or packet delivery. If a malicious car attempted to implement a broadcast storm attack, it would paralyze the entire network; hence, a network management mechanism to control the data transmission is critical. Because the fixed equipment of IoV requires the government to install massively, and the drivers need to operate the system to transmit messages, which may cause safety issues. If we expect to construct the universal devices for constituting IoV, such as dashboard cameras, these devices should judge real-time road conditions intelligently and share the data to third parties or nearby cars based on drivers' privacy agreement. Regarding the networks, the system will need stable and high coverage of mobile communication to increase the stability of packet delivery, which also ensures vehicle privacy and data security through effective identity authentication.

Today, many cars have installed dashboard cameras, and many of those have equipped with a network communication function. Thus, it is possible to judge road conditions by recognizing objects in the videos of dashboard cameras and sharing the conditions with legal third parties, such as the department of transportation or police stations. This article utilizes two types of records in dashboard cameras to judge road conditions. Firstly, identify the objects from the videos to confirm road conditions, such as any roadworks signs in the videos. Secondly, pinpoint car locations, driving speeds, and directions by the built-in Global Positioning System (GPS) in the cameras; the speeds from the GPS information help the system to judge if there is any traffic congestion. This study identifies the dashboard camera data by Artificial Intelligent (AI) technology and delivers road conditions automatically instead

of requiring drivers to enter relevant information personally, which makes IoV more intelligent. As many cars have installed dashboard cameras, this will significantly reduce the IoV hardware installation cost. Furthermore, employing federated learning, the system enables cameras to update parameters. For achieving an optimal solution in federated learning, the system conducts gradient descent to enhance recognition accuracy. For identifying the objects in videos, the study utilizes Faster Region-based Convolutional Neural Networks (R-CNN) to check if there are roadworks signs or other obstacles on the road. Afterward, adding GPS information to confirm the driving speed and direction for judging the level of traffic congestion. Finally, the system will use machine learning to segment road conditions and then implement the push notification system to share road conditions and relevant videos, helping to notify other cars about the situation. It protects drivers' privacy via federated learning to avoid tapping and stealing video data. The suggested system in this article fulfills the safety requirement of IoV, ensuring data transmission security.

## 2 RELATED WORKS

The research primarily focuses on IoV intelligent identification system. Reference [13] presents a novel elliptic-curve encryption technique. Due to the fixed curve length of the elliptic curve, the system will encounter hardware compatibility in the on-board platform; hence, the technology utilizes dynamic curve lengths and random keys to ensure data transmission security for both sides. Reference [12] offers an approach for vehicles to produce anonymity for k times because IoV requires private and conditional tracking; therefore, cars need to be anonymous. As each anonymity will cause workload to the centralized server, the study approach sets cars and servers to produce anonymity from random keys for k times. In Reference [5], the research demonstrates that drones carry radar to support IoV and industrial sensors to transmit messages, avoiding data packet lost in short-distance delivery. Reference [8] proposes a self-driving application in IoV, which requires each car to send messages intensively to ensure the movement conditions. IEEE 802.11p is mainly for short-distance transmission for GPS to locate cars in general conditions; nonetheless, in complicated road situations, one-dimensional positioning may cause safety concerns. Thus, the research creates a two-dimensional positioning method for the system to locate cars. In Reference [2], the study points out that drones can build base stations in the cloud, regularly collecting the data from IoT sensors; equally, IoV can use the same theory, which benefits packet collection.

With the popularity of AI, to implement real-time applications requires stable and fast network communication. The applications combined with the 6th Generation Network (6G Network) in Reference [15] are AI, blockchain, and big data; the one terahertz (THz) transmission speed of 6G Network enables these applications to achieve real-time functions. Reference [3] reveals that the 5th Generation Network is primarily for supporting IoT functions, while the 6G Network provides the features of low latency and high Quality of Service (QoS). The 6G Network offers applications in AI, quantum computing, and relevant technologies, and it can attain real-time connections, such as Augmented Reality (AR) and Virtual Reality (VR). Reference [11]

proposes a method to obtain 6G Network's real-time feedback in machine learning; moreover, the article discusses that applications in smart healthcare help obtain synchronous surgery and remote control because of the 6G Network's high transmission speed. In Reference [1], the article utilizes dynamic bandwidth in part of the network communication, regularly recycling unused bandwidth for other devices to use; by using Multiple-Input and Multiple-Output (MIMO) technique to achieve low latency and low loss rate.

