Privacy-Aware Inter-Regional Data Sharing of Local User Information in OpenRoaming

Yasuo Okabe
Academic Center for Computing and Media Studies
Kyoto University
Kyoto, Japan
okabe@i.kyoto-u.ac.jp

Hideaki Goto
Cyberscience Center
Tohoku University
Sendai, Japan
hgot@cc.tohoku.ac.jp

Eisaku Sakane
National Institute of Infomatics
Tokyo, Japan
sakane@nii.ac.jp

Takenori Hirose
Local 24 Inc.
Kyoto, Japan
hirose@local24.jp

***Abstract*—In the international framework of OpenRoaming, a secure and open public Wi-Fi roaming network, we develop a system that ensures user information is shared in a pseudonymous manner to the Wi-Fi access network provider at the visiting location, with the user's consent, facilitating interregional data integration. We design mechanisms to collect user data that can be disclosed with their consent, and create systems to share user information across regions with privacy considerations, enabling mutual data integration across multiple regions. This interregional data sharing, conducted under privacy protection constraints, aims to address regional challenges, such as promoting tourism.**

Keywords—Wi-Fi roaming, privacy policy, pseudonymity, user consent, identity provider, access network provider

I. Introduction

OpenRoaming [1, 2], an international framework for open public wireless LAN roaming, offers exceptional convenience by enabling users to seamlessly connect to Wi-Fi access networks at their destinations using their existing accounts. This framework prioritizes security and privacy, ensuring strict protection of user pseudonyms [3]. However, public wireless LAN service providers utilizing OpenRoaming face a significant challenge: the inability to access information about roaming users. This limitation restricts their capacity to leverage such data for purposes such as promoting tourism and other related activities.

In this research, four organizations in Japan, Kyoto University Academic Computing and Media Center, Local24 Inc., Tohoku University Cyber Science Center, and the National Institute of Informatics, are collaborating to develop a mechanism that allows Wi-Fi account providers to disclose limited user information to Wi-Fi access network providers of the destination with the user's consent, enabling mutual data sharing between regions. Specifically, we will design and implement a mechanism for the IdP (Identity Provider) that issues accounts in OpenRoaming to collect data that can be disclosed with the user's consent, and a mechanism for sharing user information with the roaming Wi-Fi access network provider (ANP), while ensuring pseudonymity and taking privacy into consideration.

Using the proposed system, we plan to conduct a demonstration experiment of mutual data sharing in multiple regions to examine the appropriate extent of information disclosure required of users and what regional issues it will lead to solving. The demonstration experiment will be carried out in a real environment across multiple regions, including commercial facilities in Sapporo and accommodation facilities in Kyoto, to verify whether data sharing under the constraints of privacy protection will lead to the solution of regional issues such as tourism promotion.

The rest of this paper is organized as follows. In Section II the current social situation and background is described. Section III presents the issues to be resolved, and Section IV proposes ways to address these issues. Section V describes the configuration of the proposed system, and Section VI provides an overview of the planned demonstration experiment. Section VII is a summary.

II. Social Situation and Background

Nowadays, as a complement to mobile data communication services such as LTE/5G, public wireless LAN services (Wi-Fi services) using IEEE802.11 wireless LAN technology are being deployed mainly in so-called hotspot areas where there is a lot of communication traffic and performance degradation of mobile data communication occurs. The convenience of visiting users is being sought by "mobile data offloading" which distributes the load by redirecting data communication. Previously, many of these Wi-Fi services required a cumbersome authentication procedure via a Web browser called captive portal [4], which is intrinsically unsafe in terms of security. To solve this problem, the Wi-Fi Alliance, an industry association of wireless LAN product vendors, and the Wireless Broadband Alliance (WBA), an industry association of public wireless LAN service-related operators including major mobile carriers around the world, jointly promoted and standardized the Passpoint standard as Next Generation Hotspot (NGH). With Passpoint, when a device receives a beacon frame from an access point (AP) notifying it that it is a Passpoint-compatible Wi-Fi service, regardless of the SSID, the device checks the NAI (Network Access Identifier), roaming partner, and authentication type based on ANQP (Access Network Query Protocol), and authentication is automatically and securely established using 802.1X authentication.

