An Intelligent Edge-Chain-Enabled Access Control Mechanism for IoV

Yuanni Liu, Man Xiao, Shanzhi Chen, *Fellow, IEEE*, Fan Bai, Jianli Pan, *Member, IEEE*, and Di Zhang, *Senior Member, IEEE*

***Abstract*—The current security method of Internet-of-Vehicles (IoV) systems is rare, which makes it vulnerable to various attacks. The malicious and unauthorized nodes can easily invade the IoV systems to destroy the integrity, availability, and confidentiality of information resources shared among vehicles. Indeed, access control mechanism can remedy this. However, as a static method, it cannot timely response to these attacks. To solve this problem, we propose an intelligent edge-chain-enabled access control framework with vehicle nodes and roadside units (RSUs) in this study. In our scenario, vehicle nodes act as lightweight nodes, whereas RUSs serve as full and edge nodes to provide access control services. Considering the low accuracy of risk prediction due to limited training sets, we leverage a generative adversarial networks (GANs) to convert the risk prediction to a sequence generation. Moreover, aiming at the problems of gradient disappearance and mode collapse existed in the original GANs, we devise a Wasserstein combined GANs (WCGANs). Simulation results demonstrate that WCGAN has higher prediction accuracy than the original GANs. Additionally, it can also improve the accuracy of access control of risk prediction-based access control (RPBAC) model.**

***Index Terms*—Access control, blockchain, edge computing (EC), generative adversarial networks (GANs), Internet of Vehicles (IoV).**

Manuscript received August 1, 2020; revised November 12, 2020 and December 9, 2020; accepted February 17, 2021. Date of publication February 23, 2021; date of current version July 23, 2021. This work was supported in part by the Open Fund of the Ministry of Education Key Laboratory of Networks Security and Intelligent Technology, Beijing University of Posts and Telecommunications; in part by the General Program of Natural Science Foundation of Chongqing under Grant cstc2020jcyj-msxmX1021; in part by the Science and Technology Research Program of Chongqing Municipal Education Commission under Grant KJZD-K202000602; in part by the National Science Fundation of China (NSFC) under Grant 62001423; in part by the Henan Provincial Key Research, Development and Promotion Project under Grant 212102210175; and in part by the Henan Provincial Key Scientific Research Project for College and University under Grant 21A510011. *(Corresponding author: Di Zhang.)*

Yuanni Liu is with the School of Cyber Security and Information Law, Chongqing University of Posts and Telecommunications, Chongqing 400065, China (e-mail: liuyn@cqupt.edu.cn).

Man Xiao is with the School of Communication and Information Engineering, Chongqing University of Posts and Telecommunications, Chongqing 400065, China (e-mail: 2802646455@qq.com).

Shanzhi Chen is with the State Key Laboratory of Wireless Mobile Communications, China Academy of Telecommunication Technology, Beijing 100191, China (e-mail: chensz@cict.com).

Fan Bai is with the Beijing Institute of Spacecraft System Engineering, Beijing 100094, China (e-mail: baifan_waseda@163.com).

Jianli Pan is with the Department of Computer Science, University of Missouri, St. Louis, MO 63121 USA (e-mail: pan@umsl.edu).

Di Zhang is with the School of Information Engineering, Zhengzhou University, Zhengzhou 450001, China (e-mail: dr.di.zhang@ieee.org).

Digital Object Identifier 10.1109/JIOT.2021.3061467

I. Introduction

INTERNET of Vehicles (IoV) utilizes effective wireless communication to share information among vehicles [1]–[3], which helps to achieve self-driving and maintain the traffic safety [4], [5]. Recently, a green-car report finds that the amounts of vehicles exceed one billion and is expected to reach two billion by 2035 [6], [7]. As explosive on-road devices are connecting to Internet, communication security becomes a big issue. As we know, the communication security method of current IoV devices is rare, making it easy to be attacked. Such malicious attacks include replay, camouflage, message tampering attacks, etc., [8]. The attacked IoV devices may rise potential risks, such as critical electronic control unit hacking and control, untrustworthy messages from attacked devices. Meanwhile, due to the pervasive distribution and mobility features of vehicles, the current centralized cloud model is difficult to expand through massive weak devices [9]. Moreover, the communication distance between IoV devices and clouds is relatively long, which may consume amounts of bandwidth, time and energy. The cloud server is a bottleneck of current IoV networks. A single failure of the server will disrupt the entire network. Therefore, it is critical to prevent unauthorized access to the IoV ecosystems on a large-scale area, which is one of the motivations of this article.

On the other hand, in our previous work, we have integrated blockchain and smart contracts capabilities into the intelligent edge computing (EC) framework as the foundations [10], [11]. The goal is to develop a resource-oriented and blockchain-embedded edge Internet-of-Things (IoT) framework named edge chain to provide the quality of experience services for IoT devices and to control their behaviors. In our intelligent edge-chain ecosystems, EC provides a possible solution by pushing more resources to the edge, including intelligence, networking, computing, and storage resources. The IoT applications that are delay sensitive, data sensitive, and bandwidth constrained can benefit from it. In addition, for the sake of resource and jurisdiction constraints, edge nodes cannot provide comprehensive services for IoT devices [12]. Therefore, blockchain can bring in a decentralized edge cloud solution, in which applications perform operations without a trusted intermediary [13]. Additionally, combined with smart contracts, blockchain can enable a trustless environment and provide a system with validity, traceability, faulty tolerance, and the automatic execution of policy. The integration of blockchain also enables behavior identification of IoT devices, and fault tolerance through consensus mechanisms such as practical Byzantine fault tolerant [14], even when some edge servers are compromised. Despite the proposed edge chain implemented in the IoT area, to the best of our knowledge, very few effort has combined the blockchain and smart contracts based on the edge IoV systems. Therefore, we try to leverage our edge-chain concept in the IoV access control area. The goal is to construct an intelligent and blockchain-embedded edge-chain-enabled system to tackle the key challenges collectively by facilitating the secure access control for IoV devices.

However, traditional access control mechanisms, such as role-based access control (RBAC) [15] and attribute-based access control (ABAC) [16], are usually static, which makes it difficult to adapt to frequent changes of IoV devices. For example, RBAC restricts network access based on the roles of IoV devices. Once an IoV device has obtained the accessible permissions, the device will maintain the permissions for a certain period. It is thus hard for the current IoV access control mechanism to make a timely response while encountering some attacks. To this end, machine learning algorithms have been introduced to dynamic access control mechanisms in the IoV systems. By analyzing the historical behavior of IoV devices, a risk prediction model was constructed [17]. However, machine learning-based accurate risk prediction requires a lot of data for training, which is tricky to be adopted directly. In order to solve this problem, the generative adversarial networks (GANs) are widely developed, such as image generation, video generation and so on. GANs utilize generator and discriminator to play a zero-sum game to achieve Nash equilibrium, and finally produce suitable training samples [18]. Consequently, GANs can guarantee a satisfactory accuracy even with less training sets by using the generated samples to fine-tune and optimize. However, the mode collapse and gradient disappearance are some challenges of the original GANs. In the early training stage, poor learning ability of generator results in nasty collapses and produces limited varieties of samples. Consequently, the discriminator is easy to distinguish generated samples. There will be no effective gradient information of discriminator fed back to the generator, leading to low accuracy of prediction of generator and slow convergence speed of GANs.

In order to cope with these problems, we introduce an edge-chain-enabled system to facilitate the secure access control of IoV devices in this study. Furthermore, to accommodate the frequent network status changes of IoV devices, we propose a dynamic access control model, named risk prediction-based access control (RPBAC). We also introduce GANs to get rid of the constraint of training set number. Additionally, aiming at the problems of gradient disappearance and mode collapse in the original GANs, we design a Wasserstein combined GANs (WCGANs) method, which is inspired by Wasserstein GANs (WGANs) method in [19] and two discriminators used in progressive growing of GANs (D2PGGANs) method in [20]. The main contributions of this article are summarized as follows.

