Design and implementation of autonomous collaboration service between IoT using distributed platform

1st Chang -Su Lee
Dept. of Electronics & Information Engineering
Korea Univ.
Sejong, Korea
cslee@korea.ac.kr

2nd U-Seok Ji
Dept. IoT Service Development
R&D center
Riwha Networks, co, ltd
Cheongju, Korea
jus2236@riwha.co.kr

3rd Mi-Hyang Jeon
Dept. IoT Service Development
R&D center
Riwha Networks, co, ltd
Cheongju, Korea
mhjeon10@riwha.co.kr

Abstract—**In order for various IoTs to share information and collaborate on the internet, a common use environment and a lot of data transmission are inevitable. In this study, a distributed platform was designed, and an application service was implemented in which IoTs equipped with decentralized identifiers socialized with each other and collaborated using social networking. Distributed platforms can reduce network usage costs by reducing network traffic, and decentralization can increase the efficiency of shared information protection between IoTs.**

***Keywords*— Autonomous collaboration service, Distributed platform, IoT, Decentralized identifiers, WebID**

I. Introduction

As various IoTs have emerged, a common use environment that IoTs can easily connect, and share has become necessary. In addition, there is a demand for a collaboration service in which IoT recognizes and cooperates with each other to provide necessary information to each other. As a method for this, there have been studies on IoTs socializing and collaborating, but research and service implementation on how to register IoTs, how IoTs find others and autonomously establish and disconnect social networks, and how to minimize network traffic never had one yet. In this study, we designed and implemented a collaboration service in which IoT have unique decentralized identifiers [1] and distributed platforms and socialize with other IoTs to share information. Distributed platform is a platform where IoTs recognize each other with decentralized identifiers and share information through social networking. IoT have WebID as a decentralized identifier. WebID was explained in detail in Session II. IoT find collaborators on a decentralized platform and verify each other's identity with WebID. And socialize, share information, and provide services.

Pedestrian safety service was implemented as an IoT collaboration service. Pedestrian safety service is a service in which vehicles and pedestrians socialize with the V2P server and share location information so that the V2P server sends an alarm to the vehicle when there is a pedestrian on the crosswalk. The network connection configuration of the pedestrian safety service is shown in Fig. 1.

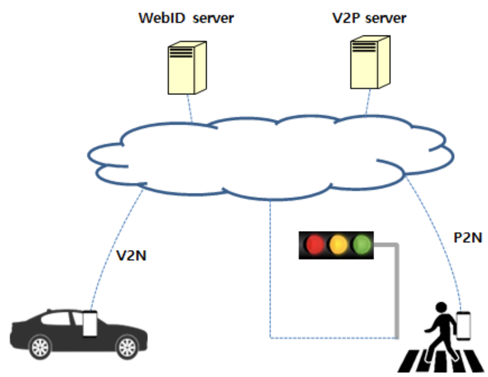


Fig. 1. Pedestrian safety service connection configuration

Existing pedestrian safety services include floor traffic lights, crosswalk intensive lighting, child protection zone speed limit notifications, nighttime safety logo lights, and pedestrian guidance lights. However, these existing services mainly function to warn pedestrians. To prevent accidents, not only pedestrians but also vehicle drivers need services that require safe driving at crosswalks.

In Session II, WebID was explained as a background of related technologies, and in Session III, the distributed platform of things was explained. In Session IV, implementation services were explained in detail, and in Session V, conclusions and future research directions were presented.

II. Background

A. WebID

A WebID is an HTTP URI referring to an Agent (person, organization, group, device, etc.). WebID provides a globally unique decentralized identifier by using a URI.[2] A WebID profile is a document that contains information describing the owner of a WebID in RDF data format. The data in this document is defined through an ontology that describes each relationship. The relationship between WebID URI and WebID profile document is shown in Fig. 2. The WebID URI is created by appending the hostname of the WebID Server to the HTTPS protocol and attaching the location of the profile document. The reason why HTTPS protocol is used is that WebID authentication and security are performed using TLS. The location of the profile document in the WebID URI can be specified using a hash tag. The WebID protocol integrates authentication and trust into the concept of WebID. The idea behind the WebID protocol is to link an SSL client certificate to a WebID profile, allowing WebID owners to authenticate to other websites that support the WebID protocol. Authentication and security of WebID uses TLS, so this protocol is called WebID-TLS protocol.[3]