As an international Wi-Fi roaming framework based on the Passpoint specification, the OpenRoaming Federation was launched in 2020 under the initiative of the WBA. From Japan, NGH Special Interest Group led by Goto at Tohoku University participated in OpenRoaming as Cityroam since the trial stage in 2017 and 2018, and Local24, as a telecommunications carrier responsible for operating Wi-Fi services and building infrastructure for Wi-Fi services, has been providing OpenRoaming at commercial facilities, accommodation facilities, stations, parks, etc. throughout the country that it has built and provided. In April 2023, the Tokyo Metropolitan Government launched the OpenRoaming service as "TOKYO FREE Wi-Fi", taking over the Nishi-Shinjuku Smart Pole pilot experiment for FY2021 and FY2022, and more than 600 access points were

Some of these research result were obtained from the commissioned research JPJ012368C04401 and 23610 by National Institute of Information and Communications Technology (NICT), JAPAN. .

979-8-3315-0694-0/25/$31.00 ©2025 IEEE

established within the FY2023 fiscal year. KDDI and Wi2 have begun providing OpenRoaming to local governments as a business, and the "au Smart Wi-Fi" app now has a function for issuing OpenRoaming accounts, leading to the expansion of OpenRoaming among local governments in Hakodate and Kyoto. The efforts to popularize and raise awareness of OpenRoaming have borne fruit, and the safety and convenience of OpenRoaming as a new generation public wireless LAN has become widely recognized in society, and it is believed that the system is moving into a period of widespread adoption.

On the other hand, there are challenges in maintaining and expanding public wireless LAN infrastructure, not limited to OpenRoaming. In Japan, public wireless LAN has been developed by mobile carriers as a data offload destination when mobile phone lines became congested during the LTE era in the 2010s. However, due to the COVID-19 pandemic, the number of tourists (especially foreign tourists visiting Japan) had decreased, and at the request of the government, mobile phone companies have begun to offer plans with lower communication capacity in exchange for lowering monthly communication fees. In order to recover the investment in installing 5G base stations, it is said that they are taking a strategy of reducing the access points of free Wi-Fi services and making users feel a lack of communication capacity in order to induce contract users to higher rate plans with higher communication capacity. In fact, it is said that the number of free public wireless LAN access points has decreased from 2020 to 2021. In this situation, in 2023, NTT Docomo has raised concerns about the line congestion of 4G base stations in urban areas, and offloading to public wireless LAN has once again attracted attention, but this has not led to a major change in mobile carriers' policies.

Furthermore, following the Noto Peninsula earthquake in January 2024, which severely disrupted mobile phone networks, the importance of providing public Wi-Fi at evacuation shelters has become clear. As a result, there is growing interest in OpenRoaming, which offers a safe and easy way for people to connect to Wi-Fi. The provision of Wi-Fi services by OpenRoaming at municipal facilities such as community centers and gymnasiums that function as evacuation shelters in the event of a disaster, as well as at elementary, junior high, and high schools, is expected to be important as a public infrastructure in Japan from the perspective of disaster prevention. However, since it costs a lot of money to comprehensively deploy Wi-Fi services in such facilities that are ubiquitous throughout the country and maintain them in the medium to long term, it cannot be said that it is worth the cost investment, even if it is considered as a set with the provision of convenience to citizens and tourists in peacetime. When promoting the development of public Wi-Fi as an offload destination, including for emergency use, it is important to consider not only the safety and ease of OpenRoaming, but also the need to ensure sufficient line quality. There are many Wi-Fi service access points that are not a problem when the number of connected terminals is small, but when the number of terminals increases, they become unable to connect properly due to overflow of the router's NAT table, etc. Even now, situations like this can be found in hotels, municipal facilities, and other places where public wireless LAN was installed relatively early on. Future Wi-Fi services will require high quality standards as a telecommunications business, such as ample line quality and monitoring systems in anticipation of emergencies such as disasters, data protection in wired sections upstream from access points, and systems for preserving logs and responding to incidents, but the question of who should bear the costs and in what form is becoming more apparent than ever before.