1) We introduce an intelligent edge-chain system, to enable a flexible and secure access control framework for IoV devices. In our framework, the blockchain network consists of vehicle nodes and roadside units (RSUs), where vehicle nodes act as lightweight nodes. On the contrary, RSUs act as full nodes, which also serve as edge nodes, providing access control service for vehicle nodes. IoV activities are recorded as transactions in the blockchain for secure data auditing. An intelligent management and control module is built to provide the edge nodes with intelligence to generate access control policies based on the behavior data of vehicle nodes stored in the blockchain. The access rules and policies enforcement are programmed as smart contracts and integrated into the proposed framework to regulate and audit the access behaviors of vehicle nodes.
2) In the intelligent management and control module, we propose an RPBAC model to predict the risk level based on historical behaviors, and to assign IoV devices with different access authorities based on their predicted level. Aiming at the constraint of training set number on the accuracy of machine learning models, we select the GANs to convert the problem of risk prediction to a sequence generation problem. The generator of GANs can generate new sequences by fitting the probability distribution of real data sets, which can be used to improve the accuracy of prediction of generator.
3) In order to overcome the problems of gradient disappearance and mode collapse in the original GANs, we introduce a WCGANs. By using multiple generators, the improved GANs can cover the probability distribution of different modes.

The remainder of this article is organized as follows. Section II discusses the related work. Section III describes the edge-chain-enabled access control framework, and Section IV introduces the RPBAC model. Section V describes the problems existed in the original GANs, formulates the WCGAN method and explains the related algorithm. Section VI presents and analyzes the experimental results of the proposed method and the proposed model. This article is finally concluded in Section VII.

II. Related Works

The current access control mechanisms are based on the centralized architecture and distributed architecture. In a centralized architecture, all logics of decision are transferred to a single central module. For example, Denis *et al.* [21] have proposed a secure data exchange method for vehicle to everything system, in which records contained sensitive information and access control policies are stored in cloud in an encrypted form. The resource owner acquires the access authority of requesting node through structured query language. Daewon *et al.* [22] have leveraged an RBAC model, and established a self-registration vehicle management system. Once a vehicle has registered the management items to the management system, the system can automatically create and management the policies of this accessing item. However, like most centralized architectures, these solutions have a single point of failure [23]. In a distributed architecture, decision logics are built by resource owners themselves. For example, Marcel *et al.* [24] have presented an adapted ABAC model for automotive architectures. The model uses different functional modules to preserve multiple communication channels and prevent unauthorized access. Dina *et al.* [25] have devised a community-based access control structure for IoT devices, in which the devices with resources constraints can evaluate access authorities of external entities without a central authorization system.

In order to accommodate the high mobility of vehicles, novel technologies have been proposed for the IoV network. Such as EC, which aims at reducing latency by offloading services to the edge of network [26]. Celimuge *et al.* [27] have exploited decentralized mobile edge and multitier edge clustering to meet the requirements of high throughput and low latency, by conducting distributed data caching and computing at edge vehicles. Celimuge *et al.* [28] have proposed a collaborative learning-based routing scheme for multiaccess vehicular EC environment. This scheme can find routes with low communication overhead by utilizing a reinforcement learning algorithm on the basis of end-edge-cloud collaboration. By integrating proactive and preemptive actions, this scheme achieves better packets forwarding speed. Similarly, Jingyun *et al.* [29] have designed an autonomous edge/cloud hybrid framework to improve the computation capability by utilizing the available computing resources among nearby vehicles, RSUs and cloud through multiple access networks. Guanhua *et al.* [30] have leveraged the flexible trilateral cooperation among macrocell stations, RSUs and smart vehicles, and proposed a cooperative edge caching scheme for the IoV. The RSUs serve as edge nodes to decide which content should be cached, and minimize the access cost of content. However, neighboring vehicles perhaps reluctant to cache information of other dishonest devices.

Recently, blockchain has attracted much attention [11]. Zhenyu *et al.* [31] have presented an energy trading model for demand response to improve the security of Internet of Electric Vehicles (IoEV), by integrating computing intelligence, blockchain, and smart contracts. Among them, blockchain is used to guarantee the security of energy trading by encrypting and digitally signing. Smart contracts customize contracts according to the distinct characteristics of each EV type, maximizing social welfare. Computing intelligence derives the probability distribution of EV types through offline training and online estimation. Madhusudan and Shiho [32] have designed an IoV access control framework founded on blockchain, named FairAccess. The framework treats a bitcoin system as an authorizer, and completes authorization by allocating tokens signed on behalf of resource owner. Liao *et al.* [33] have developed a task offloading framework. This framework exploits blockchain and smart contracts to mitigate various attacks and facilitate task offloading more fairness based on the possibility of success task offloading. Guy *et al.* [34] have presented a personal data management system with blockchain, considering the access control moderator and off blockchain storage solution. Designed as unique owners of their personal data, clients are aware of data collected about them by service providers and how they are used. However, it is only based on the simple permit/deny access policy through white/black listing.

The risk prediction model can provide a reference for the evaluation of access authorities by predicting the risk level of nodes. Hamzah *et al.* [35] have utilized traffic data sets to validate that the prediction model based on neural network is better to process the behavior data of vehicles than other models. Xunjia *et al.* [36] have leveraged hidden Markov model to predict steering angle status and quantity road traffic risk. The risk is directly presented in the form of time-varying risk form with improved prediction accuracy, enhancing traffic safety. However, it needs a great amount of training sets to ensure the accuracy of risk prediction. In order to solve this problem, GANs is proposed since it has good performance in learning the probability distributions of data sets. For example, Mehdi *et al.* [37] have used GANs to plan the accurate and reliable paths for navigation applications by learning the trajectories based on crowdsourced data. Yuqiang *et al.* [38] have leveraged the GANs to repair the parking data, which can improve the effectiveness of parking guidance system. However, due to the problems of gradient disappearance and mode collapse in the original GANs, it is not suitable to process vehicle behavior data directly [39]. Therefore, Martin *et al.* [19] have addressed the problem of gradient disappearance by replacing the Jensen Shannon (JS) divergence with the Wasserstein-1 distance, named WGAN. WGAN has made progress in training GANs stably, but sometimes still fails to converge since the limited learning ability of one generator. To this end, Zhaoyu *et al.* [20] have designed a new structure of GANs that consists of one generator and two discriminators. The structure alleviates the problem of mode collapse through the cooperation of two discriminators. Although the generator can better fit the distribution of real data sets under the guidance of the discriminator, the generation ability of generator has not been investigated.

III. Edge-Chain-Enabled Access Control Framework

In this section, we will discuss the overall edge-chain-enabled access control framework, core components and the process of vehicle access control.

A. Overview of the Proposed Framework

The overall system framework is shown in Fig. 1. In the proposed framework, edge chain is deployed on the RSU. The vehicle nodes act as lightweight nodes due to the constraints of storage and computing resources, whereas, the RSUs, deployed along roadside, serve as full nodes, which also considered as edge servers. Consequently, each edge server stores a copy of the entire edge chain, listening to messages and performing corresponding tasks. Along the message path, core components of the proposed framework include the blockchain integrated with smart contracts and the intelligent management and control module. In our implement, blockchain needs to store behavior data of vehicle nodes. The data, acting as the input of the intelligent management and control module, is to generate access control policies. The policies are written into smart contracts, supporting the automatic

