Forest Chemicals Revew
www.forestchemicalsreview.com
ISSN: 1520-0191
May-June 2021 Page No. 11-21
Article History: Received: 24 February 2021, Revised: 05 April 2021, Accepted: 08 May 2021, Publication: 30 June 2021

Intelligent Transportation System Modeling Based on Blockchain and Cloud Storage in Forest City

Liu San-jun[1*], Zhang Yuan-yuan[1]
[1]Jiaozuo University, Jiaozuo City, Henan Province, China
*Corresponding Author.

Abstract:

Green traffic corridor is the traffic link of forest city. Blockchain is an innovative technology often used in finance, Internet of things and health care. It can reach a consensus in a decentralized network and store data permanently and irreversibly in a tamper proof way. This paper describes a reputation system of intelligent transportation system, and considers that users who are interested in traffic information are the main participants of the architecture. They can safely share the data proved by the experience of other user sets. Users can choose the travel plan between the two regions through the data verified by other users or automatically generated by the system. The saved data is absolutely reliable, based on the reputation of the provider, and does not support modification. We have demonstrated the impact of malicious attacks because the average speed decreases when error information is stored in the blockchain. But as an applied route algorithm, it can guide the car to avoid the congested road, so that it can drive safely and quickly.

Keywords: *Forest city, blockchain, cloud storage, intelligent transportation system, modeling and simulation.*

I. INTRODUCTION

With the accelerated development of global social economy, the development of social productivity continues to accelerate, and people's automobile consumption level also continues to improve. China's car ownership shows a rapid growth trend [1-2]. And at present, the number of car ownership and car drivers are still in a state of rapid growth. The rapid growth of car ownership has brought great convenience to people's production and life, but when people enjoy the portability brought by cars, there are increasingly serious road traffic congestion, accidents, serious environmental pollution and other social problems [3]. At the same time, it has a great

Forest Chemicals Revew
www.forestchemicalsreview.com
ISSN: 1520-0191
May-June 2021 Page No. 11-21
Article History: Received: 24 February 2021, Revised: 05 April 2021, Accepted: 08 May 2021, Publication: 30 June 2021

threat to people's personal and property safety and caused great losses to the national economy.

Internet of vehicles (IoV) is the embodiment of Internet of things (loT) in the field of intelligent transportation system, and it is the core of the field of intelligent transportation system. The Internet of vehicles is composed of multiple vehicle nodes [4-5]. It collects and processes the real-time operation data of vehicles through wireless data communication technology, which is used for data interaction between vehicles, between vehicles and roadside basic units, between vehicles and pedestrians, so as to make vehicles better integrated into the urban network.

Each vehicle in the vehicular ad-hoc network is regarded as a node, and the status of each network node is equal. Vehicles can realize self networking, and form a strong network in the process of driving. Each node can be either a sending node or a receiving node [6]. The sending node and the receiving node are relative, which can not only exchange and share information, but also early warn the emergency. However, the environment of the Internet of vehicles has some unique network characteristics, such as low network security and poor communication concealment. At the same time, the centralized mode of the Internet of vehicles leads to a sharp increase in the risk of data intrusion by hackers. In the process of communication, it is required to optimize the vehicle traffic system by sharing information, so it is necessary to ensure the data security of the Internet of vehicles. Data security is the basis of subsequent data analysis and application, so how to manage vehicle related data security is the key problem that must be solved in the Internet of vehicles system. At present, the research on the Internet of vehicles information security is not deep enough, so it still has the value of in-depth research.

II. BLOCKCHAIN TECHNOLOGY

The so-called blockchain technology, referred to as BT (blockchain Technology), is also known as the distributed ledger technology [7-8]. This technology mainly forms a reliable database record for collective maintenance through the two advantages of decentralization and distrust. Blockchain technology allows all nodes in the system to participate in the recording of the database, and all nodes record all the data of information exchange in a period of time in a data block. The hash value of the data block is generated by a consensus method called proof of work (POW), which is used to verify and chain the next data block, and all the participating nodes in the network jointly verify whether the record is true.