This research adopts federated learning to ensure driving safety. In previous studies, Reference [14] suggests distributing data in various places and sharing relevant parameters in machine learning. To obtain an optimal solution, Reference [14] uses gradient descent to reach optimal solutions continuously and shares part of the parameters in different devices, optimizing the machine learning. Reference [9] improves the efficiency of edge computing through federated learning. IoT conducts intelligent computing when receiving data, but sending data to the centralized server will cause calculation loads. Therefore, the study conducts the calculation in IoT equipment, allowing the smart calculation to reach optimal solutions; each IoT equipment can further update relevant AI parameters, reaching higher accuracy. The federated learning application suggested in Reference [16] can provide privacy protection on personal devices. The system will consume massive data transmission and power to update all models; hence, it is necessary to optimize all models and only deliver those different parameters to reduce communication cost. Reference [6] points out that all of the data in an intelligent factory are confidential; thus, federated learning can help update and optimize machine parameters without leaking sensitive data. Meanwhile, Reference [10] mentions that every massive equipment update will cause communication workload; hence, apart from conducting partial updates, it is also necessary to do data compression. Reference [10] compares the accuracy and communication costs of the three experiments. The first method is to update all models, the second one is partial updates with data compression, and the third one is to conduct device self-training. The results prove that the second method indeed lowers communication costs and still obtains excellent accuracy. Reference [7] shows that there are many data transmission in IoV; yet, IoV usually has a higher packet loss rate; hence, the study employs blockchain to save and verify messages, protecting cars' privacy and message security verification. Finally, Reference [4] suggests that if each car in IoV uses federated learning techniques, the approach will allow cars to judge IoT conditions and reduce IoV communication cost.

This article utilizes Faster R-CNN to identify objects, judge road conditions, and share messages and videos by push notifications with drivers in the social group. Additionally, with the federated learning technique, the study improves the model parameters of dashboard cameras in cars to enhance recognition accuracy.

## 3 THE PROPOSED SCHEME

This Section will introduce the system model (3.1), 6G Network Transmission Setting and Privacy Protection (3.2), Faster R-CNN (3.3), Federated Learning (3.4), and Congestion detection and Machine Learning (3.5).

### 3.1 System Model

The system model of this study is shown in Figure 1; it assumes that every vehicle has installed a dashboard camera with 6G Network functions and a GPS sensor, and both metropolitan and rural areas have built 6G Network base stations for sufficient Internet services. When an accident happened between Car $V_{p,3}$ and Car $V_{p,2}$, cars passed the scene can share the videos and GPS information from their dashboard cameras for judging the details and point out the location for third-party legal units to implement the standard operating procedure. On the other hand, when the camera on Car $V_{p,6}$ captures a roadworks sign, the camera will identify objects from the videos and send the video clip with relevant information as a push notification. Furthermore, the system will judge traffic jams from the videos on dashboard cameras and deliver notifications to responsible units. The cryptography between cars and base stations will conduct identification authentication and produce anonymous IDs to avoid malicious tracking. All videos and messages will only send between base stations and cars, avoiding hackers amend the messages maliciously or forge identities. The 6G Network's SIM card can do authentication at base stations, evading the situations of forged base station sites to steal car information. The information security in base stations can ensure drivers' identification and data privacy.

