Journal of The Korea Society of Computer and Information
Vol. 24 No. 1, pp. 145-149, January 2019
www.ksci.re.kr
https://doi.org/10.9708/jksci.2019.24.01.145

User attribute verification method using user mobile dynamic information

Seok-Hun Kim*

Abstract

Various supplementary authentication methods are used to supplement user authentication and authorization provided by existing password verification online1. In recent years, authentication and authorization methods using user attribute information have been studied and utilized in various services. User attribute information can be divided into static information and dynamic information. The existing methods focus on research to identify users using dynamic information or to generate challenge questions for user reauthentication. Static information such as a user's home address, school, company, etc. is associated with dynamic information such as location information. We propose a method to verify user attribute information by using the association between two attribute information. For this purpose, the static information of the user is verified by using the user 's location record which is dynamic information. The experiment of this paper collects the dynamic information of the actual user and extracts the static information to verify the user attributes. And we implemented the user attribute information authentication system using the proposal verification method and evaluated the utility based on applicability, convenience, and security.

▸Keyword: User authentication and authorization, Dynamic information, User attribute information.

I. Introduction

Currently, many Internet applications require user identification information as well as simple identification information for the user. In recent years, user authentication and authorization methods using user attribute information such as user authority, status, and mission have been studied and utilized in various services1. User identity verification is the process of verifying an entity based on various user information. The user attribute information used in this process greatly affects the verification reliability of identity verification. we propose a secure user attribute verification method using dynamic attribute information of users in order to provide high accuracy of identity confirmation online in order to provide more accurate identity verification according to domestic and foreign policy situation. and the verification of the proposed method is implemented by realizing the user attribute information authentication system and verifying the performance of the system using actual user data2-4. The proposed method can divide user attribute information into identification information and auxiliary information and provide high accuracy for a large number of personal attribute information required for the identity verification level.

In Section 2, we introduce related works. In Section 3, we explain how to collect and verify user attribute information. In Section 4, we implement and evaluate the user attribute information authentication system using the proposed method. Section 5 describes the conclusion of this study.

• First Author: Seok-Hun Kim, Corresponding Author: Seok-Hun Kim
*Seok-Hun Kim(kimshn@pcu.ac.kr), Dept. of. Electronic Commerce, PaiChai University
• Received: 2018. 12. 07, Revised: 2019. 01. 26, Accepted: 2019. 01. 28.
• This work was supported by the research grant of Pai Chai University in 2018.

II. User Attribute Information

Identity verification is the process of verifying an entity based on various user information. The user attribute information used in this process greatly affects the verification reliability of identity verification. The identity verification user information is largely composed of identification attribute information and auxiliary attribute information. An identification attribute is information that is used to uniquely identify an entity in one context by combining one or more pieces of identification information. In addition to the identification attribute information, the auxiliary attribute is the attribute information necessary to support the identity verification process, and indicates the relationship or association between the information subject and the identity information. FinTech technology has evolved over the years, and technology that can pay using smart phones is pouring out. As the mobile environment becomes widespread, cases of abuse are also increasing. Smsing sends a text message impersonating an acquaintance or a public institution, and when a link in the message is clicked, an application containing malicious code is installed. The malicious code obtains the account information, certificate, and personal information contained in the user's smartphone, and then seizes money through financial transaction or micropayment. In addition it is a part that can

not ignore the credit card information theft, the illegal use of the card due to card modification, theft or loss6. In order to prevent fraudulent use of the credit card, there is an abnormal transaction detection system for preventing fraudulent use at the Fintech Service Provider. This enables the user to block or further authentication before payment even if the financial information is exposed to fraudulent use. At this time, studies on increasing accuracy of abnormal transaction detection using GPS information of user terminal have been actively carried out2. In recent years, user authentication techniques have been introduced to facilitate access to user location data. Based on this research, we intend to utilize location information which is dynamic information in user attribute verification method.

III. Identification information collection

In order to prevent the user from collecting the attribute information of the user indiscriminately, the proposed method requires only the attribute information required for the service requested by the user and can receive the input directly. Alternatively, the proposed method uses the Open API based authentication protocol such as OAuth (Structured / Unstructured) registered and generated by the user. User identity information required for each identity proofing assurance level is divided into basic verification attributes and extended verification attributes for the assurance level evaluation. The detailed data and the collection method of the verification attribute are shown in Table 1.

Table 1. Verification attribute information by LoIP

Level	Basic Verification Attribute	Expansion Verification Attribute
LoIP0	ID	-
LoIP1	Identification Information (resident registration number, email, cellular phone number)	Register Information (name, age, birthday, gender, country, etc.)
LoIP2	LoIP1 +Corroborative information	User registration information and user creation information (profile, address, school, workplace, friends list, photo, etc.)
LoIP3	LoIP1 + LoIP2 + Authoritative information (registration card, passport information, driver license)	Responses to feature-based queries, requested creation information (posts, photos, location, etc.)