2.1 Java encryption technology

The Internet has the characteristics of openness, global sharing and huge amount of information [9]. Because of these characteristics of the Internet, there are great security risks in

Forest Chemicals Revew
www.forestchemicalsreview.com
ISSN: 1520-0191
May-June 2021 Page No. 11-21
Article History: Received: 24 February 2021, Revised: 05 April 2021, Accepted: 08 May 2021, Publication: 30 June 2021

the network transmission. In order to make the data safe and reliable transmission and ensure the data integrity, it is necessary to encrypt the data. Cryptography often used in computer can be roughly divided into four categories: symmetric cryptography, asymmetric cryptography, hash function and digital signature. In symmetric cryptosystem, encryption and decryption use the same key, which requires both sides to agree on the key before communication. In asymmetric cryptosystem, encryption and decryption use two different keys, a public key and a private key. Public key encrypts and private key decrypts [10]. If private key encrypts, public key decrypts. The communication model of asymmetric cryptosystem is shown in Figure 1.

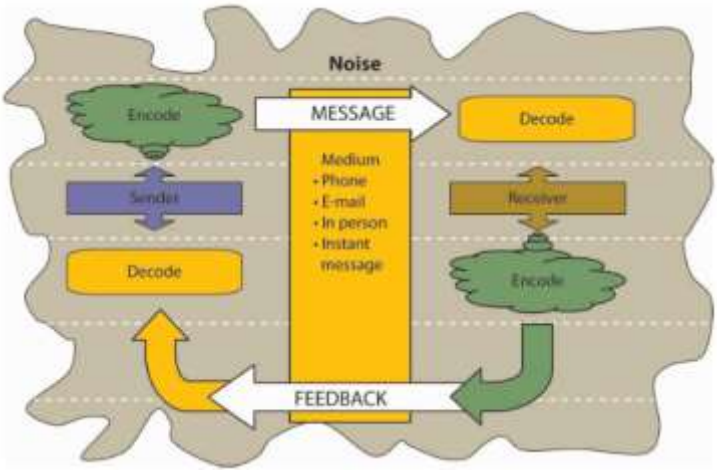

Fig 1: Communication model of asymmetric cryptosystem

2.2 Merkle Tree algorithm

Merkle Tree, also known as Hash tree, is a tree based on Hash data, which is an algorithm used to verify data consistency in blockchain technology. It was invented and proposed by Ralph Merkle in 1972 to ensure that data blocks received from peer-to-peer networks are not modified or destroyed, and that other peer-to-peer networks are not deceived to send fake data blocks. Merkle Tree refers to such a tree structure, the value of each leaf node in the tree is a hash value of data, and the value of each parent node is the hash value obtained by combining the hash values of all its child nodes and performing hash operation, and the process is continued until the root node of the tree is obtained. Merkle Tree's main advantage is that it can independently provide integrity authentication for all its child nodes by signing the parent node once.

When verifying data, you only need to compare MerkleTree of two data. First, compare whether V0 is the same. If it is the same, you can confirm that the two data are the same. If they

Forest Chemicals Revew
www.forestchemicalsreview.com
ISSN: 1520-0191
May-June 2021 Page No. 11-21
Article History: Received: 24 February 2021, Revised: 05 April 2021, Accepted: 08 May 2021, Publication: 30 June 2021

are not the same, retrieve their child nodes Nodel and Node2; if mine 1 is the same and V2 is different, retrieve their child nodes Node5 and Node6. By traversing and comparing from top to bottom, we can determine which nodes have inconsistent data. Merkle Tree is applied to the storage of information exchange data in blockchain technology, which makes use of the characteristics of Merkle Tree to ensure that every data can not be forged.

III. DESIGN OF DATA EXCHANGE SYSTEM FOR VEHICLE NETWORK

3.1 Overview of data exchange system

Based on the research of blockchain technology, this paper applies blockchain to the Internet of vehicles, and designs a data exchange system for the Internet of vehicles with the help of the idea of blockchain. The general structure of the data exchange system of the Internet of vehicles designed in this paper is shown in Figure 2. The system is composed of several alliance chains and one side chain.