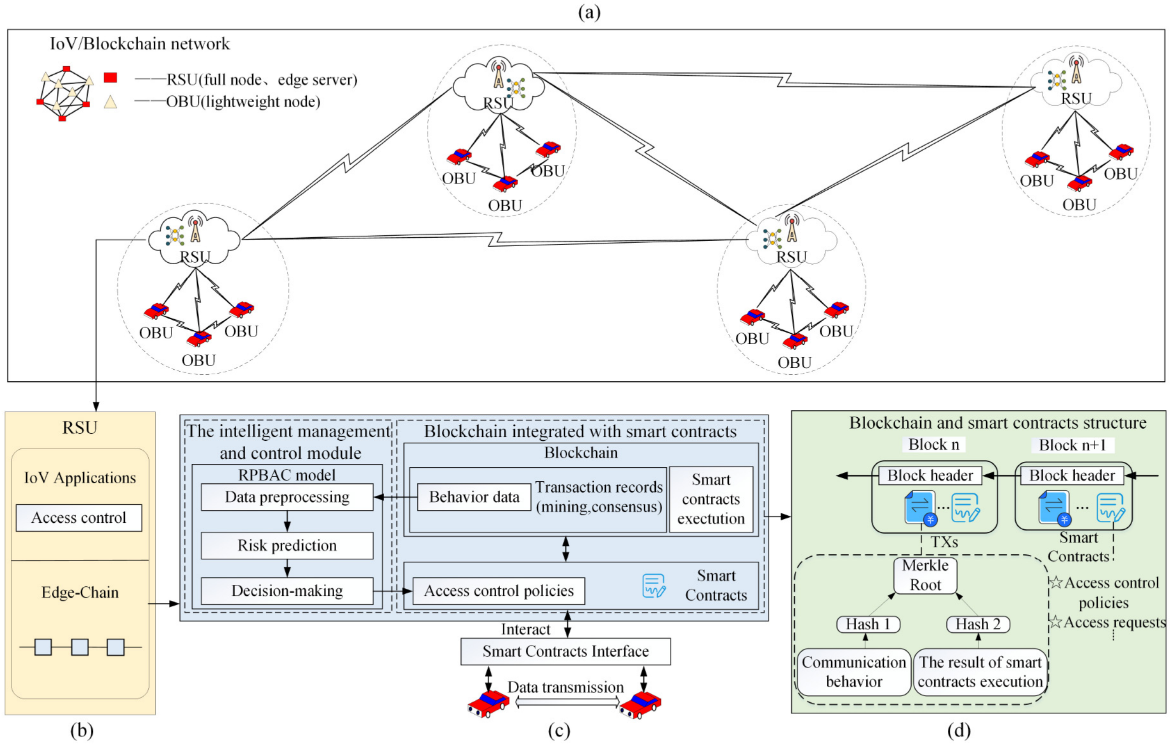

Fig. 1. Edge-chain-enabled access control framework. (a) Edge-Chain IoV System. (b) RSU. (c) Core components of the proposed framework. (d) Blockchain and smart contracts structure.

execution of access control for vehicle nodes. When a transmission activity occurs, such as information sharing among vehicles, the deployed smart contracts will be triggered to regulate and audit the access behavior of vehicles, improving the security of information resources in the IoV.

B. Core Components in the Proposed Framework

1) Blockchain Integrated With Smart Contracts: In the proposed framework, smart contracts are combined with blockchain to perform two functions. First, the blockchain is responsible for secure storing. That is, each block records a list of transactions over a given period, and every transaction has a hash associated with it. In a block, all of the transaction hashes are hashed, and the result is the Merkle root, which is utilized to prevent tampering, improving the security of storage in the blockchain. Second, the smart contracts are used to support the automatic execution of access control policies. The smart contracts are self-executing contracts. In other words, once the smart contracts become effect, the contracts will execute a predefined task if the trigger conditions are met. In the proposed framework, the request of information resources among vehicles is defined as the trigger of the smart contracts. The policy generated by the intelligent management and control module, is programmed into smart contract. The smart contract is transmitted to other full nodes for verification. We utilize the practical Byzantine fault tolerant as the consensus protocol in line with our previous work [10]. After reaching a consensus, the contract will be written into the blockchain, and become an effective contract. The programmed contract will regulate and audit the access behavior of the requesting vehicle, avoiding the abuse of resources. For example, when a vehicle node makes a malicious access behavior inconsistent with the policy, the smart contract will stop the current information sharing of the node account, prevent the malicious behavior of the node. Moreover, the behavior data will be recorded in the blockchain as the basis for evaluating the high risk of the node next time.

2) Intelligent Management and Control Module: The intelligent management and control module is responsible for intelligent decision-making. By introducing the GANs, the intelligent management and control module builds an RPBAC model. The RPBAC model obtains behavior data of the requesting vehicle from blockchain, and a numerical matrix can be obtained from the historical behaviors by data preprocessing. The numerical matrix acts as the input of the GANs to predict the risk level of the requesting vehicle. The predicted risk level, combined with the security requirements of the resource-owner vehicle, will be used to evaluate the access authorities of the requesting vehicle, and generate corresponding access control policy.

C. Process of Vehicle Access Control

In the edge-chain IoV system, nearby RSU generates access policy of requesting vehicle through the intelligent management and control module. Then, the policy is programmed into smart contract to regulate the access behavior of the requesting node. Detailed descriptions of the access control process are as follows.

1) The nearby RSU predicts the risk level of the requesting vehicle, and generates corresponding access policy through the intelligent management and control module.
2) The RSU programs the policy into smart contract.

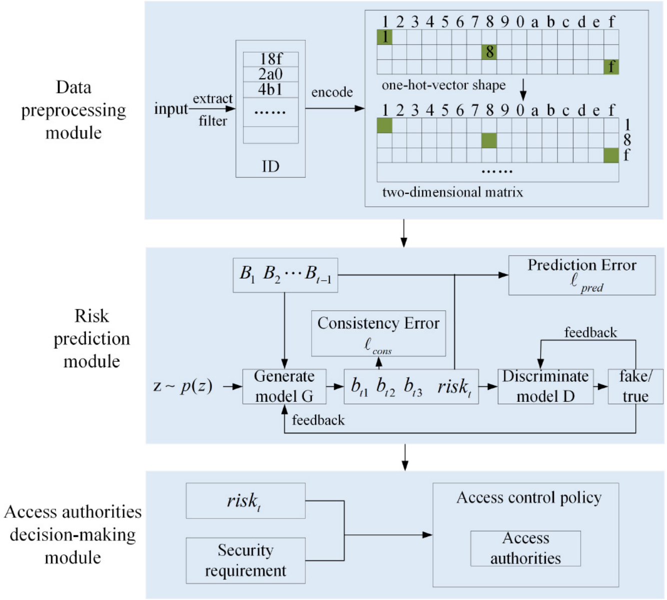

Fig. 2. RPBAC model.

3) All full nodes reach to a consensus by mining. The smart contract is recorded as transaction in blockchain.
4) The requesting vehicle accesses resources under the regulating and auditing of the smart contract.

IV. Proposed Access Control Model

In this section, we will describe the RPBAC model. As shown in Fig. 2, the model consists of data preprocessing, risk prediction and access authorities decision-making modules.

A. Data Preprocessing Module

By filtering, feature extracting and encoding, the data preprocessing module is designed to transform the input data sets into a numerical sequence or matrix that the risk prediction module can process. Specifically, in this article, the input data sets come from car-hacking data sets for intrusion detection [40], which includes denial of service attack, spoofing attack, fuzzy attack and attack-free. We first filter the invalid or corrupt values in the data sets. Then, referring to [40], identifiers (IDs) in the data sets show representative patterns of different records. Therefore, we extract the IDs from the data sets by matching keywords. The ID of each record is hexadecimal. Consequently, IDs are transformed into a 2-D feature matrix through one-hot-vector.

B. Risk Prediction Module

The major function of the risk prediction module is to predict the risk level of vehicles based on the input. Considering the constraint of training set number, this module leverages a GANs, and the problem of risk prediction can be converted to a sequence generation problem. The GANs can use not only the real data sets for training, but also the data sets generated by the generator to fine-tune the parameters of model. The prediction accuracy of GAN's generator is thus improved. As shown in Fig. 3, the GANs consist of a generator and discriminator, in which the long short-term memory acts as the generator, and the convolutional neural network acts as the discriminator. $B = \{B_1, B_2, \ldots, B_{t-1}\}$ represents the historical behavior, in which the subsequence at time $t-1$ is represented as $B_{t-1} = \{b_{t-1,1}, b_{t-1,2}, b_{t-1,3}\}$. By inputting B, the generator can generate a new sequence $B_t = \{b_{t,1}, b_{t,2}, b_{t,3}, \text{risk}_t\}$, in which risk_t represents the predicted risk level of the sequence. The discriminator distinguishes whether B_t is a real data set or a generated data set. If the result is true, it means that B_t is from a training data set, or else, the input is from the generator.

