The simple location-based authentication method using multi-layer display in Korea

KwangJong Ahn
June-Suh Cho
Hankuk University of Foreign Studies
Seoul, Korea

Keywords
location information, authentication, security, multi-layer display

Abstract

The importance of selecting an environment appropriate authentication method is the most crucial decision in designing secure systems. In particular, authentication such as login process is more considering with security threat.

This paper introduces the method of location-based authentication using multi-layer display which is the ability to authenticate pc and mobile users based on location-based information they would carry out anyway. The system generates authentication information on multi-layer display by users' current location information captured by smartphones, PCs, time, and weather information to authenticate users. We develop a simple model and application for how to perform location-based authentication, which is working on the multi-layer display, describe the benefits of our method.

Our preliminary findings support that this is a meaningful approach, whether used to increase usability or increase security and simplicity.

Corresponding author: June-Suh Cho
Email addresses for the corresponding author: jscho@hufs.ac.kr
First submission received: 12th April 2019
Revised submission received: 6th May 2019
Accepted: 20th May 2019

Acknowledgement
This study was supported by Hankuk University of Foreign Studies Research Fund of 2019.

Introduction

All the time, security is a major issue in all area including the private and public sector. In particular, authentication such as login process is more considering with security threat. Past years, authentication and authorization can be accomplished in many ways. The importance of selecting an environment appropriate authentication and authorization methods are the most crucial decision in designing secure systems.

Each authentication method has advantages and disadvantages in terms of security, usability, and breadth of support. Password-based authentication methods, however, do not provide strong security and their use is not recommended. It is recommended that you use a certificate-based authentication method for all network access methods that support the use of certificates.

Mobile devices, such as Smartphones, are more and more used by Internet users for different services including social network services, online shopping, entertainment, etc. User authentication with ID & Password on such devices is not user-friendly and does not offer secure authentication for users.

User authentication can be handled using one or more different authentication methods. Some authentication methods such as plain ID/password authentication are easily implemented but are in general weak and primitive. The fact that plain password authentication it is still by far the most widely used form of authentication, gives credence to the seriousness of the lack of security on the Internet, mobile, and within private networks.

Other authentication methods may be more complex and require more time to implement and maintain, provide strong and reliable authentication (provided one keeps its secrets secret, i.e. private keys and phrases). That being said, one of the key factors to be considered in determining which method of authentication to implement is usability. The usability factor cannot be ignored when designing authentication systems. If the authentication methods are not deemed usable by those forced to utilize them, then they will avoid using the system or persistently try to bypass them. Usability is a key issue.

In Korea, various personal authentication methods are used. Especially, since it has a public certificate issued by an authorized institution such as a bank or government agency that has increased safety, it is used more than ID and password for most personal authentication, and it is required to be used in PC or mobile. However, in order to increase safety, certificates are often required to be updated and renewed, and there is a period of use, which is inconvenient for users. Also, we use public certificates as personal certificates, which are made ActiveX based, which provides security and usability inconveniences. In this paper, to solve this inconvenience, we propose a method to securely authenticate a person without using a public certificate by using location information.

As the use of mobile phones increases, discussions about personal authentication of mobile phones will continue and will become even more important. The proposed method can be used on both pc and mobile phone.

This paper presents a simple location-based authentication method and system where the method generates authentication information by users' current location information captured by smartphones, PC, time, and weather information to authenticate users.

Background

So far, Authentication and authorization are two of the most important security features for pc as well as mobile transaction systems. With the development of the IT industry, information that can identify an individual is essential for everyday activities such as personal financial transactions, individual and corporate contracts, and transactions, and individual and individual contracts.

Recently, researchers are interested in location-based authentication to improve security. (Jaros & Kuchta, 2010; Jaros & Kuchta, 2011) (Cho et al., 2006; Hachiya & Bandai, 2013) introduced a system which is a location-based authentication using space dependent information such as service set identifier (SSID) from WLAN access points. (Albayram et al., 2014) proposed a location-based authentication system which builds a location profile for a user based on periodically logged Wi-Fi access point beacons over time and leverages this location. Also, (Li & Bours, 2018) proposed a method to authenticate the user by using WiFi and accelerometer data collected. (Takamizawa & Kaijiri, 2009) proposed and designed an authentication method using location information obtained from mobile telephones that is suitable in web-based education applications. (Jansen & Korolev, 2009) designed a location-based authentication mechanism that involves policy beacons and mobile devices. These policy beacons broadcast and communicate location data to mobile devices using Bluetooth. (Lenzini et al, 2008) analyzed how location information can be used to strengthen access control mechanisms by adding features for defining and enforcing location-based policies.