The business model for public Wi-Fi services as a complement to celluer networks has long been under consideration for some time [5, 6, 7]. Oughton et al. argued that 5G and Wi-Fi 6 are more complementary, than competitors, and that Wi-Fi will remain the dominant indoor technology for wireless internet connectivity [8]. Spruytte et al. explored public Wi-Fi roll-out negotiations using game theory, showing that balancing interests through compensation schemes leads to optimal freemium models over conflicting premium or entirely free approaches [9]. Huang et al. analyzed the development, competition, and stakeholder dynamics of municipal Wi-Fi projects worldwide, using economic models and real option analysis to evaluate their lifecycle and strategic transition points [10]. The analysis shows that public Wi-Fi projects, like Taipei's, generally offer positive value, justifying sustained investment and municipal involvement despite budget fluctuations, with proper management and evaluation critical for long-term success. However, none of these discussed how a business model can be established in Wi-Fi roaming, where the IdP (Identity Provider) that issues accounts and the ANP (Access Network Provider) that provides access points are separate.

III. Issues to Be Resolved

In response to the issue of who bears the cost of developing and maintaining public wireless LAN infrastructure described in the previous section, this proposal assumes that the maintenance manager of the facility where the access point is installed bears the cost. In OpenRoaming, the function of the IdP, which issues the accounts necessary for users to use Wi-Fi services and operates the authentication server, and the function of the ANP, which installs Wi-Fi access points and provides network access to users via upstream lines, are independent of each other, eliminating the human cost and personal burden of managing user information, such as user registration and forgotten passwords. The human costs and privacy risks associated with managing user information, such as user registration and forgotten passwords, are separated from the ANP function. Hence, if Wi-Fi network access is provided, it can be operated at a reasonable cost, mainly by installing relatively inexpensive Wi-Fi access points and maintaining normal Internet access lines.

On the other hand, the separation of IdPs and ANPs, and the fact that roaming is the primary use, means that Wi-Fi network access providers can obtain little information about roaming users. To address security incidents, authentication is pseudonymous rather than completely anonymous. While the IdP retains information that can identify users in the event of an incident, this information is not shared with the ANP during regular use. When the IdP and ANP are managed by the same operator, the IdP issues an account that allows free use of Wi-Fi services, and in exchange, with the user's consent, obtains user information such as place of residence, gender, and age group as personal information, which is used in various ways to solve local issues, such as marketing in the private sector and grasping the trends of disaster victims in local governments. However, in the case of roaming, there is currently no mechanism for data exchange between the IdP and ANP for such use.

One reason for this is that the mechanism for ensuring pseudonymity built into the OpenRoaming specification technically limits information sharing. During authentication in roaming, user authentication is conducted through an encrypted tunnel between the user's device and the IdP's authentication server. As a result, the ANP can only identify the user's associated IdP and receive a pseudonymous ID, known as CUI (Chargeable User Identity) 11], which typically has a short validity period of about one day. This means that while the ANP can observe usage trends at a broad level based on the IdP (usually on a national level), it cannot determine a user's length of stay or visit history. Previously, ANPs could track a user's movement within an area by examining their MAC address [12], but with increasing focus on privacy protection, MAC address randomization has become standard in operating systems like those on smartphones. Consequently, ANPs offering free roaming services must now develop new mechanisms for data collaboration with IdPs that can secure user consent.