The training process of GANs can be equivalent to a "minimax game" between the generator and discriminator. The generator "cheats" the discriminator by generating new data, and the discriminator "beats" the generator by discriminating whether the data is generated or real. The objective function of GANs is calculated by

$$\min_G \max_D V(D, G) = E_{b\sim p_{\text{data}}(b)}\big[\log D(b)\big] + E_{z\sim p_z(z)}\big[\log(1 - D(G(z)))\big] \quad (1)$$

where b is a real data set conforming to the distribution $P_{\text{data}}(b)$, and z is a noisy data set conforming to the distribution $P_z(z)$. $D(G(z))$ represents the probability that the generated data set $G(z)$ is discriminated as real by the discriminator. Similarly, $D(b)$ represents the probability that b is discriminated as real. Therefore, maximizing the expectation of $\log D(b) + \log(1-D(G(z)))$ is the purpose of discriminator, while minimizing the expectation of $\log(1 - D(G(z)))$ is the purpose of generator.

C. Access Authorities Decision-Making Module

The main function of access authorities decision-making module is to determine the authorities of vehicles, on the basis of the predicted risk level of requesting vehicle and the security requirement of resource-owner vehicle. In this article, we customize the security requirement with a threshold, n. The access authority is obtained by comparing n and predicted risk level. For example, if the risk level is lower than n, the requesting vehicle can access the system resource, m.

V. Proposed Method WCGAN

In this section, we will elaborate the problems existed in the original GANs, and also introduce the proposed method WCGAN.

A. Problem Statement

1) Gradient Disappearance: The objective function of original GANs can be regarded as minimizing the JS divergence between the probability distribution P_r of real data sets and the probability distribution P_g of generated data sets, which is represented as

$$\text{KL}\big(P_r || P_g\big) = \int P_r(x) \log\left(\frac{P_r(x)}{P_g(x)}\right) \text{dx} \quad (2)$$

where P_r and P_g are continuous probability distributions. As shown in (2), if the two probability distributions do not

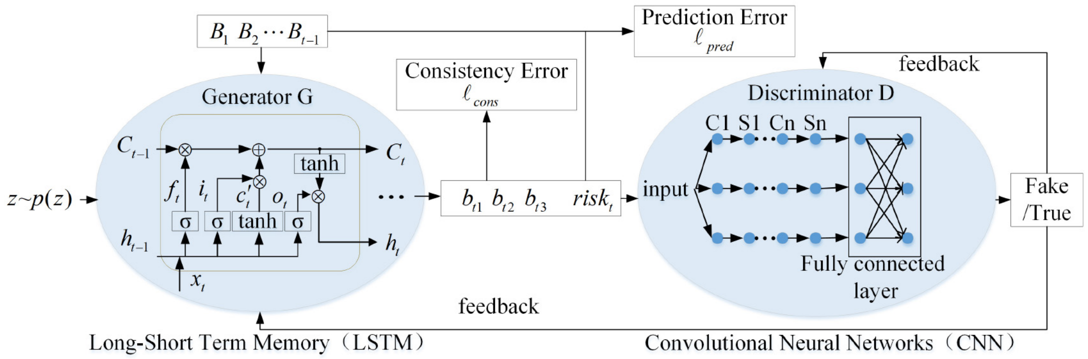

Fig. 3. Structure of GANs.

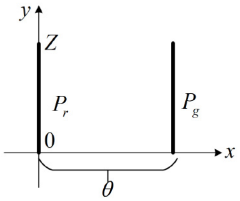

Fig. 4. Distribution P_r and P_g.

intersect, the JS divergence between them approaches to a constant. The better the discriminator is trained, the gradient of generator disappears more serious.

2) Mode Collapse: Due to the restricted ability of learning, the sole generator of GANs can only learn portion distributions of data sets, which causes deficiencies of some modes, reducing the diversity of GANs.

B. Methodology

1) Objective Function on the Basis of Wasserstein Distance: To overcome the problem of gradient disappearance, the WCGAN supersedes the JS divergence with the Wasserstein distance to measure the cost of converting P_g to P_r. The cost calculated in (3) represents the similarity of two distributions, the lower the cost is, the more similar the two are

$$W\left(P_r, P_g\right) = \inf_{\gamma\sim\prod(P_r,P_g)} E_{(x,y)\sim\gamma}\left[\|x-y\|\right] \tag{3}$$

where $\prod(P_r, P_g)$ represents all possible joint distributions of P_r and P_g. By sampling $(x, y) \sim \gamma$ from each joint distribution γ, a real data set y and a generated data set x can be obtained. The distance between two sets is calculated by $||x - y||$. Therefore, the expectation of $||x - y||$ is $E_{(x,y)\sim\gamma}[||x - y||]$. Under $\prod(P_r, P_g)$, the lower bound of $E_{(x,y)\sim\gamma}[||x-y||]$ is the Wasserstein distance, which is understood as the minimum cost.

As shown in Fig. 4, P_r is a uniform distribution of $(0, Z)$, where $Z \sim U(0, 1)$, and P_g is a uniform distribution of (θ, Z), where θ is the horizontal distance between P_r and P_g. In this way, the JS divergence and the Wasserstein distance between P_r and P_g are formulated in (4), respectively,

$$\begin{cases} JS\left(P_r||P_g\right) = \begin{cases} \log\left(\frac{P_g(x)}{\frac{1}{2}P_g(x)+0}\right) = \log 2, \text{if}\theta \neq 0 \\ 0, \text{if}\theta = 0 \end{cases} \\ W\left(P_r||P_g\right) = |\theta|. \end{cases} \tag{4}$$

If θ is equal to 0, the JS is equal to 0, otherwise, the JS is a constant. Therefore, when the gradient descent algorithm is used to optimize θ, the JS divergence cannot provide gradient information. Nevertheless, the Wasserstein distance varies with θ, which can provide an effective gradient for training.

Therefore, this article brings the Wasserstein distance into the objective function of GANs. The discriminator of GANs is a binary classifier. The last layer of discriminator is a sigmoid function to output a confidence level between 0 and 1, which is applied to judge whether the input is real or generated. In order to introduce the Wasserstein distance, the WCGAN removes the sigmoid function. Therefore, the resistance loss L_d^{Ad} of the discriminator and the resistance loss L_g^{Ad} of the generator can be expressed as

$$L_d^{Ad} = D(\tilde{s}_{0:t}) - D(s_{0:t}) \tag{5}$$

$$L_g^{Ad} = -L_d^{Ad} = D(s_{0:t}) - D(\tilde{s}_{0:t}). \tag{6}$$

In (5) and (6), $\tilde{s}_{0:t}$ represents a generated data set, and $s_{0:t}$ represents a real data set. The goal of discriminator is to minimize $D(s_{0:t}) - D(\tilde{s}_{0:t})$, on the contrary, the generator aims to minimize $D(\tilde{s}_{0:t}) - D(s_{0:t})$.

2) Combined GANs: To overcome the problem of mode collapse, the WCGAN leverages multiple generators to learn various probability distributions, which are not learned by a single generator, improving the ability of fitting real data sets and reducing the possibility of mode collapse. Fig. 5 shows a GANs composed of two generators and one discriminator, where the generators share the same input (the basis for collaboration).