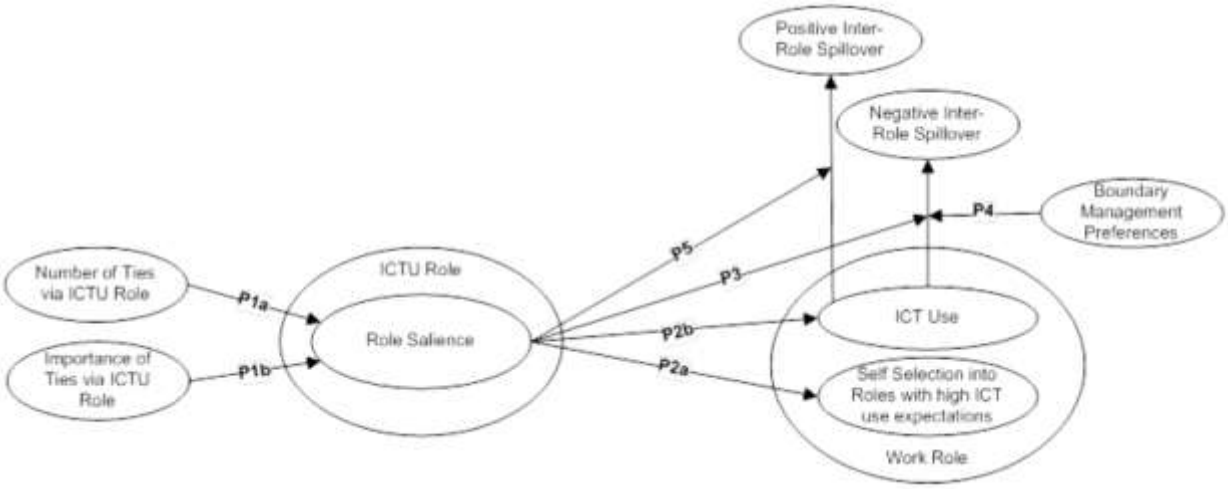

Fig 2: System structure diagram

First of all, the alliance chain of the Internet of vehicles in each city starts to work, and the data is continuously exchanged between nodes. The consensus nodes jointly record the data of message transmission between nodes, and record the data into the block through the consensus method of workload proof, so as to generate the block record of the alliance chain. When the alliance chain of the Internet of vehicles generates blocks, the side chain starts to work. At this time, each alliance chain of the Internet of vehicles selects a broadcast node from the boundary nodes by taking turns, and the broadcast node is responsible for broadcasting the data in each

Forest Chemicals Revew
www.forestchemicalsreview.com
ISSN: 1520-0191
May-June 2021 Page No. 11-21
Article History: Received: 24 February 2021, Revised: 05 April 2021, Accepted: 08 May 2021, Publication: 30 June 2021

alliance chain of the Internet of vehicles in the side chain. All broadcast nodes exchange alliance chain data and record it in the side chain block by workload proof, so as to form a unified record of National Alliance chain data of Internet of vehicles. Through the decentralized way, each node will have a copy of the data records of the Internet of vehicles, which can effectively ensure the authenticity and security of the data of the Internet of vehicles, and also provide more comprehensive and safe information services for drivers.

3.2 Design of alliance chain for Internet of vehicles

The network of vehicles alliance chain is a private blockchain composed of on board unit (OBU) and road side unit (RSU) in the city. OBU is a mobile node installed on the vehicle. Its main function is to realize information sharing between vehicles and communicate with RSU, and also obtain safety information sent by RSU, such as traffic line optimization, road condition information and collision avoidance. All central nodes participate in the consensus process of the alliance chain of the vehicle network, while OBU and boundary nodes only participate in data exchange, but ask the consensus process of data block. The flow chart of the alliance chain of the vehicle network is shown in Figure 3.

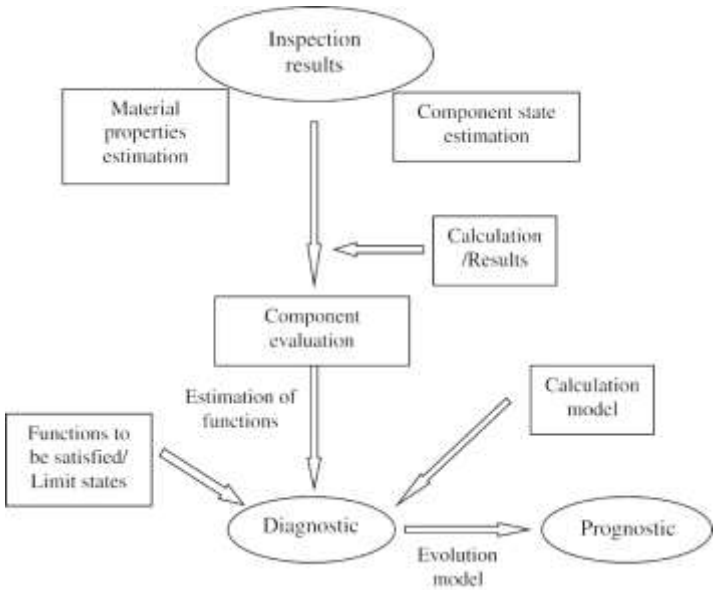

Fig 3: Flow chart of Internet of vehicles alliance chain

The design of the alliance chain of the Internet of vehicles mainly includes three parts: the establishment of node communication, the communication between nodes, and the generation of alliance chain block. The node communication part also includes vehicle to vehicle (V2V)