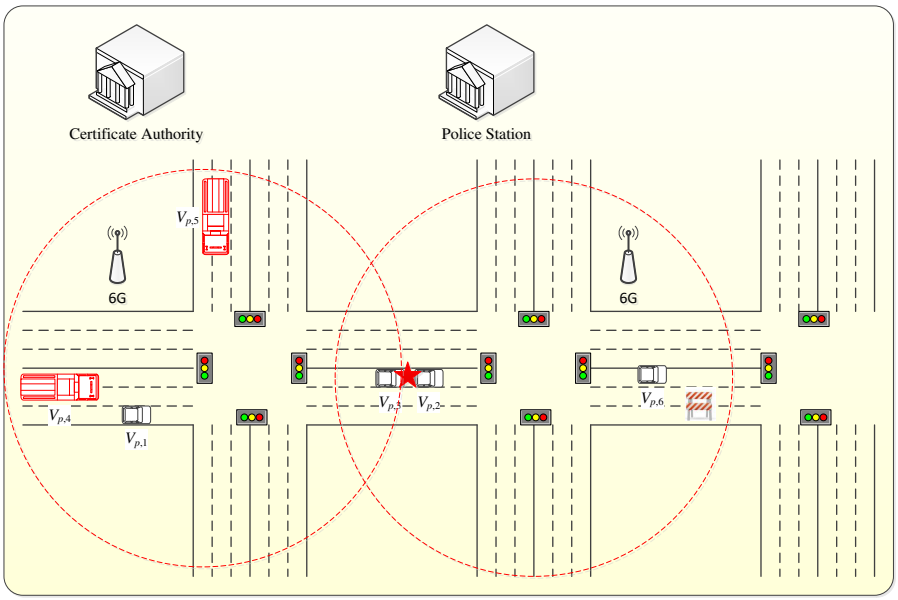



**Fig. 1** System Diagram

### 3.2 6G Network Transmission Setting and Privacy Protection

This article uses the 6G Network for IoV transmission, and the speed can be up to 1 THz ; it assumes that the 6G Network supports MIMO technology and possesses the priority processing mechanism for data packets. Meanwhile, the IoV of this study will need to implement privacy protection by identifying drivers' authentication from the serial number on SIM cards. The system employs bilinear pairings to process identification authentication, private communication, and develop anonymous IDs. Firstly, using the public key $\left(\mathcal{PR}_{ID_{t,B_i}}\right)$ and private key $\left(\mathcal{PR}_{ID_{t,B_i}}\right)$ from a base station to proceed with private communication, and Car $(ID_{t,V_i})$ will send encrypted SIM card information and the private key to the base station through the public key, which is $\mathcal{PK}_{ID_{t,B_i}}\left(SIM_{ID_{t,V_i}}||CK_{ID_{t,V_i}}||h_{ID_{t,V_i}}\right)$, where $SIM_{ID_{t,V_i}}$ is the SIM card serial number of the car, $CK_{ID_{t,V_i}}$ is the key from symmetric encryption between the base station and the car, and and $h_{ID_{t,V_i}}$ is the vehicle's anonymous ID. When the base station receives an encrypted message from a car, it will decrypt the data with a private key and build the symmetric encryption by $CK_{ID_{t,V_i}}$. The calculation for the car's anonymous ID is $ID_{p,V_i} = H\left(h_{ID_{t,V_i}}||SIM_{ID_{t,V_i}}\right)$. Next, the base station will transmit the encrypted message back to the car, $ID_{p,V_i} = H\left(h_{ID_{t,V_i}}||SIM_{ID_{t,V_i}}\right)$, allowing the car to decrypt the message by $CK_{ID_{t,V_i}}$ after receiving the data. During the message transmission process, only the car and the base station can have $CK_{ID_{t,V_i}}$, blocking other vehicles or hackers to decrypt the message even if they have received the data. Moreover, the anonymous ID will change whenever a car sends a new message, as the calculation $ID'_{p,V_i} = H\left(h_{ID_{t,V_i}}||ID_{p,V_i}\right)$, where $H$ represents the Hash function. Consequently, other cars or hackers cannot derive $h_{ID_{t,V_i}}$ and $ID_{t,V_i}$ from $ID_{p,V_i}$. If a car sent a malicious message or attempted to conduct a hacker attack, we could find out the actual identity of the car from $h_{ID_{t,V_i}}$ and $ID_{t,V_i}$.

### 3.3 Faster R-CNN

Our study recognizes objects by Faster R-CNN, as Figure 2 demonstrates. The selective search theory is similar to image segmentation, applying a hierarchical grouping algorithm to generate object proposal. Because of the hierarchical relationship between objects, the sizes of the objects will become uncertain in images; thus, the selective search will consider every large or small area altogether. The system utilizes similarities to proceed with image segmentation, merging alike blocks if the similarities are high by the formula, $d\left(C_i,C_j\right) = \sum_{a\in C_i\cup C_j} \|a-u\|$. Afterward, the process will calculate eigenvalues by the input image $I$ and filter $F$ after segmenting the image. The formula of convolutional layers is:

$$G\left[i,j\right] = \sum_{u=-k}^{k}\sum_{v=-k}^{k} I\left[i-u, j-v\right] F\left[u,v\right] \tag{1}$$

Next, output the convolutional layers on RGB images:

$$C\left(i,j\right)=\sum_{m=1}^{3}C_{m}\left(i,j\right),\forall i,j \tag{2}$$

The pooling layer calculation is:

$$P\left(i,j\right)=\frac{1}{2n}\sum_{u=0}^{n-1}\sum_{v=0}^{n-1}C\left(ni-u,nj-v\right),\forall i,j \tag{3}$$