Another reason is the absence of clear guidelines on how much user information the IdP should collect and disclose to the ANP while maintaining privacy protection. Key issues include determining how much information users are willing to consent to share when creating an account, what level of incentives, such as points, should be offered as compensation for their consent, and what degree of detail is necessary in user data to effectively use Wi-Fi usage history to address local challenges. Additionally, there is concern about whether tracking a user's movement history over multiple days, even if pseudonymized, could risk identifying individuals and result in unintended privacy breaches. Previous guidelines have often prioritized privacy protection and restricted data sharing or, conversely, taken the stance that data can be freely used once user consent is obtained. However, there has been insufficient consideration of the balance between data utilization and privacy protection in the context of Wi-Fi roaming services.

Unfortunately, this current situation is impeding the spread of Wi-Fi services in the region, particularly open and secure services such as OpenRoaming. While the importance of OpenRoaming may be conveyed during the installation or upgrade of Wi-Fi services in local commercial facilities, the benefits for users are generally well understood. However, the appeal of the benefits for access point installers remains weak, posing a challenge to business models where installers bear the costs. Presently, one way to circumvent this issue is for entities to act as both the IdP and the ANP. However, this could result in an overabundance of IdPs and encourage users to register with multiple providers, which is counterproductive. Such a scenario would undermine OpenRoaming's greatest advantage: enabling users to register with a single IdP and access roaming services worldwide.

IV. Proposal for the Issues

To address the aforementioned issues, this study proposes a mechanism that facilitates mutual data sharing between regions by loosely connecting the IdP, which manages user registration and provides OpenRoaming accounts, with the ANP, which offers Wi-Fi network access, assuming they are located in different regions. This mechanism would enable the IdP to obtain user consent in advance and disclose limited user information to the ANP during roaming.

Specifically, we design and implement a system where the IdP that issues OpenRoaming accounts can collect data that can be shared with the user's consent, and a mechanism to disclose and share this user information in a limited manner with the provider of the Wi-Fi network used for roaming, all while ensuring privacy, including pseudonymity. This mechanism is an application of our previous research [13].

Additionally, we will explore, through the development of specific business use cases, how much personal information IdPs should request users to disclose, what kind of explanations should be provided to users, under what conditions it would be suitable to share this information with the ANP, what local challenges could be addressed by combining pseudonymized user data with Wi-Fi access usage history, and what risks of privacy violations might arise from inadequate handling.

Figure 1 illustrates an example of data sharing of roaming user information between Wi-Fi service providers in different regions, as enabled by this research proposal. A user who registers an account through an app provided by the Wi-Fi service provider in the originating region, acting as an IdP, reviews the terms of service, including the privacy policy, and consents to sharing their user information with the Wi-Fi service provider in the destination region. When the user travels to another region, they are automatically connected to an OpenRoaming-compatible Wi-Fi service in that area. If the destination service provider has a data-sharing arrangement with the provider in the originating region, user information is securely shared while maintaining pseudonymity. This allows the user information to be utilized in the destination region, such as for analyzing tourist behavior and demographics. As an incentive, a coupon redeemable at the destination is sent to the user via the app from the originating region.

V. Proposed Sysetm Configuration

A. Overview

In this study, we design and implement a mechanism to collect user data that can be disclosed with their consent, enabling IdPs and ANPs to share user data across regions while ensuring pseudonymity and respecting privacy within the OpenRoaming framework. In OpenRoaming, user authentication is conducted through an encrypted tunnel between the user's device and the IdP's authentication server, ensuring pseudonymity by preventing the ANP from directly accessing user IDs and other sensitive information. To allow the ANP to recognize that the same user is using the service, OpenRoaming transmits a random value (hash value) that is valid for a relatively short period (typically one day).

This study designs and implements a protocol that allows for the sharing of a long-term pseudonymous ID from the IdP to the ANP through a secure communication channel, assuming cross-regional linkage between the IdP and ANP. In addition to the pseudonymous ID, we also consider linking data such as the user's residence, gender, and age group, with their consent.