The dynamic attribute of the user is received from the dynamic attribute information server and is compared with the static attribute information. The server collecting the dynamic attribute information consists of a method of receiving the location information record from the user and a method of collecting the location record information collected from the user's mobile terminal through the program developed in the present invention by transmitting the information to the dynamic property information server .Google can provide users with enhanced search results and recommendation services by using Location History on their mobile device (Android OS). For example, you can get recommended services depending on where you visit with the logged-in device, or you can use predictive information about the daily traffic situation on your commute. The information stored in the location record can be controlled by the user, and the record can be deleted at any time. You

can enable or disable the location mode of your Android device. You can also collect your location history from your iOS on iPhone, which can be configured using the Google app. You can also change the location accuracy mode of your device. Accuracy mode uses several different sources to predict the location of the device. Using location information on your device, you can get your location (dynamic) information based on the location of your Android device. For example, the user's dynamic information can be obtained through the position record as shown in Figure 1.

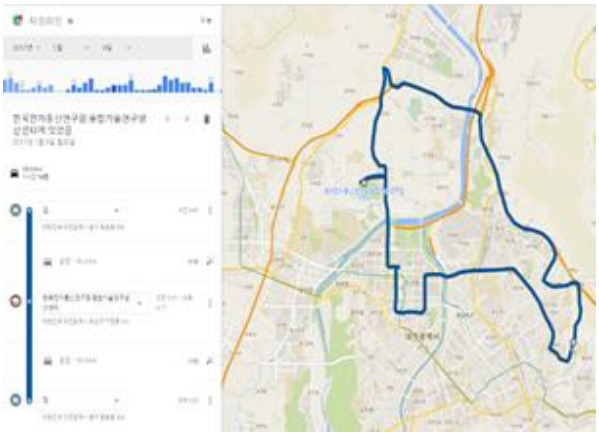

Fig. 1. User's location record using Google Map

The location record thus stored can be confirmed on the web or mobile, and it is also possible to receive this information as data. In this study, user 's user download directly using data download function of Google and submit dynamic information to IDP server which is a proposed system. In this study, JSON format is used to collect and process dynamic information.

Dynamic attribute (Above) In order to collect information, user must install dedicated application for location information and connect to server. Figure 3 shows the results of the user performing authentication and collecting location information in the application to collect dynamic attribute information.

Fig. 2. Screenshot of the user logging in to the location-gathering application

After logging in, the activity that controls GPS information is activated by default. When the START button is pressed, the GPS collection information is activated and collects the data and transmits it to the database automatically. At the bottom, the most recently collected information is displayed together with the presence or absence of GPS collection. At the very first request, the user is asked to use the location data in the application and the service is activated at the time of permission agreement.

Fig. 3. Location Permission Setting Screen

The collected information is transmitted to the database every time the location is changed. The collected location information is transmitted to the database by applying the location information update request method described above for duplication of values or efficient data extraction at the time of storage. In the user authentication page, the user is authenticated using the location information based on the accumulated dynamic information transmitted by the user. The user can authenticate the user by comparing the analyzed static property information with the collected static property information.

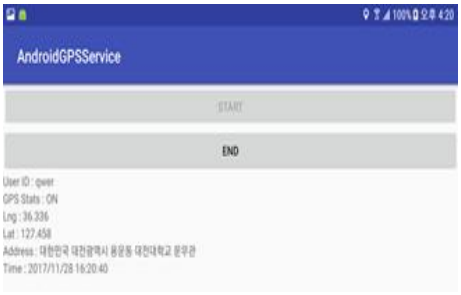

Fig. 4. Example of location information collect

IV. Implementation and verification of proposed method (evaluation)

In this paper, we propose a method for verifying the user 's static attribute information based on the user' s dynamic information and verifying the user 's non - face - to - face identity in order to improve the reliability and accuracy of guarantee based on this. I will use it. In order to perform non-face identification verification, it is very important to extract and analyze highly accurate dynamic information based on the user's accumulated dynamic information. The location data provided by Google is provided in the form of JSON or KML file. In this study, we performed the work based on the JSON file.

```
{
  "locations" : [ {
    "timestampMs" : "1507691825020",
    "latitudeE7" : 363380993,
    "longitudeE7" : 1274570465,
    "accuracy" : 192,
    "velocity" : 0,
    "altitude" : 190
  }, {
    "timestampMs" : "1507670573827",
    "latitudeE7" : 363380993,
    "longitudeE7" : 1274570465,
    "accuracy" : 192,
    "velocity" : 0,
    "altitude" : 190
  }, {
    "timestampMs" : "1507670570488",
    "latitudeE7" : 363380993,
    "longitudeE7" : 1274570465,
    "accuracy" : 192,
    "velocity" : 0,
    "altitude" : 190,
    "activity" : [ {
      "timestampMs" : "1507670569894",
      "activity" : [ {
```