In general, there are five common authentication methods including Password and PIN-based authentication, SMS based authentication, Symmetric-key authentication, Public-key authentication, and Biometric authentication.

First, Password and PIN-based authentication are using a password or Personal Identification Number (PIN) to login is the most common knowledge-based (something you know) authentication method.

Second, SMS based authentication is used as a delivery channel for a one-time password (OTP) generated by an information system. The user receives a password through the message shown in the cell phone and enters the password to complete the authentication.

Third, Symmetric-key authentication is that user shares a unique, secret key with an authentication server in symmetric key authentication. The user may be required to send a randomly generated message encrypted by the secret key to the authentication server. If the server can match the received encrypted message using its shared secret key, the user is authenticated. A slight variation of this approach is the use

of OTP tokens, which generate the OTP on the user side for matching with that generated on the server side.

Fourth, Public-key authentication is that Public-key cryptography provides an authentication method that uses a private and public key pair. A private key is kept secretly by the user, while the corresponding public key is commonly embedded in a certificate digitally signed by a certification authority. The certificate is made available to others.

Finally, Biometric authentication is a method by which a person's authentication information is generated by digitizing measurements of a physiological or behavioral characteristic. Biometric authentication verifies the user's claimed identity by comparing an encoded value with a stored value of the concerned biometric characteristic. (Mahbub et al., 2016)

Biometric recognition is largely studied in computer science. The use of biometric techniques, such as the face, fingerprints, iris, and ears are a solution for obtaining a secure personal authentication method. (Yang & Nanni, 2013) (Ninassi et al., 2018) proposed a method using fingerprint and behavioral biometrics to enhance the security of user authentication. The behavior when entering a pattern-based authentication on the smartphone touch screen is considered as a fast and usable solution for users. The names of countries around the world are slightly different, but they give their numbers to individuals for identification. That is, a personal identification number is assigned for the purpose of providing tax administration services such as social security programs such as pensions and taxation. The United States gives the Social Security Number (SSN), the United Kingdom the National Insurance Number (NIN), and Australia gives the taxpayer the Tax File Number (TFN). Although these numbers are issued for specific administrative services such as welfare or taxation, they have the function of identifying individuals, such as the Korean resident registration number, and they are actually used as such functions.

In the United States, public institutions and corporate sites, except financial sites, can be used only by inputting their name, birthday, address, etc. without a clear authentication system. It is difficult to find Internet services that require authentication in Australia. This is because the authentication for membership is limited to a specific service. The case of Japan is not so different from those of the above two countries. In the case of Germany, it is possible to authenticate through the existing chip card when the online identity verification is needed. As a means of personal authentication, which is widely used in Korea, there are public certificates, IPIN, and mobile phone authentication. Among them, public certificates are used most often as personal authentication methods. The authorized certificate includes information such as a serial number, an owner's real name, an electronic signature verification key (public key), an issuer identification name, a certificate valid period, an issuer certificate policy, and an electronic signature value. This identifies the trading partner and prevents the document from being altered or altered. Individuals or corporations wishing to issue certificates should visit the accredited certification body or registrar agency in person. There are general purpose certificates that can be used in all fields, and restricted use certificates that can only be used in specific fields such as banking transactions.

IPIN is a self-certification tool created by the government to minimize the damage of personal information. It is positive that the information is not disclosed to the other party unlike the authentication of the mobile phone. However, since it is inconvenient to use and this also creates a new account, if the account is hacked, the same ID and password can be used to create a bigger problem. Also, because it requires troublesome usage, it is criticized as a waste of tax, and in recent years, users are gradually falling. Most people use personal authentication of a mobile phone rather than a universal certificate or IPIN because it is a simple procedure. In case of personal authentication of mobile phone. There are more cases where consent items are exposed in the same place to agree to unnecessary advertising. In addition, accurate information about the contents of the service was not provided, so that there was a problem of being exposed to secondary marketing in addition to the leakage of the primary personal information.

The identity verification by mobile authentication is mainly OTP token method, and it is not popularized because it has a disadvantage that the user has to buy it by the token in spite of security advantage that only a dynamic password can be generated by exclusive use. So, what is mainly used is

identity authentication by the SMS method. This is a method of verifying the information entered by the user with the database of the mobile communication company and transmitting the disposable authentication number when authenticating the authentication number. This is an authentication technology that enhances security by adding a procedure to compare with the database of the mobile communication company as compared with the method of performing only the existing one-time authentication.