Given a set of m generators, the discriminator produces a probability distribution of soft-max over $m + 1$ classes. The probability that the input belongs to a real data is denoted by $D_{m+1}(.)$. We optimize the cross entropy between the output of soft-max and the Dirac delta distribution $\delta \in \{\ 0{,}1\}^{\ m+1}$. Consequently, if the data set belongs to generator i, $\delta(i) = 1$, otherwise $\delta(m + 1) = 1$, where $i \in \{1, \ldots, m\}$. In order to

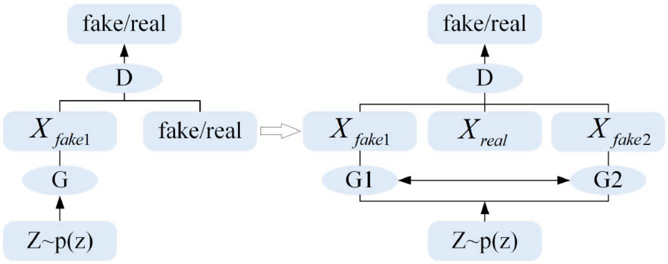

Fig. 5. Combined GANs.

identify which generator produces a given fake set, the discriminator must learn how to push different generators toward different recognizable patterns. However, the goal of each generator is still the same as in the traditional GANs. Therefore, compared with (1), the objective function of the combined GANs is calculated as

$$\min_{G}\max_{D} E_{x\sim p_{\text{data}}} D_{m+1}(x;\theta_d) + E_{x\sim p_z}\Big(1 - D_{m+1}\Big(G_i\Big(z;\theta_g^i\Big);\theta_d\Big)\Big) \qquad (7)$$

where θ_d is the parameter of discriminator, θ_g^i is the parameter of generator i, and $G_i(z;\theta_g^i)$ represents the generate function of generator i.

Compared with (5), when $x \sim p$ (where p can be a real data set or a generated data set) and the corresponding δ are given, aiming at the output of generator i, the loss function ℓ_D^i of discriminator is calculated in

$$\ell_D^i = D_{m+1}\Big(G_i\Big(z;\theta_g^i\Big);\theta_d\Big) - D_{m+1}(x;\theta_d). \qquad (8)$$

In (8), the discriminator aims to maximize the probability that the real data set x is discriminated as a real data set, and minimize the probability that the generated data set $G_i(z;\theta_g^i)$ is discriminated as a real data set. Then, aiming at the output of all generators, the loss function L_D of the discriminator is calculated as

$$\begin{aligned} L_D &= \frac{1}{m}\sum_{i=1}^{m}\ell_D^i \\ &= \frac{1}{m}\sum_{i=1}^{m}\Big(D_{m+1}\Big(G_i\Big(z;\theta_g^i\Big);\theta_d\Big) - D_{m+1}(x;\theta_d)\Big). \end{aligned} \qquad (9)$$

The gradient descent algorithm is used to find θ_d that minimizes the value of L_D, as calculated in

$$\begin{aligned} \nabla_{\theta_d} L_D &= \nabla_{\theta_d}\left[\frac{1}{m}\sum_{i=1}^{m}\ell_D^i\right] \\ &= \nabla_{\theta_d}\left[\frac{1}{m}\sum_{i=1}^{m}\Big(D_{m+1}\Big(G_i\Big(z;\theta_g^i\Big);\theta_d\Big)\Big)\right] \\ &\quad - \nabla_{\theta_d}\left[\frac{1}{m}\sum_{i=1}^{m} D_{m+1}(x;\theta_d)\right]. \end{aligned} \qquad (10)$$

Combined with (5), (6), and (8), the goal of the generator i is the opposite of the discriminator. Therefore, the loss function of the generator i is calculated in

$$\ell_G^i = D_{m+1}(x;\theta_d) - D_{m+1}\Big(G_i\Big(z;\theta_g^i\Big);\theta_d\Big). \qquad (11)$$

Algorithm 1 Training Algorithm of the WCGAN

```
Input: learning rate $\lambda = 0.0002$, parameter $\theta_d$ and $G_{\theta_g}$, the number of generators $m = 2$, the number of iterations $n_{disc} = 5$, historical behavior data sets of vehicles, random distribution $z \sim p(z)$.
Output: the $m$ generators $G_{\theta_g}$.
Initialization $\theta_d$ and $G_{\theta_g}$
while $G_{\theta_g}$ has not converged do
    Sample real behavior data sets of nodes $B = \{B_0, B_1, \cdots, B_{t-1}\}$ from blockchain, and set random distribution $z \sim p(z)$
    for $t = 1$ to $n_{disc}$ do
        for $i = 1$ to $m$ do
            $B_t^i \leftarrow G_t^i(B, z)$
            Calculate $\ell_D^i \leftarrow D_{m+1}(G_i(z;\theta_g^i);\theta_d) - D_{m+1}(x;\theta_d)$
        end for
        Update the parameters $\theta_d \leftarrow \theta_d + \lambda\nabla_{\theta_d}\frac{1}{m}\sum_{i=0}^{m}\ell_D^i$ of the discriminator
    end for
    for $i = 1$ to $m$ do
        $B_t^i \leftarrow G_t^i(B, z)$
        Calculate $\ell_G^i \leftarrow D_{m+1}(x;\theta_d) - D_{m+1}(G_i(z;\theta_g^i);\theta_d)$
    end for
    Update the parameters $\theta_g^i \leftarrow \theta_g^i + \lambda\nabla_{\theta_g^i}\ell_G^i$ of generator $i$
end while
Return to the $m$ generators $G_{\theta_g}$
```

The gradient descent algorithm is also used to find θ_g^i that minimizes the value of ℓ_G^i, which is calculated in

$$\nabla_{\theta_g^i}\ell_G^i = \nabla_{\theta_g^i}\Big[-D_{m+1}\Big(G_i\Big(z;\theta_g^i\Big);\theta_d\Big)\Big]. \qquad (12)$$

In this case, all generators can be updated in a parallel way. The generators form a hybrid mode caused by the objective function. When $p_d = (1/m)\sum_{i=1}^{m} p_{g_i}$, each generator represents a hybrid component to achieve global optimality.

3) WCGAN Procedure: In order to overcome the problems of gradient disappearance and mode collapse in the original GANs, we design a WCGAN training algorithm. Supposing there are m generators for cooperation training in the WCGAN. Algorithm 1 specifies the proposed WCGAN training algorithm. In Algorithm 1, we aim to obtain the parameters of m generators, $G_{\theta_g} = \{\theta_g^1, \theta_g^2, \ldots, \theta_g^i, \ldots, \theta_g^m\}$. The generators and discriminator are trained alternately. Additionally, generators are trained only after the discriminator has been trained n_{disc} times, to play the supervisory role of the discriminator.

VI. Numerical Results

In this section, we will present experimental results to illustrate the effectiveness of the WCGAN method and RPBAC model. In our experiments, the WGAN, D2PGGAN, and WCGAN methods are compared in respect of Wasserstein

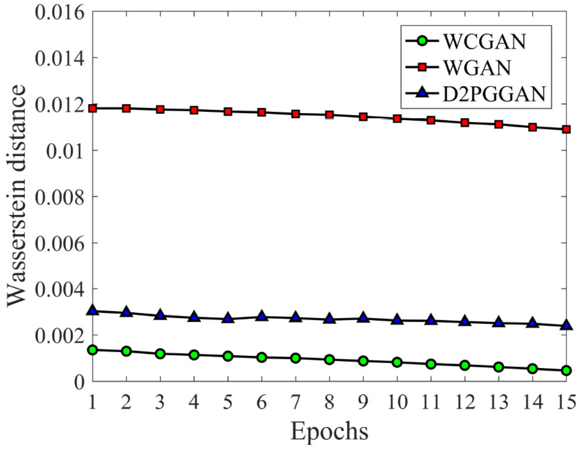

Fig. 6. Comparison of the Wasserstein distance.