Finally, the eigenvalue formula is:

$$\hat{y}=\text{Softmax}\left(Wf+b\right) \tag{4}$$

Afterward, define the loss function of Region Proposal Network (RPN) as:

$$L\left(\left\{pi\right\},\left(t_{i}\right)\right)=\frac{1}{N_{cls}}\sum_{i}L_{cls}\left(pi,pi^{*}\right)+\lambda\frac{1}{N_{reg}}\sum_{i}pi^{*}L_{reg}\left(t_{i},t_{i}^{*}\right) \tag{5}$$

With the RPN calculation, we can find some Region of Interests (ROIs) to match the image features. By inputting the values into ROIHead to sort ROIs and divide them into various categories and refine the locations of those ROIs.

The CNN model will correct the parameters and further amend the weights $W$ for the parameters in the loss function as $W\leftarrow W-\eta\Delta W$, generating a partial differential equation for the loss function as:

$$\Delta b=\frac{\partial L}{\partial b}=\frac{\partial L}{\partial b}\frac{\partial b}{\partial W}=\Delta\hat{y} \tag{6}$$

Assuming the learning rate as $\eta\in\left(0,1\right]$, and amended the parameter as $b\leftarrow b-\eta\Delta b$, the inverse function of the corrected weights in the pooling layer becomes $\Delta P\left(i,j\right)=F^{-1}\left(\Delta f\right)$. The corrected value of convolutional layers can be derived from amplifying the pooling layer. Therefore, the corrected value of the convolutional layers is:

$$\Delta C\left(i,j\right)=\frac{1}{2n}\Delta P\left(\left\lceil\frac{i}{n}\right\rceil,\left\lceil\frac{j}{n}\right\rceil\right),\forall i,j \tag{7}$$

Set the learning rate as $\eta\in\left(0,1\right]$, and we can obtain the corrected parameter from $b_{i}\leftarrow b_{i}-\eta\Delta b_{i}$.

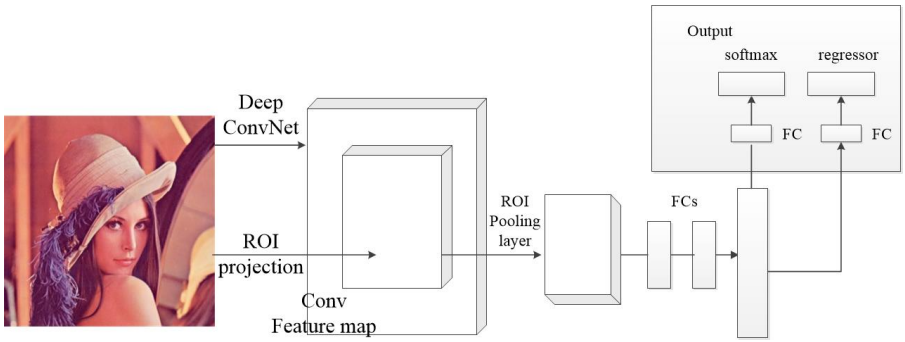



**Fig. 2** Faster R-CNN schematic diagram

### 3.4 Federated Learning

The research identifies road conditions from dashboard cameras. Set the dataset $D_i$ in videos as $D_i = d_1 \cap d_2 \cap ... \cap d_n$, and the dashboard camera will extract images chronologically to identify objects. When encountering a failure in recognition, the model will calculate the loss function and weight values based on the formulas in Section 3.3. This study applies horizontal federated learning, enabling bilinear pairing techniques to build identity-based encryption between the dashboard cameras and the server. All cameras and servers have public keys $\left(\mathcal{PK}_{ID_{t,B_i}}\right)$ and private keys $\left(\mathcal{PR}_{ID_{t,B_i}}\right)$, where $\mathcal{PK}_{ID_{t,B_i}} = ID_{t,B_i} \cdot P$. The model utilizes the public key generated by the camera ID and produces a private key from the secret key $s$, where only the server knows the secret key s that the camera or other units cannot obtain. The formula of the private key is $\mathcal{PR}_{ID_{t,B_i}} = ID_{t,B_i} \cdot s \cdot P$. When dashboard A and server B are processing private communication, they only need to attain each other's ID to generate a common session key, which allows them to implement symmetric encryption. The calculation of the common session is $\mathcal{CS}_{ID_{t,B_A} \leftrightarrow ID_{t,B_B}} = e\left(\mathcal{PR}_{ID_{t,B_A}}, \mathcal{PK}_{ID_{t,B_B}}\right)$. When dashboard camera A sends dataset $x_i^A$ to server B, the private communication calculation between them is $\mathcal{SK}_{\mathcal{CS}_{ID_{t,B_A} \leftrightarrow ID_{t,B_B}}}\left(x_i^A\right) || ID_{t,B_A}$. When server B received the encrypted data, it will decrypt the message by $\mathcal{CS}_{ID_{t,B_A} \leftrightarrow ID_{t,B_B}}$; even if other vehicles attained A and B's IDs, they could not have the secret key $s$, ensuring communication privacy and security.