The proposed method

In this paper, we introduce the unique method of authentication based on location information and multi-layer technique from devices and systems. This method uses the location information such as GPS (Global Positioning System), IP (Internet Protocol) address, time, and weather information. By comparing the user location information and approving the user authentication when the two locations coincide with each other within the set error range, the risk of hacking in the electronic financial transaction can be greatly reduced. The terminal position information can be obtained by the API (Application Program Interface) inquiry method without the user's keyboard input. In addition, it is possible to provide convenient and safe authentication means to both electronic financial provider and user by supporting cross-platform and cross browsing since there is no need to install a separate nonstandard plug-in.

For example, when a user inputs an existing user name (ID) and a password in order to log in to a system of a company or an organization to which the user belongs, and a predetermined portable terminal such as a smartphone is connected to a wireless communication device such as a Wi-fi used to confirm whether or not the portable terminal ID is coincident and whether the current position is an authorized position set in advance. This technology further strengthens user identification and ultimately improves security against organizational systems and access to confidential information.

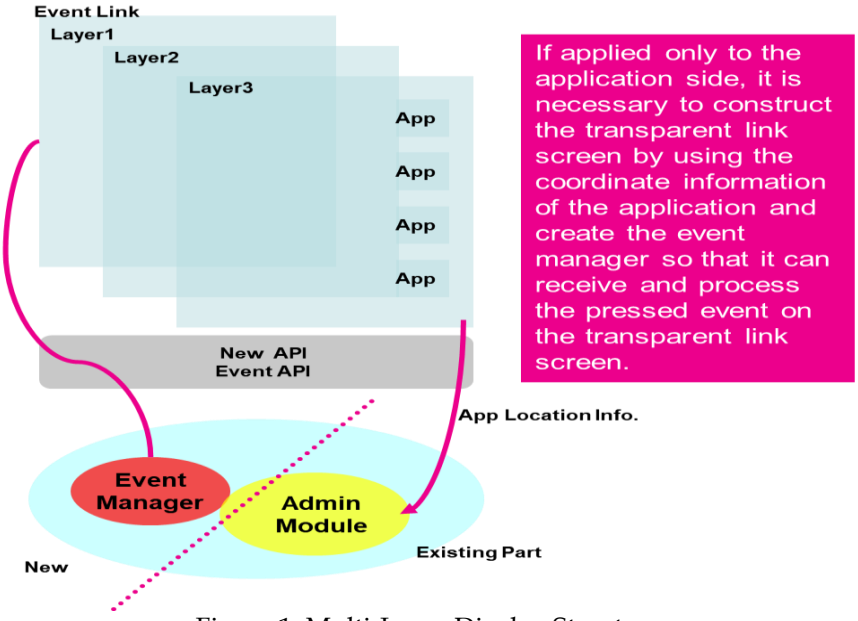

Figure 1. Multi-Layer Display Structure

3.1 Multi-Layer Display Method

A device such as a computer or a smartphone has a display, and a display of a program executed according to a user's operation is displayed on the display. For example, when a user runs an Internet Explorer on a general desktop computer, a screen of a web site accessed by the computer is displayed on the desktop of the monitor provided in the computer. A plurality of GUIs (Graphic User Interfaces) is provided in a general web site screen. The user places a cursor on the desired portion of the various GUIs provided on the web site screen and then executes the desired function in such a manner as clicking with a mouse or moves to another web site linked to the GUI.

Figure 1 shows the multi-layer display which provides running different applications at each layer. If applied only to the application side, it is necessary to construct the transparent link screen by using the coordinate information of the application and create the event manager so that it can receive and process the pressed event on the transparent link screen. Here we utilize the layers in which location information appears. Each layer serves as a window so that you can log in only when the four types of location information provided a match. Using these four types of information, the four layers perform location information matching with each type of information. If the type of information matched, the login window is activated so that an ID and a password can be inserted.

The Location-Based Authentication Method

3.2.1 Location-based Login

To location-based login, four types of location information should be matched including smartphones, PC, time, and weather information. Figure 2 shows the structure of the location-based login process.

In Korea, two authentication methods are generally used. One is to use a user ID and password, and the other is to use a public certificate. To use a public certificate, you need to install a certificate program, which works in ActiveX format. In addition, the certificate must be installed as needed, renewed annually for continued use, and the certificate must be stored on a PC, laptop, or USB device.

Figure 2. Location-based Login Process

In the proposed method, the smartphone provides sources of data from authentication including location and co-location data from GPS coordinates. PC also provides a known access point as an indicator such as IP address and time. The weather data provides secure data with location information of devices.

In the case of PC, all of the above four pieces of location information are needed, but in case of mobile, the remaining pieces of location information excluding the information provided by PC are used.

3.2.2 Location-based Login Service Structure

According to the proposed method, the following information must match in order to log in. Figure 3 shows the login service structure using location information including mobile chip data, internet IP data,

her data, and time data. After matching this data, the process can be input id and password. The boundary of this location information is 50 meters from the central location.

It uses location information using GPS of a mobile terminal that is currently owned, uses location information such as IP address from PC or laptop to use, uses safe location information data of Meteorological Agency, and provides stable location-based time data is used. If these types of information do not match, IDs and passwords cannot be entered, and only when the provided information matches.

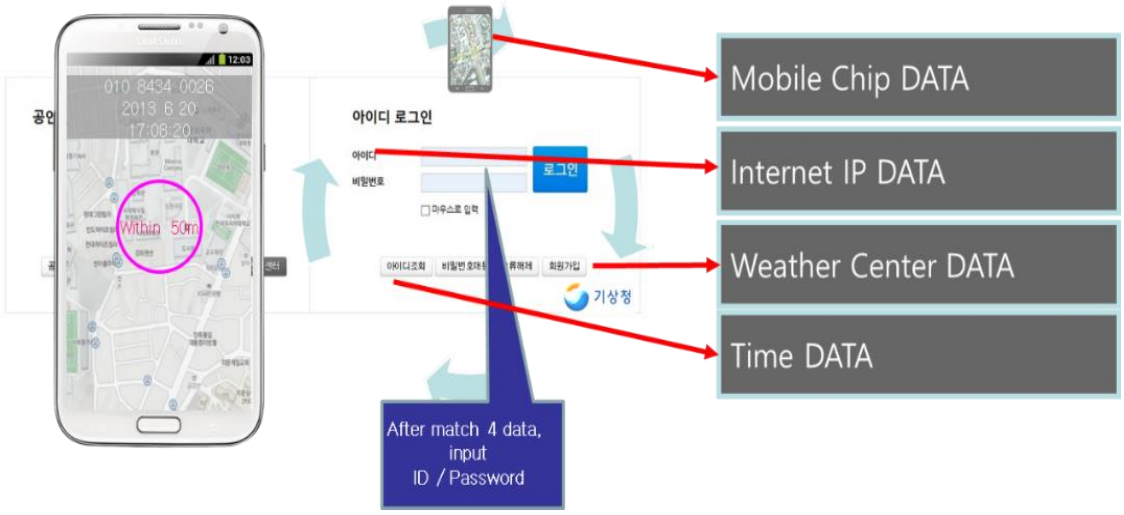

Figure 3. Location-based Login Service Structure

3.2.3 Service Feature

In figure 4, the features of the proposed location based services are as follows. First, login can be done only if the location information is matched. This location-based service does not need to use the ActiveX for a public certificate that is currently used. The method provides a simple UI since old methods are too complicated and use the secure data of the telecommunication communication companies. It also utilizes secure networks and weather data from the national weather center and provides the convenience of not using certificates such as a public certificate. Especially, it is a key feature to remove ActiveX which is still widely used in Korea and to utilize stable data provided by telecommunication company, system and meteorological center.

Based on these facts described above, the proposed method can be a potential solution for location-based authentication and authorization schemes. Also, it is not necessary to set up a specialized infrastructure in order to use our method. Compared with most existing methods, described in the related work, where special devices must be used for location-based services, in our method users do not have to use specific devices. The proposed method is easy and flexible to integrate with any existing authentication/authorization systems. Our method can work as a security plugin for existing systems.

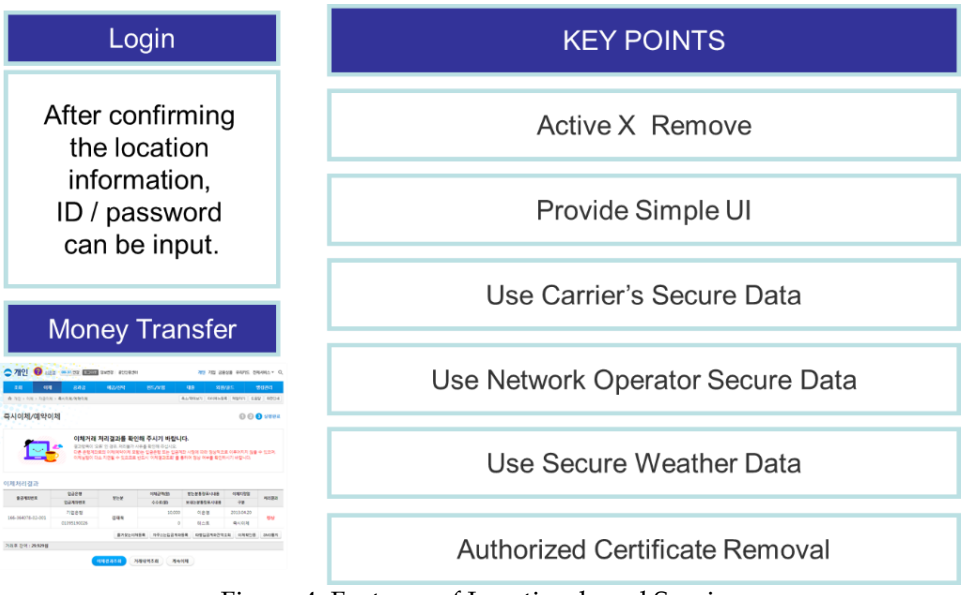

Figure 4. Features of Location-based Service

Conclusion and discussion

This paper presented a simple location-based authentication method and system where the method generates authentication information by users' current location information captured by smartphones, PC, time, and weather information to authenticate users.

In this paper, a location-based authentication mechanism using smartphones and PCs are proposed and described. The proposed method provides comprehensive protections for transmission, procession, and verification of location information. For location verification, we propose a hybrid approach, which combines various technologies. This approach improves the confidence of verification results, compared with other solutions where only one factor is used for location verification.

Other authentication methods may be more complex and require more time to implement and maintain, provide strong and reliable authentication. We proposed a simple model and application for how to perform location-based authentication, which is working on the multi-layer display. As a result, our location-based authentication mechanism becomes more secure and valid. The proposed method provides increasing usability, security, and simplicity. As the use of mobile phones increases, discussions on personal authentication of mobile phones will continue. The disadvantage of the mobile phone personal authentication method in Korea is that there is a high possibility of leakage of personal information when the mobile phone personal authentication is performed in comparison with other countries, and there is a troublesome method.

Until now, personal authentication methods of mobile phones have been changed and applied according to need. Such a mobile personal authentication method is likely to cause problems in continuity. In the future, it is highly likely that the authentication of the user based on the mobile phone becomes more active. Therefore, it is necessary to simplify a lot of current services, and it is necessary to complement the shortage of current systems and to organize them into a single system.

The first area that needs to be developed is convenience. Currently, mobile phone personal authentication service in Korea is convenient because it can be used anytime and anywhere, but it has a disadvantage that it is difficult to know because it is so diverse.

The second area to be improved is security. So far, laws and regulations have not been developed according to the development of technology. There is little law that cannot regulate the leakage of personal information. Most people think that the importance of personal information and security is important. Now, because of the convenience of personal authentication, personal information is leaked and abused frequently.

Finally, it is necessary to continuously check and evaluate the method of personal authentication of the mobile phone. In recent years, personal authentication methods have been continuously developed and new information communication environments are being developed. Therefore, cases of accidents will increase more and more cases will be used in important fields. Therefore, it is necessary to continuously supervise and improve the personal authentication services of mobile phones through evaluation.

In Korea, it is difficult to find internet services that do not require self-certification, but on the other hand, it is difficult to find internet services that require self-certification overseas. This is because the authentication for membership is limited to a specific service. In Korea 's view, this perception is due to Korea' s gloomy information security situation. All transactions are always exposed to fraud risk, regardless of whether they are offline or in a dark situation where most people's social security numbers and other credit information are leaked once and personal information is being traded on the black market. Moreover, because the certification itself through the resident registration number is also lost in trust, the possibility of e-commerce without authentication is perceived as fear in Korea.

On the other hand, personal information is securely stored in overseas countries such as the United States, Australia, and Germany, and fraud by impersonation is not as serious as in Korea. Rather, Korea has such a diverse and complicated self-certification system that there is a voice that it is a preventive measure for companies to take responsibility for the leakage of customer information. Nevertheless, there are many problems in Korea such as personal information theft and leakage, and it is a sensitive issue. Therefore, in the situation where personal authentication is essential, mobile phone authentication is surely a convenient and suitable means of personal authentication for people living in Korea.

Korea is a mobile advanced country including mobile phones, and it provides a variety of services through mobile, and in the process, it requires a means of confirming identity verification in various fields.

In the future, the development of various technologies will lead to a different approach to the authentication service through mobile phone. In applying the authentication service of the user, the universality, persistence, uniqueness, convenience, security, economic efficiency, Etc., to ensure the diversity of means of identity verification based on safety. One of the most emphasized and important aspects of personal authentication is how securely the individual's information used for authentication is used without being leaked, ie, 'security'. From this point of view, it can be said that multi-element authentication, which requires various authentication factors, is more secure than single-factor authentication, which requires only one authentication factor for the user.

'Convenience' is also an important factor, and the development of personal authentication technology for mobile phones is widely used in various fields. Therefore, it can be said that the method of personal authentication of the mobile phone should also provide the user with a certain degree of convenience. From this point of view, the most convenient method among individual mobile phone personal authentication methods presented in the above can be said to be authentication methods using single-factor authentication. Among the cellular phone personal authentication methods, a strong security authentication method requires a relatively complicated and inconvenient authentication procedure, and a relatively low-security authentication method tends to have a relatively convenient and quick authentication procedure. It is natural that the more complex and longer the authentication procedure becomes, the more tedious and uncomfortable the user feels. So how do you minimize the security and convenience gap in personal authentication? The correct answer is in 'Converting individual consciousness of users'. In fact, many of the personal authentication related security incidents are caused by the carelessness of individual users. No matter how fast and diversified personal authentication technology develops due to the technological advances that become more and more sophisticated over time, if the security consciousness of the user is assumed, the true development cannot be achieved. Therefore, the user should try to overcome the security culture delay phenomenon and to have the right security consciousness by always taking care of his/her information and account and participating actively in multi-factor authentication.

In the future, security and convenience should be applied to the issues of personal authentication continuously and methods for solving the problems.

References

Albayram, Y., Khan, M., Bamis, A., Kentros, S., Nguyen, N., & Jiang, R. (2014). A Location-Based Authentication System Leveraging Smartphones. IEEE 15th International Conference on Mobile Data Management.

Cho, YounSun, Godrich, Michael & Bao, Lichun. (2006). "Secure Access Control for Location-Based Application in WLAN Systems", Mobile Adhoc and Sensor Systems (MASS).

Hachiya, T. & Bandai, M. (2013). Location-based authentication system using space dependent information, MobiSys.

Jakobsson, M., Shi, E., Golle, P. & Chow, R. (2009). "Implicit Authentication for Mobile Devices", Hotsec.

Jansen, W. & Korolev, V. (2009). "A Location-Based Mechanism for Mobile Device Security", in WRI World Congress on Computer Science and Information Engineering, Los Angeles, California USA.

Jaros, D. & Kuchta, R. (2010). "New Location-based Authentication Techniques in the Access Management", Sixth International Conference on Wireless and Mobile communications.

Jaros, D., Kuchta, R. & Vrba, R. (2011). "The Location-based Authentication with The Active Infrastructure", The Sixth International Conference on Internet and Web Applications and Services.

Lenzini, G., Bargh, M. & Hulsebosch, B. (2008). "Trust-enhanced Security in Location-based Adaptive Authentication," Electronic Notes in Theoretical Computer Science, vol. 197, pp. 105-119.

Li, G. & Bours, P. (2018). Studying WiFi and Accelerometer Data Based Authentication Method on Mobile Phones. ICBEA.

Mahbub, U., Sarkar, S. & Chellappa, R. (2016). Active user authentication for smartphones: A challenge data set and benchmark results. IEEE 8th International Conference on Biometrics Theory, Applications and Systems.

Ninassi, A., Vernois, S. & Rosenberger, C. (2018). Privacy Compliant Multi-Biometric Authentication on Smartphones. ICISSP.

Takamizawa, H. & Kaijiri, K. (2009). "A Web Authentication System using Location Information from Mobile Telephones", Proceedings of the IASTED International Conference Web-based Education.

Yang, I. & Nanni, L. (2011). State of the art in Biometrics. InTech.