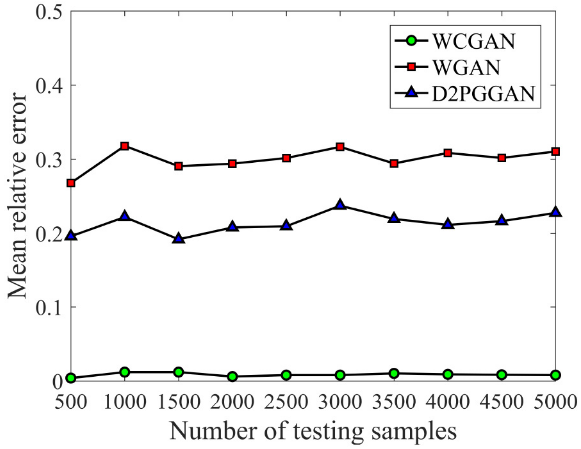

Fig. 8. Comparison of the mean relative error.

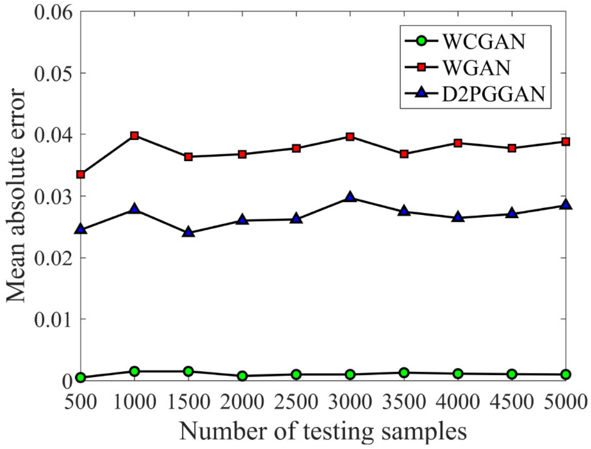

Fig. 7. Comparison of the mean absolute error.

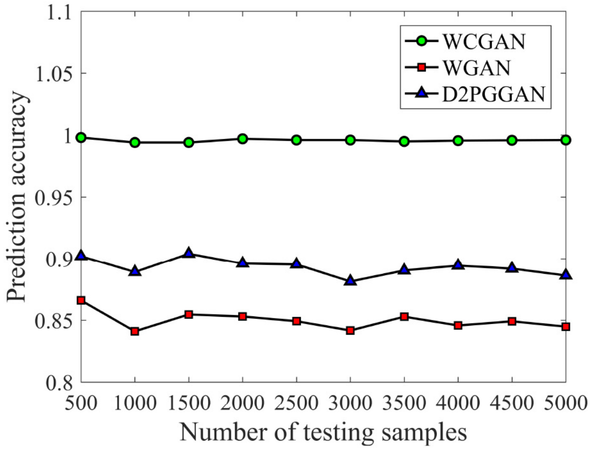

Fig. 9. Comparison of the prediction accuracy.

distance, mean absolute and relative error, and prediction accuracy. Furthermore, we will also discuss the utility of the RPBAC model in respect of accuracy and response time of access control.

A. Experimental Environment

The risk prediction model is built on Tensorflow 1.12.0 and coded through Python. The data sets for this experiment are from car-hacking data sets for intrusion detection [40]. This data sets were collected from real vehicles while performing denial of service attack, spoofing attack, fuzzy attack and attack-free. The learning rate is 0.0002.

B. Performance of the WCGAN Method

To exhibit the feasibility and effectiveness of WCGAN method, we convert different malicious behavior data into different risk levels, which is represented as a binary form with four digits. After preprocessing, we extract 10 000 records from the data sets for training, which includes 5000 attack and 5000 attack-free records. We compare the Wasserstein distance of WGAN, D2PGGAN and WCGAN methods under the extracted training sets. Then we extract 500, 1000, 1500, 2000, 2500, 3000, 3500, 4000, 4500, and 5000 records from the data sets for testing, respectively. Each testing set contains half of attack records and half of attack-free records. We compare the mean absolute and relative error, and the prediction accuracy among the three methods under the extracted testing sets.

Fig. 6 is the variation of Wasserstein distance with different iterations. As shown in Fig. 6, after 15 iterations of training, the Wasserstein distance of WGAN is about 0.0108, the D2PGGAN is about 0.0023, and the proposed WCGAN approaches 0. The results indicate that WCGAN has completed the probability distribution learning of training sets, and the data sets generated by WCGAN are more similar to the real data sets than the WGAN and D2PGGAN. This is probably because the three models leverage Wasserstein distance to calculate the loss function, alleviating the problem of gradient disappearance in the original GANs. Additionally, the WCGAN utilizes two generators, improving the learning ability of model.

Fig. 7 shows the mean absolute error of prediction changes with different number of testing sets among the three methods. As shown in Fig. 7, the WCGAN has the least mean absolute error giving the same testing set number. Similarly, Fig. 8 shows the mean relative error of prediction changes with different number of testing sets. In Fig. 8, the mean relative error of WCGAN is about 0.01, which is much smaller than the values of WGAN and D2PGGAN. The results indicate that the

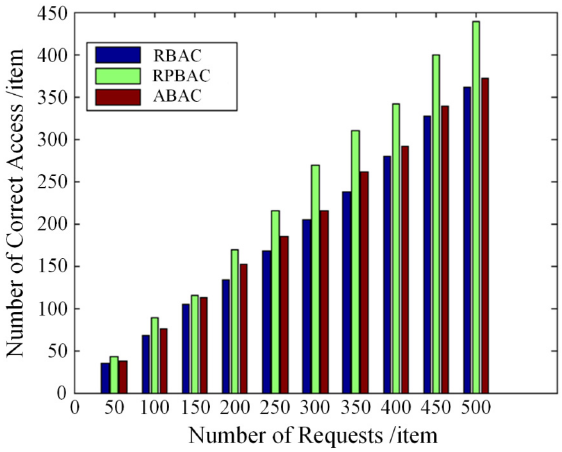

Fig. 10. Comparison of the access control accuracy.

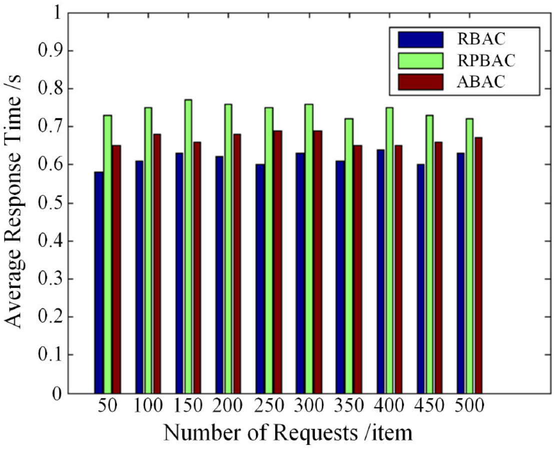

Fig. 11. Comparison of the average response time.

prediction error of WCGAN is extremely small or even negligible. This is due to the fact that the WCGAN leverages two generators to cover different probability distributions of data sets, reducing the problem of mode collapse.

The variation of prediction accuracy in different number of testing sets is displayed in Fig. 9. As shown here, the prediction accuracy of WCGAN is about 0.99, the WGAN is about 0.85, and the D2PGGAN is about 0.89. Compared with the other two models, the WCGAN has maintained a high prediction accuracy by utilizing two well-trained generators for prediction.

C. Performance of the RPBAC Model

The experimental data sets consist of different access requests. Each request contains four properties: the subject (the vehicle that initiated the access request), the object (the vehicle being requested), the form and occurrence time of access. The requesting vehicles in each request are randomly selected, and generate 10 rounds of requests, $R_1, R_2, \ldots, R_{10}$. The requests of each round are generated by 50 vehicles. Each vehicle launches i requests, and i $\in \{1, 2, \ldots, 10\}$. The occurrence time of each request is random. The requests alternately consist of malicious and normal requests. The normal requests mean that the vehicle has no malicious behavior. The malicious requests mean that the vehicle has malicious behavior. The RBAC model in [15], the ABAC model in [16], and the proposed RPBAC model are used to conduct the access authorities of 10 group access requests, respectively. The three models are compared in terms of the accuracy of access control and average response time to validate the utility of the RPBAC model.