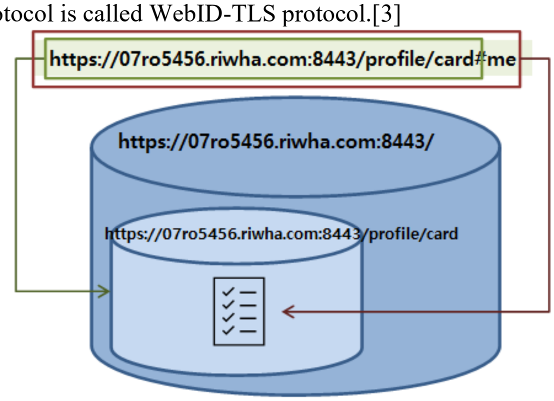


Fig. 2. Relationship between WebID and WebID profile

B. *WebID Server (Solid server)*

Solid Server is a server program provided by Solid and has functions of creating and managing WebID. Solid is a name created by taking the first letter of each word in Social Linked Data. It provides a set of rules and tools that are proposed to build decentralized social applications based on linked data principles.[4] Solid Server was used as the WebID server that creates and manages WebID and profile in the information sharing service between IoTs implemented in this paper.

III. Approach

A. *Distributed platform*

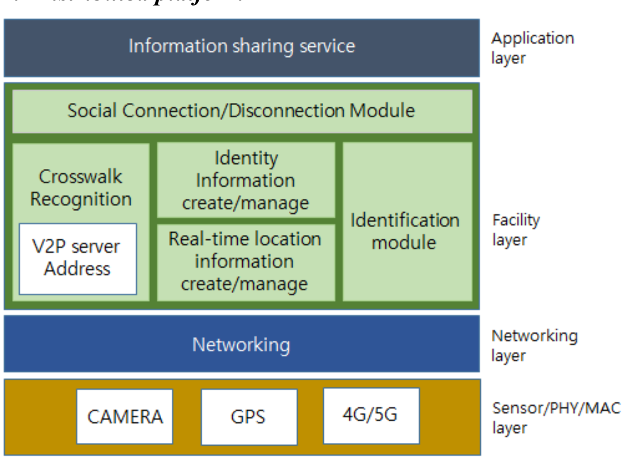


Fig. 3. Pedestrian app platform

Fig. 3 is the platform for the pedestrian app.

- **Crosswalk Recognition Module** - The pedestrian platform contains the address of the V2P server where the location information of the crosswalk is recorded. The platform calculates the distance between the pedestrian and the crosswalk and recognizes the nearest crosswalk.
- **Identity information creation and management module** - Pedestrian platform has a WebID and profile. For example, a pedestrian whose phone number is 01035373708 may have a WebID such as https://010 35373708.riwha.com:8443/profile /card#me.
- **Creation and management of real-time location information** - This is a module that checks one's location information in real time from the GPS sensor of a smart phone.
- **Identity verification Module** - This module verifies the profile with the received WebID.
- **Social connection and disconnection module** - This module connection or disconnection social after confirming the profile of other IoT through the identification module.

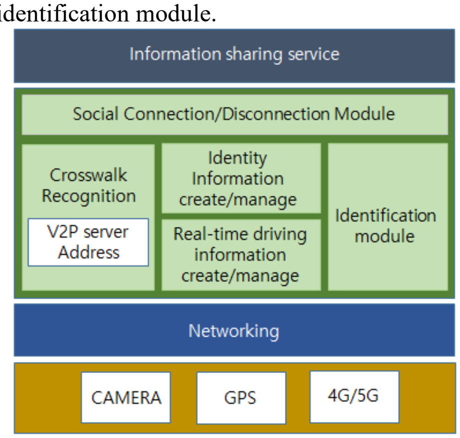


Fig. 4. Vehicle app platform

The vehicle app's platform is shown in Fig. 4.

- **Identity information creation and management module** - Vehicle platform has a WebID and profile. For example, if your plate number is 07ro5456, https://07ro5456.riwha.com:8443/ profile/card#me.
- **Real-time driving information creation and management module** - A module that checks vehicle's location information, driving speed, and distance to crosswalk.

The V2P server platform is shown in Fig. 5.

- **Identity information creation and management module** – V2P server has WebID and profile. For example, in the case of the second crosswalk on Osongsaengmyeong 2-ro, Chungcheongbuk-do, it can have a WebID such as https://CBOsongSM2ro-02.riwha.com:8443/profile/card#me.