While the IdP in OpenRoaming can identify which ANP-controlled access point is being used, it cannot directly identify the specific access point. This research includes designing and implementing a protocol that enables users to

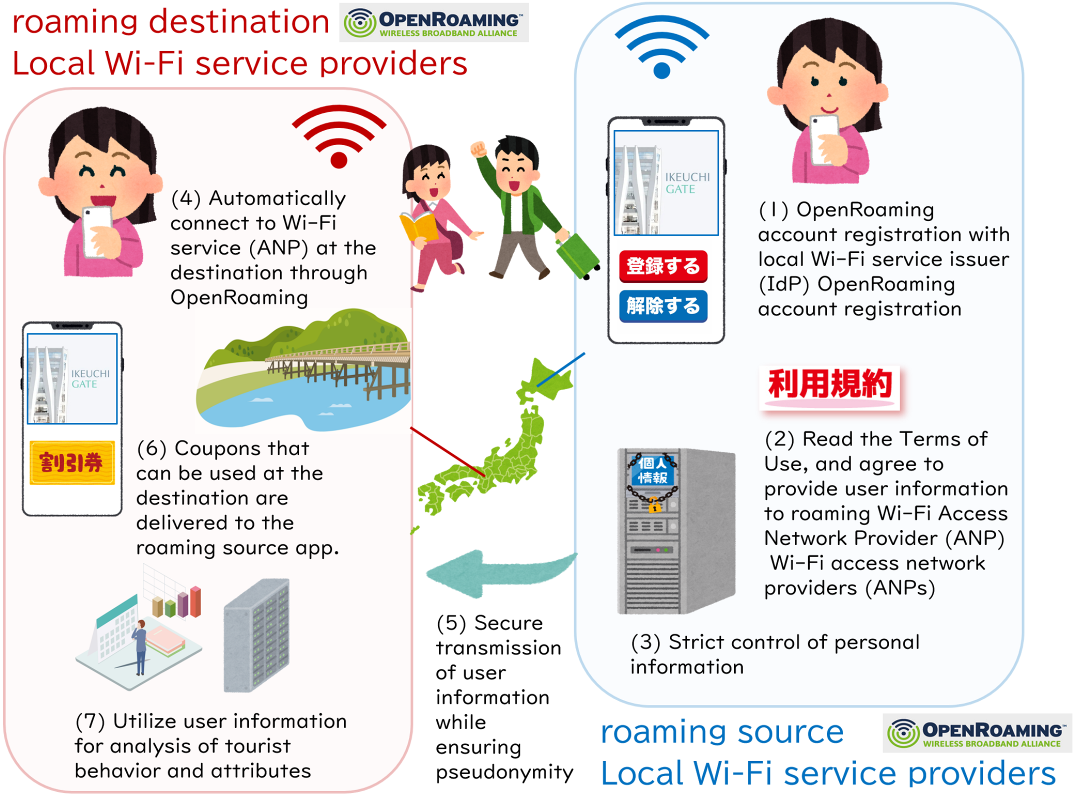
roaming destination
OpenRoaming WIRELESS BROADBAND ALLIANCE
Local Wi-Fi service providers
(4) Automatically connect to Wi-Fi service (ANP) at the destination through OpenRoaming
IKEUCHI GATE
割引券
(6) Coupons that can be used at the destination are delivered to the roaming source app.
(7) Utilize user information for analysis of tourist behavior and attributes
(5) Secure transmission of user information while ensuring pseudonymity
IKEUCHI GATE
登録する
解除する
(1) OpenRoaming account registration with local Wi-Fi service issuer (IdP) OpenRoaming account registration
利用規約
(2) Read the Terms of Use, and agree to provide user information to roaming Wi-Fi Access Network Provider (ANP) Wi-Fi access network providers (ANPs)
個人情報
(3) Strict control of personal information
roaming source
OpenRoaming WIRELESS BROADBAND ALLIANCE
Local Wi-Fi service providers

Fig. 1. Inter-regional data sharing of roaming user information with user consent

receive location-based services at their destination when using OpenRoaming, contingent on their explicit consent.