Fig. 10 is the comparison of the accuracy of access control in different number of requests among the three models. As shown in this figure, the RPBAC model has the highest accuracy of access control giving the same request number. The RPBAC model dynamically decides the authorities of vehicles by evaluating the real-time risk level of vehicles, improving the feasibility of access control. Moreover, as the growing amounts and types of requests, the advantages of RPBAC model in access authorization become more obvious, better protecting the security of information resources than traditional access control mechanisms.

Fig. 11 shows the comparison of average response time in different number of requests among the three models. With the increasing number of access requests, the average response time of each model fluctuates partially. However, the overall trend is stable. The response time of the proposed model is longer than the ABAC and RBAC models slightly, because it spends some time in evaluating the risk level of nodes. For the RBAC model, once the role of a node is verified, the access authorities of this node will be fixed. The ABAC model needs some time to calculate whether a set of attributes meets a certain condition for the authorization judgment. In contrast, in each access request, the RPBAC model needs to calculate the risk level of a node, and adjusts the access authorities dynamically. However, only a tiny time increment is caused via this method, which is acceptable in the IoV.

VII. Conclusion

In this article, we leverage the intelligent edge chain to enable the access control for IoV devices, and propose an RPBAC model, to regulate the behaviors of vehicles. In addition, we introduce the GANs to build a risk-prediction module. We afterward analyze the problems of gradient disappearance and mode collapse in the original GANs, and devise a WCGAN method. Compared with the existing WGAN and D2PGGAN methods, experimental results demonstrate that the WCGAN method matches closer to the real data in respect of probability distribution, and has higher accuracy. The results further show that the RPBAC model displays higher accuracy of access control than the RBAC and ABAC models.

References

[1] S. Chen *et al.*, “Vehicle-to-Everything (V2X) services supported by LTE-based systems and 5G,” *IEEE Commun. Stand. Mag.*, vol. 1, no. 2, pp. 70–76, Jul. 2017.

[2] J. Hu *et al.*, “Link level performance comparison between LTE V2X and DSRC,” *J. Commun. Inf. Netw.*, vol. 2, no. 2, pp. 101–112, Jun. 2017.

[3] S. Chen, J. Hu, Y. Shi, and L. Zhao, “LTE-V: A TD-lte-based V2X solution for future vehicular network,” *IEEE Internet Things J.*, vol. 3, no. 6, pp. 997–1005, Dec. 2016.

[4] X. Cheng, R. Zhang, S. Chen, J. Li, L. Yang, and H. Zhang, "5G enabled vehicular communications and networking," *China Commun.*, vol. 15, no. 7, pp. 3–6, Jul. 2018.

[5] B. Yu and F. Bai, "PYRAMID: Probabilistic content reconciliation and prioritization for V2V communications," *IEEE Trans. Veh. Technol.*, vol. 67, no. 7, pp. 6615–6626, Jul. 2018.

[6] J. Wang, C. Jiang, Z. Han, Y. Ren, and L. Hanzo, "Internet of Vehicles: Sensing-aided transportation information collection and diffusion," *IEEE Trans. Veh. Technol.*, vol. 67, no. 5, pp. 3813–3825, May 2018.

[7] J. Voelcker. *We Now Have One Billion Vehicles on the Planet*. Accessed: Sep. 16, 2016. [Online]. Available: http://www.greencarreports.com/news/1065070_its-official-wenowhave-one-billion-vehicles-on-the-planet/

[8] L. Zhao *et al.*, "Vehicular communications: Standardization and open issues," *IEEE Commun. Stand. Mag.*, vol. 2, no. 4, pp. 74–80, Dec. 2018.

[9] S. Guleng, C. Wu, Z. Liu, and X. Chen, "Edge-based V2X communications with big data intelligence," *IEEE Access*, vol. 8, pp. 8603–8613, 2020.

[10] J. Pan, J. Wang, A. Hester, I. Alqerm, Y. Liu, and Y. Zhao, "EdgeChain: An edge-IoT framework and prototype based on blockchain and smart contracts," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4719–4732, Jun. 2019.

[11] C. Feng *et al.*, "Efficient and secure data sharing for 5G flying drones: A blockchain-enabled approach," *IEEE Netw.*, vol. 35, no. 1, pp. 130–137, Jan./Feb. 2021.

[12] Z. Zhou *et al.*, "Robust mobile crowd sensing: When deep learning meets edge computing," *IEEE Netw.*, vol. 32, no. 4, pp. 54–60, Aug. 2018.

[13] T. Jiang, H. Fang, and H. Wang, "Blockchain-based Internet of Vehicles: Distributed network architecture and performance analysis," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4640–4649, Jun. 2018.

[14] (2009). *Bitcoin: A Peer-to-Peer Electronic Cash System*. [Online]. Available: https://bitcoin.org/bitcoin.pdf/

[15] N. Solanki, Y. Huang, I. Yen, F. Bastani, and Y. Zhang, "Resource and role hierarchy based access control for resourceful systems," in *Proc. IEEE 42nd Annu. Comput. Softw. Appl. Conf. (COMPSAC)*, vol. 2, Jun. 2018, pp. 480–486.

[16] M. Gupta, F. Patwa, and R. Sandhu, "An attribute-based access control model for secure big data processing in hadoop ecosystem," in *Proc. 3rd ACM Workshop Attribute Based Access Control*, Mar. 2018, pp. 13–24.

[17] Y. Liu *et al.*, "An access control mechanism based on risk prediction for the IoV," in *Proc. IEEE 91st Veh. Technol. Conf.*, Jun. 2020, pp. 1–5.

[18] Q. Jin, X. Luo, Y. Shi, and K. Kita, "Image generation method based on improved condition GAN," in *Proc. IEEE 6th Int. Conf. Syst. Informat. (ICSAI)*, Feb. 2019, pp. 1290–1294.

[19] M. Arjovsky, S. Chintala, and L. Bottou, "Wasserstein GAN," 2017. [Online]. Available: arXiv:1701.07875.

[20] Z. Zhang, M. Li, and J. Yu, "D2PGGAN: Two discriminators used in progressive growing of GANs," in *Proc. IEEE Int. Conf. Acoust. Speech Signal Process. (ICASSP)*, Apr. 2019, pp. 3177–3181.

[21] D. Ulybyshev, A. O. Alsalem, B. Bhargava, S. Savvides, G. Mani, and L. B. Othmane, "Secure data communication in autonomous V2X systems," in *Proc. IEEE Int. Congr. Internet Things (ICIOT)*, Sep. 2018, pp. 156–163.

[22] D. Kim, H. Ju, B. Jung, and J. Na, "An access control method for vehicle management system," in *Proc. IEEE Int. Conf. Inf. Commun. Technol. Converg. (ICTC)*, Nov. 2018, pp. 949–952.

[23] D. Zhang, Y. Liu, L. Dai, A. K. Bashir, A. Nallanathan, and B. Shim, "Performance analysis of FD-NOMA-based decentralized V2X systems," *IEEE Trans. Commun.*, vol. 67, no. 7, pp. 5024–5036, Jul. 2019.

[24] M. Rumez, A. Duda, P. Gründer, R. Kriesten, and E. Sax, "Integration of attribute-based access control into automotive architectures," in *Proc. IEEE Intell. Veh. Symp. (IV)*, Jun. 2019, pp. 1916–1922.

[25] D. Hussein, E. Bertin, and V. Frey, "A community-driven access control approach in distributed IoT environments," *IEEE Commun. Mag.*, vol. 55, no. 3, pp. 146–153, Mar. 2017.

[26] X. Chen, H. Zhang, C. Wu, S. Mao, Y. Ji, and M. Bennis, "Performance optimization in mobile-edge computing via deep reinforcement learning," in *Proc. IEEE 88th Veh. Technol. Conf. (VTC-Fall)*, Apr. 2018, pp. 1–6.