When server B attains the dataset $x_i^A$ from dashboard A, it will initiate the model training with the formula below:

$$\min_{\Gamma A \leftrightarrow \Gamma B} \sum_i \left\| \Gamma A x_i^A + \Gamma A x_i^B - med_i^B \right\|^2 + \frac{\lambda}{2}\left( \left\| \Gamma A x_i^A \right\|^2 + \left\| \Gamma A x_i^B \right\|^2 \right) \quad (8)$$

, where $med_i^B$ represents the videos that encountered recognition failure, $\Gamma$ is the model of the training evaluation board, and $\lambda$ represents the normalization parameter. Set $u_i^A = \Gamma A x_i^A, u_i^A = \Gamma B x_i^B$, the formula is $\|L_A\| = \left\| \sum_i \left(u_i^A\right)^2 + \frac{\lambda}{2} \|\Gamma A\|^2 \right\|$,

$\|L_B\| = \left\| \sum_i \left(u_i^B - med_i^B\right)^2 + \frac{\lambda}{2} \|\Gamma B\|^2 \right\|$. Next, by integrating $\|L_A\|$ and $\|L_B\|$, the result becomes $\|L_{AB}\| = 2 \sum_i \left\| u_i^A \left(u_i^B - med_i^B\right) \right\|$. To obtain the optimal solution of the loss function, we apply gradient descent to create below calculation:

$$\left\| \frac{\partial L}{\partial \Gamma A} \right\| = 2 \sum_i \|d_i\| \, x_i^A + \|\lambda \Gamma A\|, \left\| \frac{\partial L}{\partial \Gamma B} \right\| = 2 \sum_i \|d_i\| \, x_i^B + \|\lambda \Gamma B\| \quad (9)$$

After attaining $\left\| \frac{\partial L}{\partial \Gamma A} \right\|$ and $\left\| \frac{\partial L}{\partial \Gamma B} \right\|$, the system can transmit relevant loss function information to other dashboard cameras, allowing them to update data.

### 3.5 Congestion detection and Machine Learning

Employing the driving speeds, directions, and positions from GPS information, this research can detect traffic jams. The definition of congestion sets to be at half of the maximum speed limit $(SP_{half})$. Firstly, the system will judge if the average driving speed is lower than $SP_{half}$; if yes, it means the car is experiencing congestion. The formula is:

$$RS = \begin{Bmatrix} true, SP_{avg} <= SP_{half} \\ false, otherwise \end{Bmatrix} \quad (10)$$

, where $RS$ reveals the congestion condition and $SP_{avg}$ shows the average driving speed.

The system in this article selects messages for drivers based on the GPS information, as dashboard cameras will have the current GPS data for the system to calculate distances and eliminate those position data that are too far away. Next, the model will sort the data by Support Vector Machine (SVM) in machine learning, such as putting road maintenance and road construction signs into the category of roadworks. Sorting messages by SVM into n categories, the formula is as below:

$$\max_w \left\{ \frac{n}{\|w\|} \right\} \rightarrow \min_w \frac{1}{n} w^T w \quad (11)$$

Afterward, the result is as below:

$$y_i \left(w^T x_i + b\right) \geqslant 1 \quad (12)$$

, where $x_i$ represents the information after Fast R-CNN and $y_i$ shows the message after running SVM.

## 4 Experimental Results

This section discusses the network security analysis in Section 4.1, and summarizes the system results in Section 4.2.