Forest Chemicals Revew
www.forestchemicalsreview.com
ISSN: 1520-0191
May-June 2021 Page No. 11-21
Article History: Received: 24 February 2021, Revised: 05 April 2021, Accepted: 08 May 2021, Publication: 30 June 2021

communication, road to road (R2R) communication, and vehicle to road (V2R) communication. Wave is a protocol for vehicle to vehicle and vehicle to road information interaction. The application layer of the protocol uses SAEJ2735 protocol as the security message set. In the process of communication, in order to ensure the integrity and verifiability of information and mutual trust between nodes, a digital signature is added after the information. The digital signature adopts the elliptic curve digital signature algorithm (ECDSA). When the node needs to send information, it uses its own private key to sign the information. The receiver uses the sender's public key to verify the signature. After the verification, it obtains the location, speed and other information.

Basic safety message (BSM) is exchanged between vehicles. BSM defines the information of vehicle itself: position, speed, direction, braking status, etc. The data exchange process between vehicles is as follows:

1. Sending information, the on-board sensors of the vehicle node monitor the state of the vehicle at all times, and transmit the monitored data parameters to the OBU. The OBU will receive various data parameters, which are defined according to the SAE j2735 protocol standard. The basic security message (BSM) is the information that must be sent for data exchange between vehicles. The OBU sends BSM periodically without interruption.

2. After the application layer defines the security message, it encrypts it with its own private key to generate the signature Sigprivx (m), where privx represents the private key of vehicle X and sends the information and signature to the network layer together. The corresponding security information is encapsulated by wsmp (wave short message protocol) protocol and TCP / IP protocol of network layer to get WSM (wave short message) packets, which are sent out in the form of multi triangle network multicast communication routing through LLC layer and physical layer.

3. the sent WSM information is monitored by the OBU of the surrounding vehicle on the control channel (CCH). When the OBU of the surrounding vehicle monitors the WSM information, the data package will be submitted to the corresponding application program of the application layer.

4. after receiving WSM data package by corresponding program of application layer, it unpacks WSM, obtains signature and information in accordance with SAEJ2735 standard format. OBU of surrounding vehicles uses public key of sending vehicle to decrypt signature, and obtains information about location and speed after verification, and displays it on the developed user interface. The data exchange process between OBU and OBU is shown in

Forest Chemicals Revew
www.forestchemicalsreview.com
ISSN: 1520-0191
May-June 2021 Page No. 11-21
Article History: Received: 24 February 2021, Revised: 05 April 2021, Accepted: 08 May 2021, Publication: 30 June 2021

Figure 4.

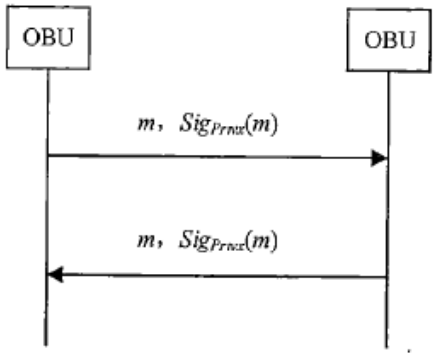

Fig 4: OBU and OBU data exchange process

IV. SYSTEM SIMULATION RESULTS AND ANALYSIS

4.1 Content and result analysis of alliance chain simulation

The process of establishing communication by adding nodes to the network of vehicles alliance chain. In this paper, the socket connection is used to establish the node communication in the simulation experiment. Socket is also called socket. The program provides the port to communicate with the external, that is, port communication. Through socket connection, data transmission channels can be provided for both parties. It has the advantages of low loss rate of data report, simple use and easy to transplant. First, the server side listens on the connection of the client. When a client requests a connection, the server verifies the legitimacy of its identity. If it is legal, establish a communication connection with it.