Additionally, when users register or manage their accounts with an IdP via an app or web application on devices like smartphones, a user interface that transparently presents not only the benefits but also the potential risks and obtains explicit user consent is necessary. To incentivize data sharing, we are also considering incorporating a data distribution feature within the app or application to provide information about areas or facilities using Wi-Fi services, encouraging users to share their data.

B. Secure sharing of user information from IdP to ANP via RADIUS

In OpenRoaming, user authentication is performed through an encrypted tunnel between the user’s device and the IdP’s authentication server, and pseudonymity is ensured by preventing the ANP from directly viewing user IDs, etc. A CUI (Chargeable User Identity) attribute is sent from the IdP to the ANP as a means for the ANP to determine that the same user is using the service, but in RADIUS the CUI is not protected by encryption or other methods, and OpenRoaming specifies that a random value (hash value) that lasts for a relatively short period of time should be sent as the CUI.

In this research, we design and implement a protocol that safely share information about users from IdP to ANP by encrypting and embedding it in attributes exchanged via RADIUS, on the premise that IdPs and ANPs cooperate between regions and share a common key in advance. On the premise that users have given explicit consent by registering an account with the IdP, the information to be shared is expected to include the user's pseudonymous ID, which will remain valid as long as the account is valid, as well as data such as prefecture or municipal level residence, gender, and age group.

On the other hand, in authentication federation by RADIUS, the IdP can know which access point under which ANP the user is using, but cannot directly know which access point the user is using specifically. This is important from the viewpoint of protecting the location privacy of the user, but currently, even with the user’s consent, location information cannot be securely sent from the ANP to the IdP. RFC5580 (Carrying Location Objects in RADIUS and Diameter) [14] specifies a method of adding Location-Data to RADIUS Accounting-Request, etc., but since this is exchanged without protection such as encryption, there is a risk of eavesdropping or tampering by a man-in-the-middle. In this research, we design and implement a protocol that enables location information to be shared securely between the IdP and the ANP via RADIUS using common key encryption, assuming the explicit consent of the user.

C. Designing a user interface for obtaining prior consent from users while respecting their privacy

The use of the user information sharing mechanism developed in Section V-*B* is premised on the prior consent of the user. In this study, we design and develop a user interface that openly present incentives as well as potential risks to users when they register or manage their accounts with an IdP via an app or web application on a device such as a smartphone, and then obtain explicit consent. The design enable users to easily check the ANPs to which they have consented to data sharing at that time, as well as the details of disclosure at each ANP, and to easily revoke consent.

In addition, as an incentive to disclose information, the same app or application incorporates a data distribution function such as discount coupons that can be used in areas or facilities where Wi-Fi services are used, encouraging users to share their data.

Furthermore, we develop a system that issues pseudonymous OpenRoaming accounts through web authentication integration as a service of the Academic Authentication Federation (GakuNin) operated by the National Institute of Informatics for users affiliated with academic institutions, and incorporate a user interface for obtaining prior consent and an information distribution function for incentives, making it possible to use it in demonstration experiments and in preparation for commercialization.

D. Business use cases through data integration of roaming user information

We consider multiple use cases to see how the inter-regional data sharing of roaming user information envisioned in this research and development can help solve regional issues in peacetime and in emergencies.