### 4.1 Network Security Analysis

The study applies bilinear pairing techniques to implement network security and privacy protection. Encrypt the car's SIM card serial number by the public key of a cell site and building a session key between the car and the base station; the system can conduct private communication. During the process, if any vehicle wants to decrypt the message in the public key, it will need to have the private key from the base station, and it is not possible to obtain the secret key of the base station from the public key. Cars can build a common session key with the server through identity-based encryption, and each of the common session keys between a car and a server is unique because the calculated values by bilinear pairing from Car ID, server ID, and the secret key are different. For any cars that attempt to forge the common session key, it will need to attain the secret key; however, from the feature of bilinear pairing technology, even if hackers managed to have the common session key, car ID, and server ID, they cannot derive the secret key from the data. According to the above analysis, the transmission between cars and base stations is safe, ensuring messages' data security and privacy.

### 4.2 Results of the System

The dashboard camera of our research consists of Raspberry Pi, GPS, and a camera lens, as shown in Algorithm 3. The Raspberry Pi supports identifying the objects in videos; when the system detects road issues, it will send a message to the server, and the server will share the road condition by push notifications. Algorithm 4 demonstrates the push notification hardware, and the system can judge road conditions from videos. As shown in Algorithm 5, the system uses Faster R-CNN for recognition and have 3,000 images for training and 1,000 images for testing. Algorithm 6 reveals that the proposed approach can achieve a decent recognition rate. The system amends Faster R-CNN weights by federated learning, as shown inAlgorithm 7, obtaining the optimal solution by gradient descent.

## 5 Conclusion

This article aims to develop an IoV traffic condition system by AIoT, identifying road conditions through recognizing video objects in dashboard cameras and sharing with nearby cars to improve traffic safety. In the past, most IoV systems work based on the messages provided by drivers, and this proposed approach automatically sends video clips by push notifications for drivers to be aware of the road conditions. Additionally, to ensure network security and data privacy, our system applies bilinear pairing technology to build the mechanism. The safety analysis section has proven data security and privacy during transmission; moreover, from the experimental results, this system proves the feasibility in practical operation with an adequate recognition rate. By sending push notifications to specific social groups, the drivers in the group can be aware of the road conditions, enhancing traffic safety. In this study, the system utilizes

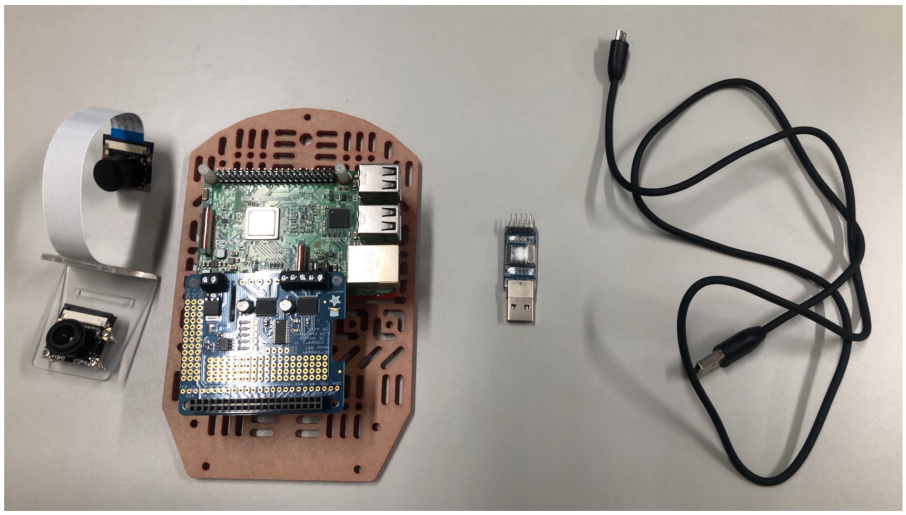
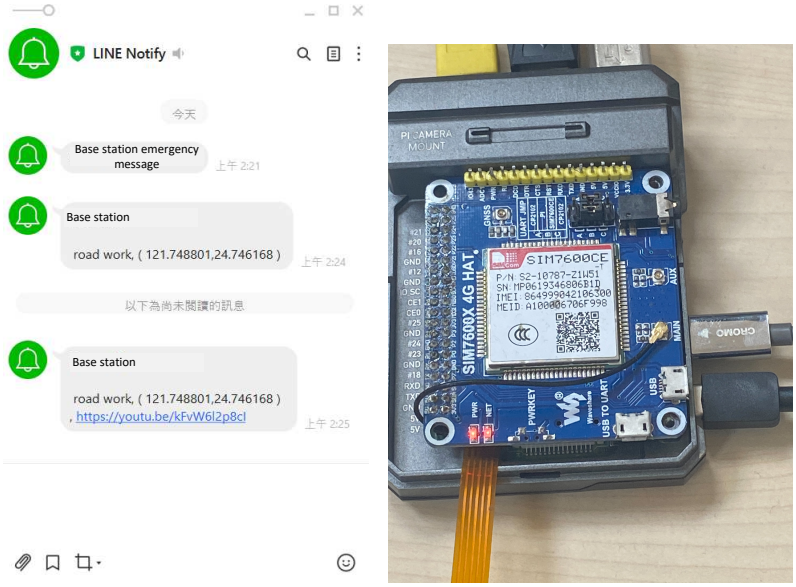