Firstly, the user enters the user name and the JP address of the server in the login interface through the Android client, where the user name represents the identity of the vehicle node and the roadside unit node. In this experiment, eight vehicle nodes, namely obul.obu8, are set as legal nodes, and three roadside unit nodes, namely RSU 1.rsu3, are set as legal nodes. Then click the connect button to enter the alliance chain of the Internet of vehicles. The user sends the node's identity information to the server through the Android client, and then the server verifies the node's identity information. If the authentication fails, the connection request will be rejected, and 0 will be returned to represent the illegal node. Enter "CL" in the user name, and the Android client will prompt "the authentication failed, unable to enter the network!". If the verification is passed, establish a communication connection with the client and return 1. After

Forest Chemicals Revew
www.forestchemicalsreview.com
ISSN: 1520-0191
May-June 2021 Page No. 11-21
Article History: Received: 24 February 2021, Revised: 05 April 2021, Accepted: 08 May 2021, Publication: 30 June 2021

the communication connection is established, the Android client enters the vehicle status interface.

In the process of data exchange between the nodes of the Internet of vehicles, the hash hash of the information to be sent needs to be signed when it is instantiated. When processing the transmission information, the receiver should first verify the signature to verify its reliability. The key code of digital signature is shown in Figure 5. Digitalsign is a method for digital signature. Its general process is to take out the private key object, instantiate the signature method, initialize the signature private key and update the data to be signed, and obtain the signature data by calling the sign method. SignatureVerify is a method used to verify the signature. Its process is similar to the signature process. First, take out the public key object, initialize the verification public key and update the data to be verified, then call the verify method to verify the signature, and return the verification result of boolean type.

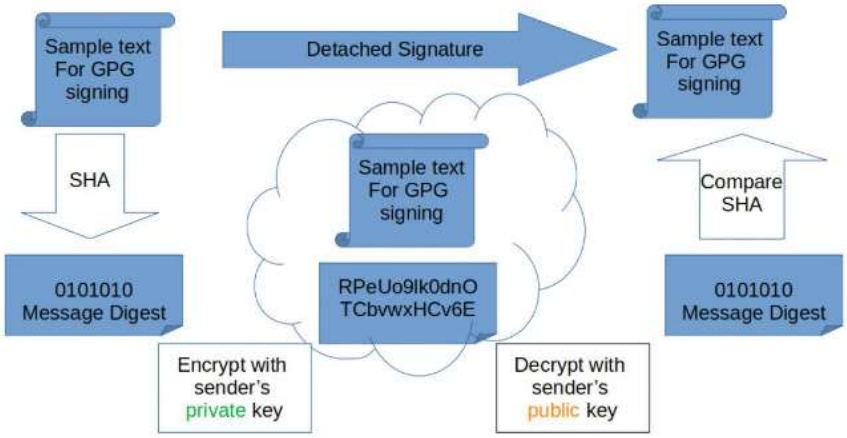

Fig 5: Key code of digital signature

4.2 System security analysis

In this paper, the data exchange system of Internet of vehicles based on blockchain is designed. Its security mainly comes from the asymmetry of ECDSA and POW consensus method. The so-called asymmetry means that it is easy to operate from one direction, but difficult to operate from the other. The digital signature algorithm ECDSA is used to ensure the verifiability of information and make the communication between nodes safe and reliable; Workload proof POW consensus method is used for consensus among nodes, so as to achieve the goal of decentralization and form a safe and reliable data record. This paper analyzes the performance of ECDSA and pow:

Forest Chemicals Revew
www.forestchemicalsreview.com
ISSN: 1520-0191
May-June 2021 Page No. 11-21
Article History: Received: 24 February 2021, Revised: 05 April 2021, Accepted: 08 May 2021, Publication: 30 June 2021

The asymmetry of workload proof POW consensus method is that it is very easy to verify whether the block header file meets the workload proof POW condition, and it only needs to verify bash hash once. However, it is very difficult to complete a workload proof. The workload proof function used in this paper is sha256, that is to say, there are two outputs for a POW operation. For the current computer's computing power, it is impossible to solve this problem, so it is impossible for a single node to destroy.