An example of using location information for marketing is a chain store app that uses GPS to obtain location information and allows users to “check in” to nearby stores to earn points. In a similar way, there is a need for a service that gives users some kind of points or delivers discount coupons when they visit a facility and use the Wi-Fi service on OpenRoaming. However, in OpenRoaming, which connects without the user's explicit operation and where the data link between the IdP and ANP remains a loose pseudonym, it requires ingenuity to implement such a service. As a premise, it is assumed that the app of the IdP (typically near the user's residential area) for which the user registered an OpenRoaming account is installed on the user's smartphone, but the app of the area or facility to be visited is not installed. Such a linkage of local apps is one use case. In addition, we will consider what kind of information consent to be obtained from users when realizing such a service.

On the other hand, the inter-regional data sharing of roaming user information is carried out with the prior consent of the user, but from the perspective of the user who is asked to consent, it is not easy to technically understand the linking of user information between IdP and ANP using pseudonyms. Even experts often overlook the potential risks how disclosure of information to ANPs could lead to privacy violations. Therefore, in the case of roaming use of Wi-Fi services in which IdPs and ANPs are separated and linked using pseudonyms, we will formulate guidelines on how much user information the IdP side should collect and disclose to the ANP while taking privacy protection into consideration, and a privacy policy based on those guidelines. Furthermore, we create easy-to-understand explanatory content corresponding to the formulated use cases so that general users can agree to disclosure within the scope of the guidelines without being overly cautious but can also understand that disclosure beyond that scope entails risks and think carefully about it.

VI. Plan for Demonstration Experiment

Based on this study, a demonstration experiment will be conducted to share user information across multiple regions, with user feedback collected through surveys to determine the appropriate level of information disclosure and assess how data sharing can address regional issues in both normal and emergency situations. This demonstration will take place in a real-world setting across multiple regions, including commercial facilities in Sapporo and accommodation facilities in Kyoto, involving general users to verify whether data sharing under privacy constraints can help resolve regional issues such as tourism promotion.

First, various use cases will be considered to identify how the inter-regional sharing of roaming user information can address regional challenges in both peacetime and emergency scenarios. Business use cases that can be implemented as services within OpenRoaming will be developed, featuring loose pseudonymous data linkage between the IdP and ANP. It is assumed that the user has installed the IdP's app (typically associated with their residential area) on their smartphone, but not the app of the region or facility they are visiting. Inter-regional linkage of regional apps is one such use case. Additionally, the type of user consent required to enable such services will be considered.

For OpenRoaming, which operates under pseudonymous linkage, guidelines will be formulated regarding how much user information the IdP should collect and disclose to the ANP while considering privacy protection, along with a privacy policy based on these guidelines. Furthermore, clear explanatory content corresponding to these use cases will be created to ensure that general users can agree to data disclosure within the guideline limits without undue concern, while understanding that disclosures beyond those limits carry risks and should be approached thoughtfully.

The foundational public wireless LAN infrastructure for the demonstration experiment is already operated by Local24 as an OpenRoaming-compatible Wi-Fi service. In addition to Local24’s account issuance service primarily offered in Kyoto, Maruyo Ikeuchi provides account issuance as a feature of its IKEUCHI GATE app in Sapporo, which will be enhanced with this additional functionality. Furthermore, a system will be developed to issue pseudonymous OpenRoaming accounts through web authentication collaboration as part of the Academic Authentication Federation (GakuNin), operated by the National Institute of Informatics, for users affiliated with academic institutions, promoting broad participation in the demonstration.

This demonstration experiment, involving real users in an authentic environment, will be achieved through the collaboration of the National Institute of Informatics, Tohoku University, and Kyoto University—organizations that have long operated the international academic wireless LAN roaming framework, eduroam, in Japan—and Local24, one of the pioneering private Wi-Fi service providers to support both eduroam and OpenRoaming.

VII. Concluding Remarks

In this study, we have detailed a mechanism within the OpenRoaming framework—an international system for secure and open public wireless LAN roaming—that enables the IdP issuing accounts to collect data, with the user's consent, and share it with the Wi-Fi access network provider (ANP) while ensuring pseudonymity and respecting privacy. We have also highlighted the importance of determining the appropriate amount of information users should be asked to disclose, understanding the regional issues this data sharing aims to address, and formulating a corresponding privacy policy.