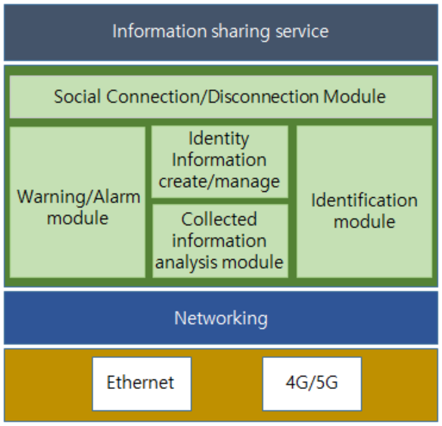


Fig. 5. V2P server platform

- **Collected information analysis module** - This module analyses and manages the collected information of pedestrians and vehicles. The V2P server provides a real-time service that notifies pedestrians and vehicles of warnings, a data searching service that checks past records, and an analysis service that analyses collected information to identify pedestrians and vehicles that are likely to cause accidents. The V2P server collects pedestrian location information and analyses the pedestrian's crosswalk entry time and congestion time. And by collecting the driving information of the vehicle, it analyses the change in deceleration in front of the crosswalk.

Fig. 6 shows the real-time service screen of the V2P server and the screen for selecting the date and time for data inquiry service.

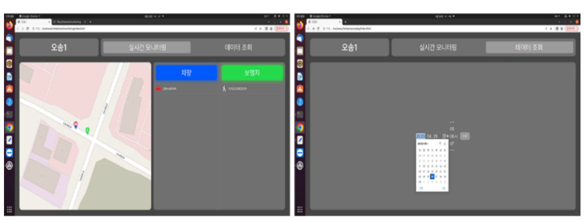


Fig. 6. Service screen of V2P server

B. *Service flow*

The flow of location information sharing service between pedestrian and vehicle is shown in Fig. 7.

① WebID - When a pedestrian approaches a crosswalk within 5M, the WebID is transmitted to the V2P server registered on the pedestrian platform.

② Get the profile - The V2P server collects the pedestrian's profile using the identified WebID.

③ Social connection - V2P servers socialize with pedestrian terminals with IP and port information identified in the profile.

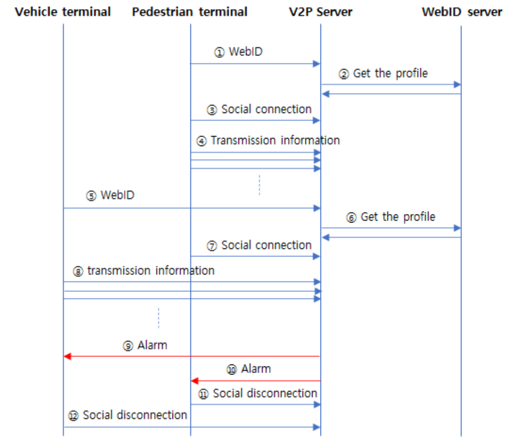


Fig. 7. Service flow

④ Pedestrian terminals transmit location information to the V2P server every second. Transmission latency is within 100ms. These messages are shown in Table 1.

Table 1. Pedestrian location information message format

Name		Type	Range	Note
ID		Var[n]	N=1~11 byte	Pedestrian ID
Date/Time		DATETIME		Current date and time
location	Latitude	INT		Current location (GPS)
	Longitude	INT		
	elevation	INT		

⑤ WebID - When the vehicle approaches the crosswalk within 500M, the WebID is sent to the V2P server of the crosswalk registered on the platform.

⑥ Get the profile - The V2P server collects vehicle profiles using WebID.

⑦ Social connection - V2P servers socialize with vehicle terminals with IP and port information identified in the profile.

⑧ Transmission information - The vehicle terminal transmits driving information to the V2P server. Transmission delay time is within 100ms. The driving information message is shown in Table 2.

Table 2. Driving information message format

Name		Type	Range	Note
ID		Var[n]	N=1~10byte	Vehicle ID
Date/Time		DATETIME		Current date and time
location	Latitude	INT		Current location (GPS)
	Longitude	INT		
	Elevation	INT		
Distance		INT		Distance to V2P server
Speed		INT		Vehicle speed (km/h)

⑨ Alarm - When a pedestrian is on the crosswalk, the V2P server sends a warning message and alarm to the vehicle terminal. Transmission delay time is within 100ms.

⑩ Alarm - If the speed of a vehicle approaching the crosswalk is very high, the V2P server sends a warning message and alarm information to the pedestrian. Transmission delay time is within 100ms.

⑪ Social disconnection - When leaving the crosswalk, the pedestrian terminal terminates social with the V2P server.

⑫ Social disconnection - When passing a crosswalk, the vehicle terminal terminates social with V2P.