**Fig. 3** Development hardware tools

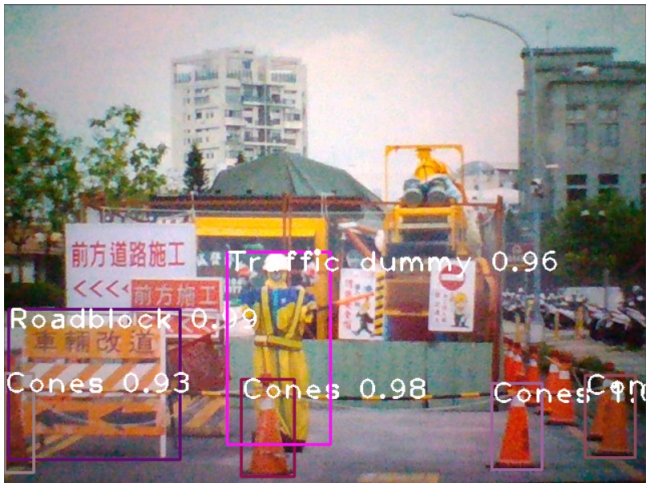



(a) Push Broadcast System (b) Push broadcast system hardware

**Fig. 4** Push Broadcast System experiment results

dashboard cameras in cars to detect situations; with the camera and GPS functions, the system can recognize video objects and locate car positions. Furthermore, the suggested method does not require to build massive fixed monitoring equipment for surveillance, which fosters the implementation and penetration of IoV systems.


(a) Campus construction




(b) Road work

**Fig. 5** Faster R-CNN experiment results

## 6 Acknowledgement

The authors would like to thank the anonymous reviewers for their valuable comments and suggestions on the paper. This work was supported in part by the Ministry of Science and Technology of Taiwan, R.O.C., under Contracts MOST 109-2622-E-197 -012.

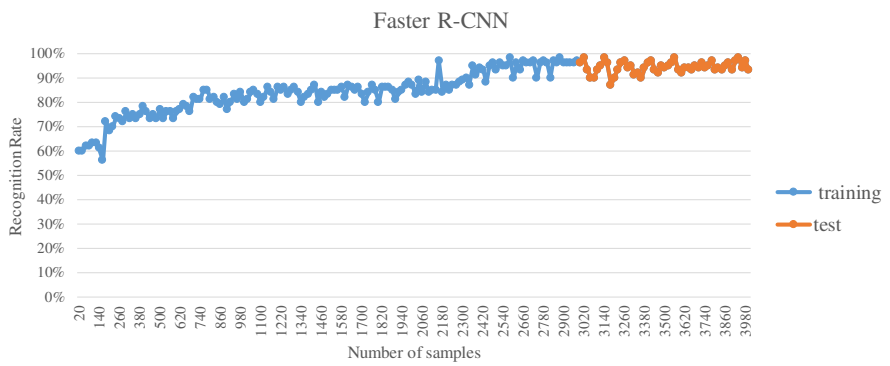



**Fig. 6** Faster R-CNN recognition rate

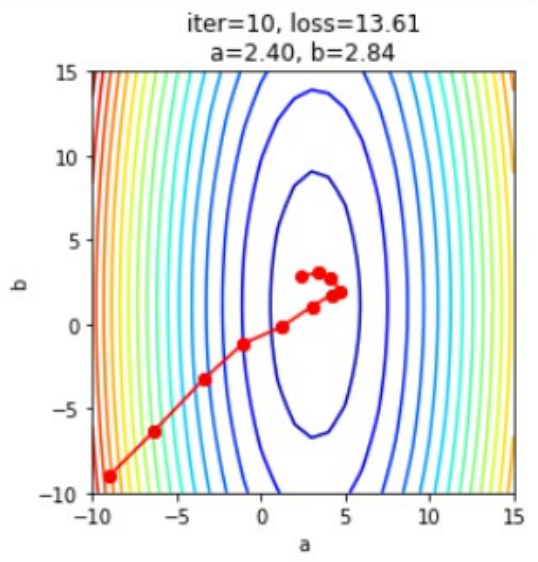



**Fig. 7** Federated Learning experiment results

## 7 Conflict of Interest

The authors declared that they have no conflicts of interest to this work. We declare that we do not have any commercial or associative interest that represents a conflict of interest in connection with the work submitted.