[27] C. Wu, Z. Liu, D. Zhang, T. Yoshinaga, and Y. Ji, "Spatial intelligence toward trustworthy vehicular IoT," *IEEE Commun. Mag.*, vol. 56, no. 10, pp. 22–27, Oct. 2018.

[28] C. Wu, Z. Liu, F. Liu, T. Yoshinaga, Y. Ji, and J. Li, "Collaborative learning of communication routes in edge-enabled multi-access vehicular environment," *IEEE Trans. Cogn. Commun. Netw.*, vol. 6, no. 4, pp. 1155–1165, Dec. 2020.

[29] J. Feng, Z. Liu, C. Wu, and Y. Ji, "Mobile edge computing for the Internet of Vehicles: Offloading framework and job scheduling," *IEEE Veh. Technol. Mag.*, vol. 14, no. 1, pp. 28–36, Mar. 2019.

[30] G. Qiao, S. Leng, S. Maharjan, Y. Zhang, and N. Ansari, "Deep reinforcement learning for cooperative content caching in vehicular edge computing and networks," *IEEE Internet Things J.*, vol. 7, no. 1, pp. 247–257, Oct. 2019.

[31] Z. Zhou, B. Wang, Y. Guo, and Y. Zhang, "Blockchain and computational intelligence inspired incentive-compatible demand response in Internet of electric vehicles," *IEEE Trans. Emerg. Topics Comput. Intell.*, vol. 3, no. 3, pp. 205–216, May 2019.

[32] M. Singh and S. Kim, "Crypto trust point (CTP) for secure data sharing among intelligent vehicles," in *Proc. IEEE Int. Conf. Electron. Inf. Commun. (ICEIC)*, Apr. 2018, pp. 1–4.

[33] H. Liao, Y. Mu, Z. Zhou, M. Sun, Z. Wang, and C. Pan, "Blockchain and learning-based secure and intelligent task offloading for vehicular fog computing," *IEEE Trans. Intell. Transp. Syst.*, early access, Jul. 21, 2020, doi: 10.1109/TITS.2020.3007770.

[34] G. Zyskind *et al.*, "Decentralizing privacy: Using blockchain to protect personal data," in *Proc. IEEE Security Privacy Workshops*, Jul. 2015, pp. 180–184.

[35] H. A. Najada, I. Mahgoub, and I. Mohammed, "Highway cluster density and average speed prediction in vehicular ad hoc networks (VANETs)," in *Proc. IEEE Symp. Comput. Intell. (SSCI)*, Jan. 2018, pp. 96–103.

[36] X. Zheng, D. Zhang, H. Gao, Z. Zhao, H. Huang, and J. Wang, "A novel framework for road traffic risk assessment with HMM-based prediction model," *Sensors*, vol. 18, no. 12, p. 4313, Oct. 2018.

[37] M. Mohammadi, A. Al-Fuqaha, and J. Oh, "Path planning in support of smart mobility applications using generative adversarial networks," in *Proc. IEEE Int. Conf. Internet Things (iThings) IEEE Green Comput. Commun. (GreenCom) IEEE Cyber Phys. Soc. Comput. (CPSCom) IEEE Smart Data (SmartData)*, Jun. 2018, pp. 878–885.

[38] Y. Sun, L. Peng, H. Li, and M. Sun, "Exploration on spatiotemporal data repairing of parking lots based on recurrent GANs," in *Proc. IEEE 21st Int. Conf. Intell. Transp. Syst. (ITSC)*, Dec. 2018, pp. 467–472.

[39] M. Arjovsky and L. Bottou, "Towards principled methods for training generative adversarial networks," Jan. 2017. [Online]. Available: arXiv:1701.04862.

[40] E. Seo, H. M. Song, and H. K. Kim, "GIDS: GAN based intrusion detection system for in-vehicle network," in *Proc. 16th Annu. Conf. Privacy Security Trust (PST)*, 2018, pp. 1–6.

Yuanni Liu received the M.E. degree from Zhengzhou University, Zhengzhou, China, in 2008, and the Ph.D. degree from the Beijing University of Posts and Telecommunications, Beijing, China, in 2011.

She currently serves as an Associate Professor with the School of Communication and Information Engineering, Chongqing University of Posts and Telecommunications, Chongqing, China. Her research interests include mobile crowdsensing, the IoT security, IP routing technology, and complex networks.

Man Xiao received the B.S. degree from Anhui Jianzhu University, Hefei, China, in 2018. She is currently pursuing the M.S. degree with the Chongqing University of Posts and Telecommunications, Chongqing, China.

Her research interests include mobile crowd sensing, IoT security, IP routing technology, and complex networks.

Shanzhi Chen (Fellow, IEEE) received the bachelor's degree from Xidian University, Xi'an, China, in 1991, and the Ph.D. degree from the Beijing University of Posts and Telecommunications, Beijing, China, in 1997.

He joined the Datang Telecom Technology and Industry Group, Beijing, and the China Academy of Telecommunication Technology (CATT), Beijing, in 1994, and has been serving as the EVP of Research and Development since 2008. He is currently the Director of the State Key Laboratory of Wireless Mobile Communications, CATT, where he conducted research and standardization on 4G TD-LTE and 5G. He has contributed to the design, standardization, and development of 4G TD-LTE and 5G mobile communication systems. His current research interests include 5G mobile communications, network architectures, vehicular communication networks, and Internet of Things. He has authored and coauthored 4 books, 17 book chapters, more than 100 journal papers, 50 conference papers, and over 50 patents in the above areas.

Dr. Chen received multiple top awards and honors by China central government, especially the Grand Prize of the National Award for ScientfiĄc and Technological Progress, China, in 2016 (the Highest Prize in China). He is an Area Editor of the IEEE INTERNET OF THINGS JOURNAL and IEEE NETWORK. He served as a member and a TPC chair of many international conferences.

Fan Bai received the Ph.D. degree from Waseda University, Tokyo, Japan, in 2016.

His current position is Engineer with the Beijing Institute of Spacecraft System Engineering, Beijing, China. His main research interests include the deep space optical communications and satellite networking.

Jianli Pan (Member, IEEE) received the Ph.D. degree from the Department of Computer Science and Engineering, Washington University in St. Louis, St. Louis, MO, USA.

He is currently an Associate Professor with the Department of Computer Science, University of Missouri in St. Louis, St. Louis, MO, USA. His current research interests include Internet of Things, edge computing, machine learning, and cybersecurity.

Dr. Pan is an Associate Editor of *IEEE Communication Magazine* and IEEE ACCESS.

Di Zhang (Senior Member, IEEE) received the Ph.D. degree from Waseda University, Tokyo, Japan, in 2017.

He is currently an Assistant Professor with Zhengzhou University, Zhengzhou, China, and an Adjunct Researcher with Waseda University. From 2017 to 2018, he was a Visiting Senior Researcher with Seoul National University, Seoul, South Korea, and a visiting student with National Chung Hsing University, Taichung, Taiwan, in 2012. He has engaged in two international projects in wireless communications and networking co-funded by the EU FP-7, EU Horizon 2020, Japanese Monbushou, and NICT. His research interests include wireless communications, signal processing and Internet of Things.

Dr. Zhang received the ITU Young Author Award and the IEEE Outstanding Leadership Award, in 2019. He serving as an Editor of IEEE ACCESS, the *KSII Transactions on Internet and Information Systems*, and *IET Quantum Communication*. He has served as a Guest Editor for IEEE WIRELESS COMMUNICATIONS, IEEE NETWORK, IEEE ACCESS, the *IEICE Transactions on Internet and Information Systems*; the Chair of IEEE flagship conferences, such as WCNC, IEEE/CIC ICCC; and a TPC member of various IEEE flagship conferences, such as ICC, GlobalSIP, WCNC, VTC, CCNC, and HEALTHCOM.