IV. IMPLEMENTATION

A. *Vehicle / Pedestrian App Login*

To create WebID, a decentralized identifier, Solid server provided by Inrupt as an open source was used. As shown in Fig. 8, when the app log-in and the profile is verified on the server, the app checks the V2P server address close to its location via GPS.

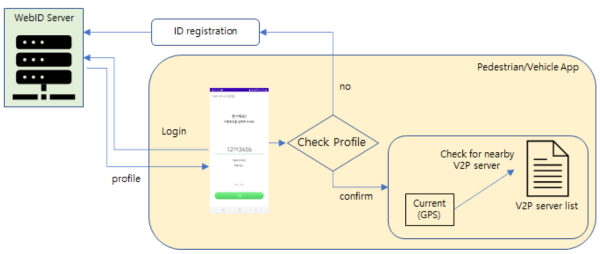


Fig. 8. Pedestrian/Vehicle App configuration

B. *Social connection and information sharing with V2P server*

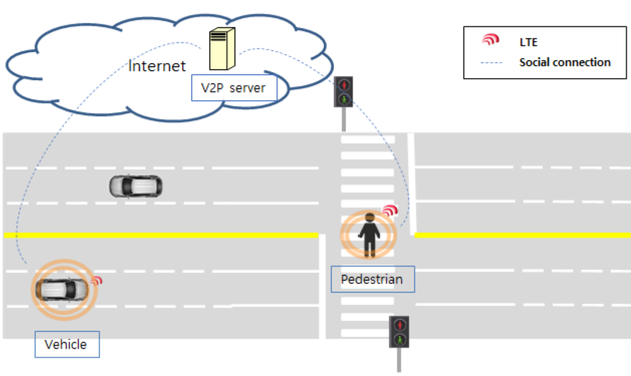


Fig. 9. Social connection

When pedestrians and vehicles approach the crosswalk, they socialize with the V2P server and share location information and driving information as shown in Fig. 9. And when a pedestrian is on the crosswalk, the V2P server sends an alarm and warning signal to the vehicle. Also, if a vehicle is approaching a crosswalk at high speed, the V2P server sends a warning signal to the pedestrian terminal as well. Fig. 10 is a vehicle app screen that received a warning signal from the V2P server.

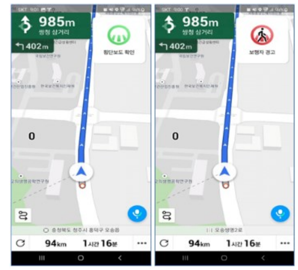


Fig. 10. Crosswalk check and warning message screen in the vehicle app

C. *Accuracy and Latency*

The Pedestrian Safety Service tested transmission delay speed and accuracy in Seongnam-si, Gyeonggi-do and Cheongju-si, Chungcheongbuk-do. Smartphones with pedestrian and vehicle apps installed are Samsung Galaxy Note20 Ultra (Qualcomm Snapdragon 865+, RAM 12GB, Android 13), A9 (Qualcomm Snapdragon 710, RAM 6GB, Android 10) and J7 (Samsung Exynos 7, RAM 3GB, Android 7.0) and LG Q7 (Qualcomm Snapdragon 450, RAM 3GB, Android 10) models were used, and each used LG U plus and SK telecom's LTE data communication. HP Z240 Tower Workstation (CPU: Intel Xeon(R) CPU E3-1225 v5 @ 3.30GHz X 4, RAM: 8GB, OS: Ubuntu 20.04.5 LTS) was used as the V2P server, and HP ProLiant DL320e was used as the WebID server. gen8 (CPU: Intel Xeon(R) CPU E3-1240 V2 @ 3.4GHz X 8, RAM: 32GB, OS: Ubuntu 20.04.3 LTS) was used. And as vehicles, we used Hyundai cars and Peugeot 308.