## References

1. Akyildiz, I.F., Kak, A., Nie, S.: 6g and beyond: The future of wireless communications systems. IEEE Access **8**, 133995–134030 (2020)
2. Asheralieva, A., Niyato, D.: Distributed dynamic resource management and pricing in the iot systems with blockchain-as-a-service and uav-enabled mobile edge computing. IEEE Internet of Things Journal **7**(3), 1974–1993 (2020)

3. Chowdhury, M.Z., Shahjalal, M., Ahmed, S., Jang, Y.M.: 6g wireless communication systems: Applications, requirements, technologies, challenges, and research directions. IEEE Open Journal of the Communications Society **1**, 957–975 (2020)
4. Du, Z., Wu, C., Yoshinaga, T., Yau, K.L.A., Ji, Y., Li, J.: Federated learning for vehicular internet of things: Recent advances and open issues. IEEE Open Journal of the Computer Society **1**, 45–61 (2020)
5. Khosravi, M.R., Samadi, S.: Reliable data aggregation in internet of visar vehicles using chained dual-phase adaptive interpolation and data embedding. IEEE Transactions on Industrial Informatics **7**(4), 2603–2610 (2020)
6. Lu, Y., Huang, X., Dai, Y., Maharjan, S., Zhang, Y.: Blockchain and federated learning for privacy-preserved data sharing in industrial iot. IEEE Transactions on Industrial Informatics **16**(6), 4177–4186 (2019)
7. Lu, Y., Huang, X., Zhang, K., Maharjan, S., Zhang, Y.: Blockchain empowered asynchronous federated learning for secure data sharing in internet of vehicles. IEEE Transactions on Vehicular Technology **69**(4), 4298–4311 (2020)
8. Ni, Y., Cai, L., He, J., Vinel, A., Li, Y., Mosavat-Jahromi, H., Pan, J.: Toward reliable and scalable internet of vehicles: Performance analysis and resource management. Proceedings of the IEEE **108**(2), 324–340 (2020)
9. Ren, J., Wang, H., Hou, T., Zheng, S., Tang, C.: Federated learning-based computation offloading optimization in edge computing-supported internet of things. IEEE Access **7**, 69194–69201 (2020)
10. Sattler, F., Wiedemann, S., Müller, K.R.: Robust and communication-efficient federated learning from non-i.i.d. data. IEEE Transactions on Neural Networks and Learning Systems **31**(9), 3400–3413 (2019)
11. Sergiou, C., Lestas, M., Antoniou, P., Liaskos, C., Pitsillides, A.: Complex systems: A communication networks perspective towards 6g. IEEE Access **8**, 89007–89030 (2020)
12. Wang, J., Cai, Z., Yu, J.: Achieving personalized k-anonymity-based content privacy for autonomous vehicles in cps. IEEE Transactions on Industrial Informatics **16**(6), 4242–4251 (2019)
13. Wang, J., Li, J., Wang, H., Zhang, L.Y., Cheng, L.M., Lin, Q.: Dynamic scalable elliptic curve cryptographic scheme and its application to in-vehicle security. IEEE Internet of Things Journal **6**(4), 5892–5901 (2019)
14. Wang, S., Tuor, T., Salonidis, T., Leung, K.K., Makaya, C., He, T., Chan, K.: Adaptive federated learning in resource constrained edge computing systems. IEEE Journal on Selected Areas in Communications **37**(6), 1205–1221 (2019)
15. Zhang, S., Xiang, C., Xu, S.: 6g: Connecting everything by 1000 times price reduction. IEEE Open Journal of Vehicular Technology **1**, 107–115 (2020)
16. Zhu, H., Jin, Y.: Multi-objective evolutionary federated learning. IEEE Transactions on Neural Networks and Learning Systems **31**(4), 1310–1322 (2020)