Moving forward, we plan to design and implement the proposed system and formulate a comprehensive privacy policy. We will then conduct a demonstration experiment in real-world environments across multiple regions, including commercial facilities in Sapporo and accommodation facilities in Kyoto, to verify whether data sharing under privacy constraints can effectively address regional challenges such as tourism promotion and emergency response by local governments. The results of these efforts will be standardized through the activities of Cityroam, which is advancing OpenRoaming in Japan, with the ultimate goal of commercializing and deploying regional data sharing solutions across Japan.

Acknowledgment

The author would like to thank Ikeuchi Group and Arashiyama Togetsutei for their cooperation in the demonstration experiments as research collaborators.

References

[1] H. Goto, “Inter-federation roaming architecture for large-scale wireless LAN roaming systems,” Journal of Information Processing, vol. 29, pp. 103-112, 2021.

[2] Wireless Broadband Alliance, “OpenRoaming,” https://wballiance.com/openroaming/ (accessed: Nov. 6, 2023).

[3] Wi-Fi IMSI Privacy Protection Group, “IMSI privacy protection for Wi-Fi – technical specification, version 1.0,” Wireless Broadband Alliance, Feb. 2021.

[4] K. Larose, D. Dolson, H. Liu, “Captive portal architecture,” RFC8952, Nov. 2020.

[5] F. Bar, N. Park, “Municipal Wi-Fi networks: The goals, practices, and policy implications of the US case,” Communications and Strategies 61 (1), 107-124, 2006.

[6] V. Gunasekaran, F. C. Harmantzis, “Towards a Wi-Fi ecosystem: Technology integration and emerging service models,” Telecommunications Policy, Vol. 32, Issues 3–4, pp. 163-181, 2008.

[7] E. M. Fraser. “The failure of public WiFi.” Journal of Technology, Law & Policy, 14(2), pp. 161-178, 2009.

[8] E. J. Oughton, W. Lehr, K. Katsaros, I. Selinis, D. Bubley, J. Kusuma, “Revisiting Wireless Internet Connectivity: 5G vs Wi-Fi 6,” Telecommunications Policy, Vol. 45, Issue 5, 102127, 2021,

[9] J. Spruytte, A. Benhamiche, M. Chardy, et al., “Modeling the relationship between network operators and venue owners in public Wi-Fi deployment using non-cooperative game theory.” J Wireless Com Network 2019, 243, 2019.

[10] Chien-Kai Tseng, Kuang-Chiu Huang, “Life Cycle of Municipal Wi-Fi,” 14th Asia-Pacific Regional Conference of the International Telecommunications Society (ITS): "Mapping ICT into Transformation for the Next Information Society", Kyoto, Japan, June 2017.

[11] F. Adrangi, A. Lior, J. Korhonen, J. Loughney, “Chargeable user ientity,” RFC4372, Jan. 2006.

[12] C. J. Bernardos, J. C. Zúñiga and P. O'Hanlon, “Wi-Fi internet connectivity and privacy: Hiding your tracks on the wireless Internet,” 2015 IEEE Conference on Standards for Communications and Networking (CSCN), Tokyo, Japan, 2015, pp. 193-198, doi: 10.1109/CSCN.2015.7390443.

[13] Y. Okabe, M. Nakamura and H. Goto, “Dynamic VLAN Assignment for Local Users Under External IdP Management in RADIUS-Based Wi-Fi Roaming,” 2024 International Conference on Information Networking (ICOIN), Ho Chi Minh City, Vietnam, 2024, pp. 484-489, doi: 10.1109/ICOIN59985.2024.10572099.

[14] Farid Adrangi , Avi Lior , Dr. Bernard D. Aboba , Hannes Tschofenig , Mark Jones “Carrying Location Objects in RADIUS and Diameter,” RFC5580, Aug. 2009.