Fig. 5. Location data in collected JSON format

In the development system, the system adds a JSON file parsing operation to primarily parse Google's JSON files that are provided by default. In order to parse and store the information, the data obtained by dividing the given data by 10000000.0 is stored in double format and parsed. The parsing work was done on the server because of the considerable time and risk consumed inside the Android, which could be designed through Java class. When the parsing is completed, the location data is stored in a table in the server, which is used for dynamic location information. Basically, the collected dynamic information and cumulative data of Google location information have a value of longitude and latitude, which is a simple data only. In order to verify with the static information inputted by the user be able to. It uses the Google API called reverse geocoding to provide the location and latitude value of the location information, obtains the address of the coordinates, and enables verification of the location information through comparison with the static address. When the collected data is uploaded, the address value is automatically stored in the database based on the latitude and longitude, and when the dynamic information is requested in the proposed system, the data of the corresponding database is searched to check whether the location is consistent. In the proposed system, dynamic information is requested in the state that the user has input the location information data as follows. The user basically does not have the information about the dynamic information, and compares the data inputted at the time of executing the request with the server database and confirms that they are matched.

V. Conclusions

Identity verification the structure of the proposed system for reliability evaluation is the identity verification service that evaluates and verifies the identity verification level and reliability information based on the user attribute verification that can be utilized by all the organizations on the online. In order to implement and verify this, this study collects and analyzes the user 's static attribute information and dynamic attribute information, performs comparative verification and evaluates it as a four - level rating, and based on the reliability information evaluated at each stage, We propose a service that evaluates and provides information.

REFERENCES

[1] H.Y. Youm, K. H. Kim, and S. H. Kim, “Guideline on Identity Proofing Management”, TTA Journal, Vol. 167, pp.78-82, 2016

[2] K. H. Kim, D. H. Yoo, S. H. Kim, B. J. Yoon, and H. Y. Youm, Gap Analysis of ISO/IEC 29115 and ISO/IEC 29003 for Electronic Financial Services Environment in Korea, Review of Korean Society for Internet Information, Vol. 16, pp.65-69. 2015

[3] Y.J. Shin, S. H. Shin, J. Lee, and W. Han, "A Study on Improvement of Identification Means in R.O.K.", Journal of Korean Association forRegional Information Society, Vol.18, No. 4, pp.59-88, 2015.
[4] E. M. Underwood, J. E. Sullivan, and R. McGeehan, "Social age verification engine", U.S. Patent 8 671 453, Mar. 11, 2014.
[5] L. Li, X. Zhao, and G. Xue, "Searching in the dark: A framework for authenticating unknown users in online social networks", in Proc. Glob. Commun. Conf. (GLOBECOM), Anaheim, CA, USA, pp. 714–719. 2012
[6] James Clause, Wanchun Li, and Alessandro Orso. Dytan: A Generic Dynamic Taint Analysis Framework. In Proceedings of the 2007 International Symposium on Software Testing and Analysis, ISSTA '07, pages 196{206, New York, NY, USA, 2007. ACM.
[7] Manuel Egele, Christopher Kruegel, Engin Kirda, and Giovanni Vigna. PiOS: Detecting Privacy Leaks in iOS Applications. In Proceedings of the Network and Distributed System Security Symposium, NDSS '11, San Diego, CA, February 2011.
[8] Maxwell Krohn, Alexander Yip, Micah Brodsky, Natan Clier, M. Frans Kaashoek, Eddie Kohler, and Robert Morris. Information Flow Control for Standard OS Abstractions. In Proceedings of 21st ACM SIGOPS Symposium on Operating Systems Principles, SOSP '07, pages 321{334, New York, NY, USA, 2007.
[9] Lok Kwong Yan and Heng Yin. DroidScope: Seamlessly Reconstructing the OS and Dalvik Semantic Views for Dynamic Android Malware Analysis. In Proceedings of the 21st USENIX Conference on Security Symposium, Security '12, pages 29{29, Berkeley, CA, USA, 2012.
[10] Rolland, C., Prakash, C., "Bridging the Gap Between Organisational Needs and ERP Functionality", RE Journal 5(3):180–193, Springer, 2000.

Authors

Seok-Hun Kim received the M.S and Ph.D. degree in Computer Engineering from Hannam University in 2003 and 2006. He is an assistant professor Mobile Media at Suwon Women's University in from 2012 to 2017. Dr.Kim is currently an assistant professor in the Electronic Commerce at Paichai University. His teaching and research specialties are in the fields Mobile computing, Web-App programming, information security.