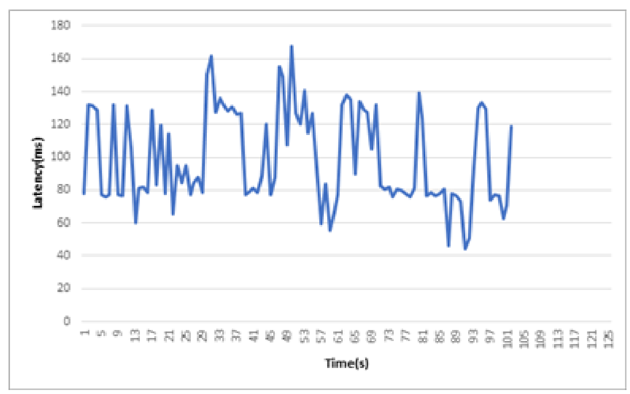


Fig. 11. Latency between vehicle terminal and V2P server

When the vehicle terminal and the pedestrian terminal socialize with the V2P server to provide pedestrian safety services, the latency was measured by checking the transmission time of the warning message sent by the V2P server to the vehicle terminal and the reception time received from the vehicle terminal. And the accuracy was measured by the reception rate of each terminal and server. Fig. 11 shows the latency measurement result, and the average latency is 99.04ms. All messages sent from pedestrian terminals and vehicle terminals were accurately received from the server, and alarm messages sent from the server were accurately received from each terminal. Fig. 12 shows the latency with each V2P server when 13 crosswalks are sequentially met while driving and pedestrian safety services are provided. The overall average latency is 98.9ms.

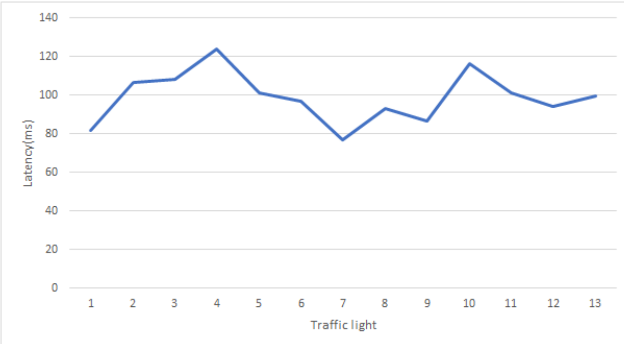


Fig. 12. Pedestrian safety service latency with 13 V2P servers while driving

It was confirmed that the latency in the pedestrian safety service satisfies the "3rd generation partnership project TS 22.185 (2022) technical specification group service and system aspect, service requirements for V2X service" required by 3GPP [5].

V. Conclusions

The performance confirmed in the pedestrian safety service can be expected to expand the collaboration service using social networks of IoT to V2I and V2V in the future. In addition, if applied not only to information sharing but also to intelligent services using the shared information, it will be possible to implement various connected car services for autonomous driving. And if you create unique identity information for things with decentralization-oriented decentralized identifiers and use a decentralized platform, you will be able to share information more easily and safely for things to socialize and collaborate.

Acknowledgment

This study was supported by the Korea Technology and Information Promotion Agency for SMEs (TIPA) project "Establishment of quality-based traffic control system and intelligent prediction system (S3179866)".

References

[1] Won-ho Kim, “ICT Expert Interview” TTA Journal vol. 203, pp. 6-11, SEP/OCT 2022, ISSN 1975-5112

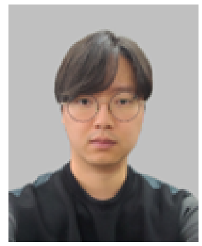
[2] Tim Berners-Lee, Andrei Sambra, Henry Story, https://dvcs.w3.org/hg/WebID /raw-file/tip/spec/identity-respec.html

[3] Toby Inkster, Henry Story, Bruno Harbulot, https://www.w3.org/2005 /Incubator/webid/spec/tls/

[4] Tim Berners-Lee, Christian Smith, Sarven Capadisli, Dmitri Zagidulin, Nicola Greco, Ruben Verborgh, https://github.com/solid/solid

[5] 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Service requirements for V2X services; Stage1(Release 17) 3GPP TS 22.185 v17.0.0(2022-03)

Chang-Su Lee is a Ph.D. graduate student in Department of Electronics and Information Engineering at Korea University, Korea. His Major is ICT Convergence Technology. He received the bachelor's degree in information & Engineering from Korea University in 1995 and received master's degree from same University in 1999. From 1995 to 1997, he worked in the field of video conference system at LG Information & Communication Co., Ltd. From 1999 to 2015, he worked in the field of CCTV and video security system at POSDATA Co., Ltd and RIFA Co., Ltd. His research interest includes, Deep Learning, IoT, autonomous collaboration system, and future networking technology.



U-Seok Ji is a chief researcher in RIWHA networks co. Korea. He received bachelor’s degree in information & engineering from Korea University in 2020. From 2020 to present, he has been working in Riwha networks co. Major interest is Web software research and development, especially multimedia streaming, and processing. Recently research interest is Deep Learning in the Browser.

Mi-Hyang Jeon is a CEO in RIWHA networks co. in RIWHA networks. She received the bachelor's degree in German language and literature. From 1993 to 1995, he worked in the field of Graphic Design at E-um communication co. From 1998 to 2000, he worked in the field of Graphic Design at T.R.I co. She has been working at Riwha networks since 2013. Her main interest is web design research and development.