In practical application, throughput and delay of system information exchange are two important performance indexes of information exchange. The data exchange system of the Internet of vehicles designed in this paper adopts the alliance chain rather than the public chain, and it does not need to maintain a high degree of decentralization, but chooses the way of multi centralization. And it can specify the number of nodes and the physical configuration of node devices to make high-speed connection between nodes. The data in the whole network can be replicated, shared and synchronized among all nodes, which can greatly improve the information exchange performance of the system. Combined with the above analysis, this paper finally compares the performance of the system in the traditional centralized and decentralized situation. As shown in Table 1, because there is no centralized data management center in the decentralized mode, everything runs automatically through preset programs, which can not only reduce costs, but also improve efficiency. Of course, decentralization also has some disadvantages in some aspects. For example, in terms of time complexity and redundancy, decentralization is a complex cluster system, so the warm-up time to wake it up will be relatively long. At the same time, the distributed system has redundancy, which is not the optimal structure. However, decentralization solves an important defect of traditional centralization. In terms of security, decentralized system is not controlled by a single node, and its security is very high compared with the traditional centralization mode. Therefore, the data exchange system of Internet of vehicles based on blockchain has practical application value.

TABLE I. System performance comparison between traditional centralization and decentralization

	COST	**EFFICIENCY**	**TIME COMPLEXITY**	**REDUNDANCY**	**SECURITY**
CENTRALIZATION	high	low	low	low	low
DECENTRALIZATION	low	high	high	high	higher

Forest Chemicals Revew
www.forestchemicalsreview.com
ISSN: 1520-0191
May-June 2021 Page No. 11-21
Article History: Received: 24 February 2021, Revised: 05 April 2021, Accepted: 08 May 2021, Publication: 30 June 2021

V. CONCLUSION

As a typical application of Internet of things technology in the field of transportation, the Internet of vehicles is a network that can realize the functions of intelligent vehicle service, intelligent traffic control and dynamic information service. Through the communication between vehicles, vehicles and roadside units, vehicles and pedestrians, the state perception of the surrounding environment can be improved. In recent years, the Internet of vehicles has gradually become a research hotspot in road traffic safety, emergency vehicle warning and other aspects. However, due to the particularity of wave network, there are many security threats, such as tampering, forgery and replay attacks of communication information. At the same time, the centralized mode of the Internet of vehicles will increase the risk of hacker intrusion in the data center. Therefore, the information security of the Internet of vehicles is the premise and key of the deployment of the Internet of vehicles. Aiming at the security problems of Internet of vehicles, this paper designs a data exchange system of Internet of vehicles based on blockchain technology. Through the in-depth study of blockchain technology, it is applied to the Internet of vehicles, and its application value and prospect in the Internet of vehicles are analyzed.

ACKNOWLEDGEMENTS

This work was supported in part by the Key R&D and Promotion Project of Henan Province (Science and Technology Research) No.202102310204..

REFERENCES

[1] Guo Yebin, Xu Xin. Research on Encrypted Cloud Storage Platform Model Based on Blockchain. Software Guide, 2020, V. 19; No.207(01):227-230.
[2] Zhang Ying, Lian Yunyan, Li Yanxiang. Intelligent Transportation System Based on Blockchain. Information Weekly, 2020, 000 (010): P.1-1
[3] Xu Lei. Research and Implementation of Cloud Forensics System Based on Blockchain. Southwest University of Science and Technology
[4] Li Xuewei. Research and Implementation of Blockchain Technology in Secure Cloud Storage. University of Information Engineering, Strategic Support Force, 2020 (10):123-127
[5] Du Lan, Chen Linlin, Dai Lili. System Architecture Model of Cloud Manufacturing Platform Based on Blockchain. Information Technology and Network Security, 2019, 38 (01): 101-105
[6] Pang Ling. Research on Cloud Storage Model Based on Intelligent Transportation System. Chinese and Foreign Entrepreneurs, 2015, 000 (032): 129
[7] Guo Lizi, Hua Chi, Ji Shengquan. Research on Vehicle Remote Intelligent Temporary Fall System for Cloud Internet of Things. Tv Technology, 2015

Forest Chemicals Revew
www.forestchemicalsreview.com
ISSN: 1520-0191
May-June 2021 Page No. 11-21
Article History: Received: 24 February 2021, Revised: 05 April 2021, Accepted: 08 May 2021, Publication: 30 June 2021

[8] Li Duo. Design and Implementation of Vehicle Cloud Service System Based on Hadoop [d]. Guangdong University of Technology, 2016

[9] Fang Wenjie. Research on the Application of Cloud Computing Technology in Intelligent Transportation. Science and Technology Innovation, 2020 (09): 67-68

[10] Wang Ke, Ye Zhigeng. Research on Dynamic Path Guidance Algorithm Based on Cloud Computing. Computer Fan, 2018, 000 (031): 159-160+175