



Multi-factor Authentication to Authorizing Access to an Application: A Conceptual Framework

Open
Access

Muhamad Zulfikri Md Zin¹, Raihana Md Saidi^{1,*}, Faridah Sappar¹, Mohamad Asrol Arshad¹

¹ Faculty of Computer and Mathematical Sciences, Universiti Teknologi MARA Melaka, Malaysia

ABSTRACT

The use of smart mobile devices in the era of Internet of Things is currently granting significant contribution to the society in moving ahead in green technology environment. This device has taking over our daily task to almost every technology around us from checking calendar to online transaction. Various industries including smart cities, smart homes and also smart campuses adopting the technology in-line with the advancement of green technology for many more beneficial functionalities. Thus, authentication is an essential security mechanism for cyber environment, to proof of identities to get access of information in the system. This paper proposed a framework for multi-factor authentication, an approach to combine more than one factor of authentication which are something you know, somewhere you are and something you have. The proposed framework is applied to allow access to mobile application namely Attendance Record Management System (ARMS) in a campus environment.

Keywords:

Multi-factor authentication; location-based factor; possession factor; inherence factor; geo-fence application

Copyright © 2019 PENERBIT AKADEMIA BARU - All rights reserved

1. Introduction

Authentication is a process that ensures information assurance (IA) and confirms a user's identity. With the advancement of technologies, most of applications require several factors to confirmation of the identity and presence of the user. Multi-factor-authentication (MFA) has provided more secure process than traditional method, also known as single-factor-authentication (SFA). According to Nag, *et al.*, [15], MFA is the current trend to genuinely identify authorized users through the active authentication process such as using passwords, biometrics and cognitive behavior. These can be extended to almost any situation where the identity of the user of credentials needs to be authenticated prior to allowing the individual access to the protected services, systems, or locations.

With the evolution of network, something that you have and something that you know is not enough to prevent from security breach. According to Mare *et al.*, [4], to gather a better understanding of the user authentication burden, the researcher conducted a study using a digital diary. However, some authentication method that is used by some organization is not convenience to use by the individual and expose to many security threads. With some people expect, especially those who working in corporate environment, to carry these authentication token and to remember a complex password is not a good practice.

* Corresponding author.

E-mail address: Raihana Md Saidi (raihana@fskm.uitm.edu.my)

To avoid any internal negligence, the best way to confirm an authentication is to implement biometric and location-based authentication. Biometric authentication is a security process that relies on the unique biological characteristics of an individual to verify that he is who he says he is. Biometric authentication is a quick, accurate, and user-friendly tool that offers an efficient solution in multiple access control systems. Biometric authentication compares a biometric data capture to stored, confirmed authentic data in a database. If both are match, authentication is confirmed.

Besides, location-based authentication is a unique procedure to prove an individual's identity on appearance simply by detecting its presence at a distinct location. According to Kawamoto and friends, location-based authentication uses ambient information, which is collected from the devices as unique information at a certain place and a certain time. Logically, this type of authentication is generated based on users' locations tracked by smartphone. The geo-fence method contribute to authentication where a virtual geographic boundary, defined by GPS or RFID technology, that enables software to trigger a response when a mobile device enters or leaves a particular area

This paper presents a framework for advanced device authentication using possession factor (MAC address of the mobile device), location-based factor (geo-fence location) and inherence factor (biometric fingerprint). An Attendance Record Management System (ARMS) has been developed to record the attendance of an employee when entering and leaving the workplace.

2. Literature Review

According to Soni *et al.*, [19], authentication is a method by which a system verifies and validates the identity of a user of the system who wishes to access it. It ensures and confirms a user's identity through a code such as a password and verifies genuineness of a document or signature, to make it effective or valid. It is the measure employed to ensure that the entity requesting access to a system is what or who it claims to be, and to counter any inappropriate or unauthorized access. Authorization is the method of giving individuals access to system objects like information, application programs based on their identity.

This paper combined three factor authentication which are location-based factor, possession factor and inherence factor to record the attendance of employee in an organization.

Location-based Authentication

Most of smartphones are inbuilt with Global Positioning System (GPS) that can which utilize satellite triangulation, or some sort of signal triangulation (e.g., mobile phone signal) to identify the approximate location of the user.

A study conducted by Zhang [8], most of smart phones is equipped with inbuilt global positioning system (GPS) chips that can accurately detect the location of the user. This is evidenced by the explosion of location-based services, such as Google Maps and Foursquare. It is feasible to determine the location of a user within meters of their actual location. Smart phones can be used to detect and send the location of a particular user to back-end servers, which shall verify the location as a factor for authentication and authorization purpose.

Geofence technology is a virtual barrier that will give notifications whenever user entering or exiting the barrier. According to Makhtar *et al.*, [13] geofence is a virtual barrier that used the global positioning system (GPS) or radio frequency identification (RFID) to define geographical boundaries. Geofence applications also incorporate with google earth to define the boundaries using the satellite. Furthermore, geofence will enable the administrator to set up triggers so when a gadget enters (or leaves) the limits of boundaries, there will be alert issued immediately.

According to Galinina *et al.*, [9], the geofence is carry out by joining a user position with a geofence perimeter. The project is conceivable to know whether the user is inside or outside the geofence or regardless of the possibility that he is leaving or entering the range. Moreover, the researcher also added that, geofence technology by technically, always keep an eye on the functionality and could be performed either appropriate on the cell phone or through some unified plan for instance telecom operator scrutinize the location for own endorser.

Kashif and Wolfgang [12], categorized the context-aware authentication for the Internet of Things as user context. The captured contextual information is based on user location, collection of nearby people, user profiles, and social situation using GPS technology.

As stated by Shraddha *et al.*, [18], location-based authentication is a technique that will take into account the geographical location of the user; which is latitude, longitude of the person who is trying to authenticate his identity.

MAC Address Authentication

A method by Sherer and Nettet [17], for improving network security in a network that configured interconnection device such as a repeater, a bridge or a switch, that has a plurality of ports adapted for connection to respective MAC layer devices includes storing authentication data in the configured interconnection device that maps MAC addresses of end stations in the network to particular ports on the configured interconnection device. Security in the data networks, and more particularly to the authentication of sources of data carrying a medium access control (MAC) layer address as a source address.

According to Gurminder and Baldev [10], MAC address filtering allows a LAN access point to permit or deny network access to clients based on known MAC addresses. MAC addresses have long been used as the singularly unique layer 2 network identifier in LANs. Through controlled, organizationally unique identifiers (OUI) allocated to hardware manufacturers, MAC addresses are globally unique for all LAN-based devices in use today. In many cases, the MAC address of a workstation is used as an authentication factor or as a unique identifier for granting varying levels of network or system privilege to a user.

Biometric Fingerprint Authentication

The measurement of biological data known as biometric which could measure, robust, distinctive, physical characteristic or personal trait of an individual used to verify, or identify themselves [11]. Nowadays, biometrics refer to one's physical authentication such as fingerprints, face and iris recognitions. Traits that can easily detect on sensor and converted into digital format define measureable while robustness define a physical characteristic to significant changes over time which can be measured.

In addition, the variation of biometric patters that can be measured known as distinctiveness. Identification used to identify an individual which device asks and attempt to answer the question "Who is X?" and also known as one to many search. Verification used to claims someone's identity using a password or token which device ask and attempt to answer the question "Is this X?" and also known as one to one search. As advantage, biometric traits cannot be misplaced, forgotten, stolen or forged [3].

Basically, biometrics can measure both physiological and behavioural characteristics. Physical characteristics is measure based on data derived from parts of human body such as fingerprint, face recognition, iris recognition, retina recognition and hand scan. While behavioural characteristics is measure based on data derived from an action such as keystroke, voice and signature scan. Biometric

have several types of recognition such as fingerprint, faces, iris retina, hand geometry, voice and signature [6].

Nowadays, the most widely deployed of biometric technology is fingerprint which valleys on the surface of fingertips and graphical patterns of ridges. The ridges ending and ridge bifurcation is called minutiae [1]. Generally, fingerprint is unique which each person have different pattern of fingerprint. Today, many applications such as ATM machine have been widely adopted [2]. Fingerprint has a high performance in ease of use, processing speed and security. A process to verify the fingerprint image in order to open the electronic lock is highlight the fingerprint verification which the image should be make comparison of data to authorised the fingerprint image.

Authentication Factors

According to Seema, there are varieties of distinctive aspects available to authenticate a particular user. Today's authentication procedures are categorized according to the distinguishing characteristic they use and are classified in terms of three factors described below and summarized in Table 1. Each factor relies on a different kind of discrete feature to authenticate individuals.

- i. Knowledge – something you know:** a password Confidential information is a unique attribute that is known only to genuine users. Even before computers came into existence, this information was shared either through a spoken password or a memorized combination or a lock. But in the computer world, it is a password, a paraphrase, or a PIN.
- ii. Possession – something you have:** a token The unique attribute of “something you have” systems is that legitimate individuals possess some particular thing. Way before computers came in existence; this particular thing was a seal with a private insignia or a key for a lock. But in the computer world it is a device like a smart card, or a magnetic strip card. Such items are called tokens. A token is an object whose features are in some way confidential, and that is difficult to duplicate.
- iii. Inherence – something you are:** a biometric A physical feature or behavior is another distinct aspect, which is exclusive to an individual being authenticated. Before computers, this might have been a personal signature, a portrait, a fingerprint, or a written description of the person's physical appearance. But nowadays, an individual's distinct features are calculated, stored digitally, and compared against an already stored pattern. Precisely, it consists of comparing some easily accessible and reliably distinct physical attribute of a human user against the system's stored values for that attribute. Well known techniques use a person's voice, fingerprints, written signature, hand shape, or eye features for authentication.

Table 1
 Authentication Factors

Factor	Benefits	Weaknesses	Example
Something you know: password	Cheap to implement	Sniffing attacks, cannot detect sniffing attacks. Passwords are either easy to guess or hard to remember, cost of handling forgotten passwords.	Password, PIN, safe combination
Something you have: token	Hardest to abuse	Expensive, can be lost or stolen, risk of hardware failure, not always portable.	Token, smart card, secret data embedded in a file or device, mechanical key
Something you are: biometric	Easiest to authentication with, portable	Expensive, replay threats, privacy risks, characteristic cannot be changed, false rejection of legitimate users, characteristic can be injured.	Fingerprint, eye scan, voice recognition, photo ID

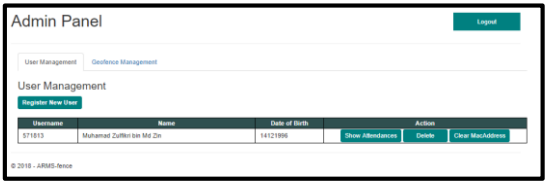
3. Research Methodology

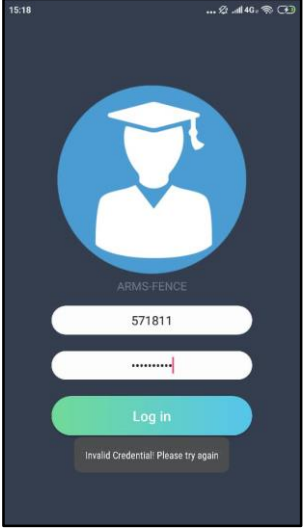
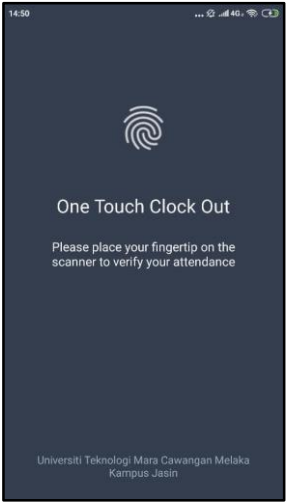
Development of Attendance Record Management System (ARMS) 3. Research Methodology

For the purpose of adapting the multi-factor authentication using the combination factors, ARMS has been developed to verify the flow of the multiple authentication. Table 2 shows the interface for the application. ARMS is a system to record the attendance of staff in an organization by using the following sequences:

- i. Verifying the registered MAC address for a mobile device.
- ii. Authorizing to accessing the application which are either to touches the time-in or time-out.
- iii. Recording the information to the database.

Table 2
 ARMS Interfaces

No	Interface Design	Description
1		Admin page: Registration of new user including personal particulars about the staff. The page also manually registering staff's MAC address of the mobile device. Every staff allowed to register one device only to prevent any misused. If that staff change their mobile device, they have to re-register the new one.

No	Interface Design	Description
1		<p>Login page: Users are not provided with sign in page since the text show to contact the administrator to register manually. The interface allow user to input his/her username which is their staff's ID and password. If success, the application will direct the user to main page of the application. This page is only show one time after installation or after the user logout from the application.</p>
2		<p>Main page: User will be provided with two button which is time-in button and logout button. When the user touches the logout button, the page will be redirect to the login page. If the user touches the time-in button, the user will be redirect to another page which will ask the user to verify their attendance. The text "Time In" will change to "Time Out" after the user has success verify their attendance. For this project, this page only appear between 500 meter radius for the virtual barrier of geofence.</p>
3		<p>Verification page: User will be asking to scan their fingerprint. Fingerprint scanning is to verify the user attendance. If the verification succeed it will redirect the user to main menu page and will automatically store the attendance record in the database. If the biometric scanning failed, it will display error and give chance 4 times before user need to wait 1 minute to continue the verification.</p>

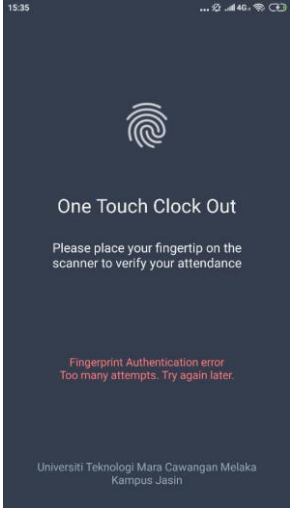

No	Interface Design	Description
		
4		<p>This page is to confirm the recording of the data, either time-in or time-out.</p>

Figure 1 shows the architecture of the system. There are two platforms that that can be use which are the android application and the web application.

- i. Android application can only be use by the staff inside the geofence area as being set inside the admin panel in web application. In order for the user to login to the application, several information will be compared with the data registered inside the database to grant access to the application which are MAC address, username and password.
- ii. Web application is only being use by the administrator. The administrator is responsible to create new user, register the MAC address of mobile device for that particular staff. Other than that, administrator responsible to produce the attendance report based on the requirement requested by the top management for the organization.

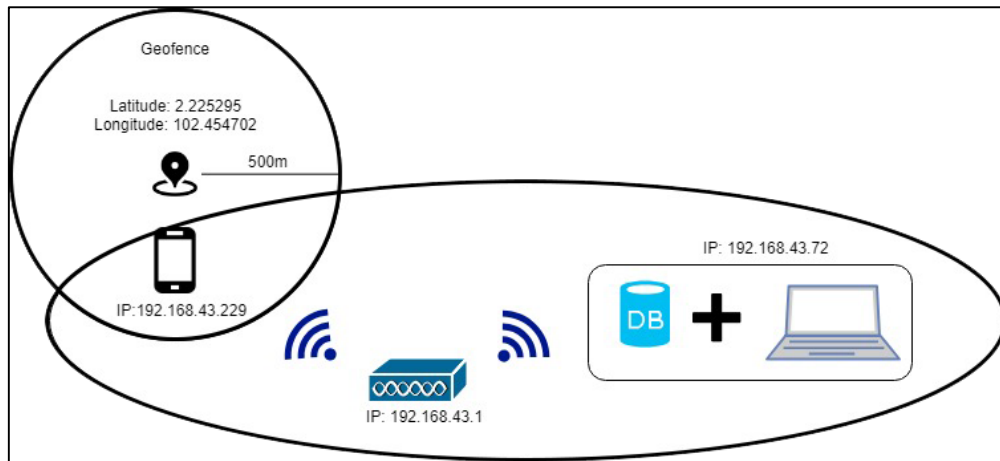


Fig. 1. ARMS System Architecture

Proposed Multi-Factor Authentication Framework

We proposed an authentication framework composed of three phases as summarize in Table 3 to authorizing the access to an application. The three phases of authentication are:

- i. MAC address authentication – ensure the registered device used by the user
- ii. Geofence location-based authentication – ensure the presence of the person at the specific location
- iii. Fingerprint authentication – digitally identify a person to grant access to systems, devices or data.

Table 3
 Multi-factor Authentication

Authentication Factor	Description	Mechanism	Available technologies
Possession	User credentials based on items that the user has with them.	Matching character	PIN, password, passphrase, OTP, MAC address
Location-based	Detection of presence at a distinct location.	Tracking method	Beacon, RFID, geofence , NFC
Inherence	Unique biological characteristics of an individual.	Individual verification	Face, voice, fingerprint , iris

4. Conclusion

In conclusion, multi-factor authentication is an approach to authentication which requires combination of the following factors:

- i. Possession factor
- ii. Location-based factor
- iii. Inherence factor

After submission, each factor must be validated for authentication to in storing data to a system. Multifactor authentication requires several independent credentials: what the user has (MAC address), where the user is (geofence location) and what the user is (biometric verification). With the presence of this framework, it is capable to verify the exact device used by the right person in a specific area, it also ensures the integrity and trust of the received data. This to eliminate the challenge of physical and logical security concerns have converged in the usage of mobile application in IoT.

References

- [1] Ali, Mouad MH, Pravin Yannawar, and A. T. Gaikwad. "Study of edge detection methods based on palmprint lines." In *2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT)*, pp. 1344-1350. IEEE, 2016.
- [2] Allen, R., Sankar, P., & Prabhakar, S. (2011). Fingerprint Identification Technology. *Biometric Systems*, (April 2015), 22–61.
- [3] Hassaballah, M., and Saleh Aly. "Face recognition: challenges, achievements and future directions." *IET Computer Vision* 9, no. 4 (2015): 614-626.
- [4] Mare, Shirang, Mary Baker, and Jeremy Gummesson. "A study of authentication in daily life." In *Twelfth Symposium on Usable Privacy and Security (SOUPS) 2016*, pp. 189-206. 2016.
- [5] Jaros, David, and Radek Kuchta. "New location-based authentication techniques in the access management." In *2010 6th International Conference on Wireless and Mobile Communications*, pp. 426-430. IEEE, 2010.
- [6] de Luis-García, Rodrigo, Carlos Alberola-López, Otman Aghzout, and Juan Ruiz-Alzola. "Biometric identification systems." *Signal Processing* 83, no. 12 (2003): 2539-2557.
- [7] El-hajj, Mohammed, Ahmad Fadlallah, Maroun Chamoun, and Ahmed Serhrouchni. "A survey of internet of things (IoT) Authentication schemes." *Sensors* 19, no. 5 (2019): 1141.
- [8] Zhang, Feng, Aron Kondoro, and Sead Muftic. "Location-based authentication and authorization using smart phones." In *2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications*, pp. 1285-1292. IEEE, 2012.
- [9] Galinina, O., Andreev, S., Balandin, S. and Koucheryavy, Y. (2013). Internet of Things, