A New Security Passcode Approach for Alzheimier Patient based on Geo-Location Identification

Amir Adhwa Afiq Samsuri, Mohamad Fakhruddin Mustafa, Nor Azhar Ahmad
Fakulti Sistem Komputer & Kejuruteraan Perisian, Universiti Malaysia Pahang, Lebuhraya Tun Razak, 26300 Gambang, Pahang, MALAYSIA
ameersamsuri2908@gmail.com, din91dns@gmail.com, nazhar@ump.edu.my

Highlights: Alzheimer disease is one of the common syndromes categorized under dementia cases. In some records, it shows that this illness can't be cured even 10 to 20 years of procedure. The common symptoms that suffered by the patients are amnesia or loss of memory and ability to thinking correctly [1] [4]. This syndrome may also affect family members, friends, and also some others institution like a company that implements security authentication system. Nowadays, as we can see, no special password authentication system should provide to Alzheimer's patients. Due to lack of authentication technology, there is a need for developing password authentication system, especially for Alzheimer's patients. This document would discuss how to develop a new security passcode approach that can use by the Alzheimer's patients with the assist of geolocation identification method.

Key words: *Alzheimer; syndrome; dementia; symptoms; authentication; password; geolocation*

Introduction

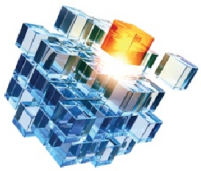
Nowadays, Alzheimer disease has become one the common syndrome suffered by the eldest people after heart disease, stroke and also diabetes. This disease can be categorized under dementia cases which may cause problem with reminiscence, thinking ability and cognitive skill [1] [2] [3] [4]. From some observation, the common syndrome that related to Alzheimer's disease is where the patient will suffer from memory loss, amnesia and lack of thinking ability. So they would difficult to judge some situation by themselves. Malaysian population especially for the eldest people aged 60 and above gradually increasing [2] similar to other countries.

Due to this growth of earliest group population in Malaysia, the number of people suffered from dementia and Alzheimer's disease increase every year [1] [4]. Based on worldwide (World Health Organization) statistics of Alzheimer's cases, it stated that Alzheimer's disease had contributed around 60% to 70% from 35 million people suffered from dementia in 2010 [4]. Some other records indicate that in 2020, the number of Alzheimer patient will increase to 34 million people around the world. In worst cases, it stated that there would be a new Alzheimer cases occurs every second. In Malaysia, the estimation of 50,000 people is diagnosed to have Alzheimer syndrome (Alzheimer Disease Foundation of Malaysia, ADFM). Alzheimer's disease affected not only the patients but also their family, friend and some other institutions mainly that used password authentication system for their authentication procedure.

Based on the observation made from some research of existed authentication system, no suitable password authentication system can be useful for the Alzheimer's

patients. Alzheimer's patients will suffer from memory loss and unconsciousness on making a decision that may affect daily activities. One of the topic that affected by the syndrome is password authentication system. When a person had Alzheimer disease, they will suffer from memory loss and usually not able to remember back their authentication password. There is a need for a development of security password authentication system for the Alzheimer's patients. For the safety purpose, any system that owns the corporate companies or government sector always include a password authentication system to be used by their customers for security measure before they can get authenticated to use the system. So, the related organizations should provide a user-friendly password authentication system for the Alzheimer patients, so they don't need to wait for authorization confirmation if they have an appointment with the organizations. A new password approach is develop using the geolocation authentication method with some assist of one-time password service. With this method, its hope that the Alzheimer's patients would get some benefit from it.

A geolocation authentication proposed in this system development as a new approach for password authentication system that may help the Alzheimer's patients and also the organization that involved. This method should assist the patient during the authentication session where they don't need to remember any password, just wait, and they can get authenticated. Most of the modern devices already equipped with a real-time location coordinator. The geolocation authentication method can prevent the vulnerability of the system to be one of the cyber-attack targets. It 's hard for someone outside the radius to authenticated because the Haversine formula used as a



method for calculation. So, the system will generate the latitude and longitude of the location for the computer that installs this system. Then, the system will calculate the distance of the computer used with the server that should be in the range that already decided. By implementing this technique, the system can eliminate any user that is outside the connection range to prevent intrusion. The geolocation also used as a key for data encryption based on symmetric encryption. A Blowfish encryption method also implemented as an addition to the encryption process to increase authentication procedure.

A two-factor authentication is used in this system to increase the security level. Geolocation authentication is used as location checker while one-time password authentication is used as the second authenticator to make the system more secure. A system can generate a unique password based on a function source code. The one-time password created a line of numbers, a string of alphabets or a combination of some characters. It is quite difficult for someone to guess the auto-generated One-time password. This method can improve the confidentiality of authentication process. Usually, a traditional authentication used as a method for password authentication in which user used their static password. But, this paper proposed to use a One-time password to improve the traditional authentication method [8]. A One-time password can avoid similar password request that related to traditional authentication [8]. It can prevent from any intruders that manage to record the password that commonly related to the phishing attack and also key-logger hackers. A volatile password could lessen the risk of the "man-in-the-middle" attack. The utilization of randomly generated

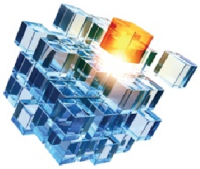
password for one-time used could prevent from password sniffing.

Content

In this section, a brief discussion of the innovation, system development, and its design is made based on the system behavior. Two topics which are geolocation authentication and one-time password methods has become the main topic to be discussed. The background of the study made for this system development will also show next. A desk checking of this proposed scheme and some user interface also provided. The result of this project based on the database will use as a proof of the development. Some future enhancement discussed at the last part of this section.

Proposed Scheme Description

A two-factor authentication is proposed to use in this system. The first authentication procedure might be successfully accessed by the hacker if the hacker understands the method applied in the system. But when second authentication method implemented, there would be some difficulty to break the procedure. So, there is a need for using two-factor authentication to improve the system security level. This system would use geolocation authentication method for the first authenticator and one-time password as the second authenticator. Geolocation generator can be implement based on Location-Sensitive Providers (LSP), while, the One-time password can be generated randomly by the system.



Background of the Proposed Innovation

The first topic to be discussed in this section is the geolocation authentication which it used as the first authenticator. This method will call for a latitude and longitude values of the computer location from the web browser provider. The site generated from Location-Sensitive Provider (LSP) based on the client location which provided in the Web browser. For example, there is some geolocation API that can be used to get current location of the computer as requested and it utilized in this system. Location-Sensitive Providers implement geolocation authentication as a method to restrict some service to some geographic location and also as a method for geolocation authentication. Geolocation authentication can prevent the development system from being a target of cyber-attacks like password guessing attack and phishing attack. The existence of geolocation provider like LSP can help in implementing geolocation authentication service inside any system. For this paper, a prototype of geolocation authentication service is developed to show how is work in authentication procedure. Any user needs to be in the range of system connection before can be authenticated. The formula used to calculate the communication range is as below,

Haversine formula:

$$a = \sin^2(\Delta\varphi/2) + \cos\varphi_1 \cdot \cos\varphi_2 \cdot \sin^2(\Delta\lambda/2)$$
$$c = 2 \cdot \operatorname{atan2}(\sqrt{a}, \sqrt{(1-a)})$$
$$d = R \cdot c$$

where φ is latitude, λ is longitude, R is earth's radius (mean radius = 6,371km); note that angles need to be in radians to pass to trig functions!

Formula 1: Haversine Formula (Veness, 2016)

Next, a one-time password is used to complete the requirement for two-factor authentication, and it commonly is a combination of alphabet and numeric values. This method is used to secure authentication

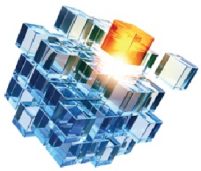
procedure by validating only one login session without relating it from password stored in the database or static password. The password used only valid for one login session, and it will change every time the user login to the system. Users don't need to remember any password because the system will generate the password to be entered by the user. So, it is difficult to attack the system by using a recorded password that usually did by the phisher or hacker to establish a connection to a target system. A One-time password can base on mathematical algorithms, geolocation value, alphanumeric combination, or time-based synchronization value. The standard methods used for one-time password delivery is by messaging service rather than email because of it available in most mobile handsets with a low cost to implement. But, for this system, it is executed on screen One-time password authentication to make it simple to be used.

Methodology of Proposed Innovation

The proposed system is conducted according to the following sequence to establish a secure authentication procedure:

Table 1: Notation for Login Phase

Notation	Description
L0	Latitude value
L1	Longitude vale
D	Distance
U	Username, Identification Number
OTP 1	Generated One-time Password
OTP 2	Generated Mathematical Challenge



Step 1: When the system initiates for login, the user needs to enter their identification card number and then verified by the system.

Step 2: The system generated geolocation of the scheme which includes latitude and longitude. Then, the system will calculate the range of user computer to the server.

Step 3: The system checked for the range and if it outside of the range, the system popup a warning message to the user. If success, it will redirect the user to one-time password login page.

Step 4: System generated a random one-time password and also a mathematical challenge. Then system displayed it to user screen. Users key in the One-time password and the mathematical challenge answer.

Step 5: If the user correctly entered both OTP1 and OTP2, the user gets authenticated to access the system

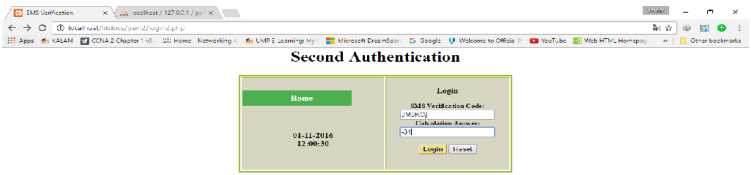


Figure 1: One-time Password Authentication Interface

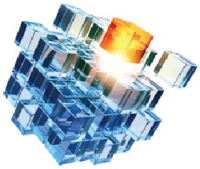
Service for the Community Use

In this proposed scheme, we consider that all users especially the Alzheimer's patient which is the primary target user has their identification card. The system is provided to help the Alzheimer's patient easily do any business with any organization if they want to use the company service. As we know, the Alzheimer's patient commonly suffered from memory loss and unable to make the decision correctly. This proposed system should benefit the target user to be authenticated before can use any system. The system will only ask for authorization of user identity based on the identification card number, and then the system will check for the business location and generated a one-time password. So, users only need to enter the generated One-time password. For future enhancement, there is a plan to use a simple mathematical challenge to replace password generator as a One-time password. One-time password can improve the authentication service.

Proposed System Advantage

Based on geolocation authentication system, the main advantage can describe to restrict a connection range can be accessed by the user. It can avoid from an intruder who wants to attack the system. If they still want to attack the system, they need to be around the connection range. It's Not a good method to be used by the hacker. The second major advantage of this procedure is an additional authentication factor to prevent password-guessing attacks which is one of the cyber-attack.

One-time password authentication is different compared to static password and not vulnerable to password-guessing attacks. It means that if there any intruders that record the used password transmitted along the network connection, they will not able to



abuse the system. Once the password was already used, the password will be replaced in the next session. Another advantage of this method is it can protect the user from being a phishing attack victim. It is because the only authorized user knows that the system is a fake if there is no one-time password service provided. It also gave benefit to the user who had a difficult to remember their password, especially for Alzheimer's patients.

Commercial Values

The primary target user of this system is the Alzheimer's patient. There is a need for any organization that deals with this group of people to use this system as their authentication service. The management doesn't need to process other authentication procedure as long the identity of the user exists in the database system. It highly recommended for any company to use this system to reduce the time consumed to authorize any Alzheimer's patient to access their service. For example, any organization like banking sector which includes insurance claim or health care organization can use this system for service authentication procedure.

Conclusion

This project is to develop a system that implements two-factor authentication which using geolocation authentication and one-time password authentication. Compared to another traditional authentication method that implements static password, this method is more secure due to the use of random password and geolocation authentication. A volatile password could lessen the risk of any cyber-attacks. The step taken in this system authentication can protect from intrusion and also password-guessing attack. The user doesn't need to remember any password, just wait for generated one-

time password and key in the password displayed. It is a benefit to Alzheimer's patient as they don't need to wait for identity verification procedure. It will reduce the time consumed by any related organization.

References

Abdou, A. M., Matrawy, A., & Van Oorschot, P. C. (2014, October). Location verification on the Internet: Towards enforcing location-aware access policies over Internet clients. In *Communications and Network Security (CNS), 2014 IEEE Conference on* (pp. 175-183). IEEE.

Abdou, A., Matrawy, A., & Van Oorschot, P. (2015). CPV: Delay-based Location Verification for the Internet.

Aljunid, S. M., Maimaiti, N., Ahmed, Z., Nur, A. M., Mohamed, N., Saher, M., ... & Koris, R. (2014). Development of clinical pathway for mild cognitive impairment and dementia to quantify cost of age-related cognitive disorders in Malaysia. *Malaysian Journal of Public Health Medicine*, *14*(3), 88-96.

El-Booz, S. A., Attiya, G., & El-Fishawy, N. (2016). A secure cloud storage system combining time-based one-time password and automatic blocker protocol. *EURASIP Journal on Information Security*, *2016*(1), 1-13.

Fiore, M. H., & Chion, M. (2012). *U.S. Patent Application No. 13/444,263*.

Habash, Z. A., Hussain, W., Ishak, W., & Omar, M. H. (2013, August). Android-based application to assit

doctor with Alzheimers patient. In *International Conference on Computing and Informatics* (pp. 511-516).

Jacob, J., Jha, K., Kotak, P., & Puthran, S. (2015, October). Mobile attendance using Near Field Communication and One-Time Password. In *Green Computing and Internet of Things (ICGCIoT), 2015 International Conference on* (pp. 1298-1303). IEEE.

Kamaruzaman, M. F., Anwar, R., & Azahari, M. H. H. (2013). Role of dynamic visual as a mode to enrich reminiscence therapy for patient with dementia. *Procedia-Social and Behavioral Sciences*, *105*, 258-264.

Nikmat, A. W., & Almashoor, S. H. (2013). Depression in Institutionalized Dementia Patients and It's Influence on the Quality of Life. *Procedia-Social and Behavioral Sciences*, *101*, 181-188.

Shivraj, V. L., Rajan, M. A., Singh, M., & Balamuralidhar, P. (2015, February). One time password authentication scheme based on elliptic curves for internet of things (IoT). In *Information Technology: Towards New Smart World (NSITNSW), 2015 5th National Symposium on* (pp. 1-6). IEEE.

Veness, C. (n.d.). Calculate distance, bearing and more between Latitude/Longitude points. Retrieved November 22, 2016, from http://www.movable-type.co.uk/scripts/latlong.html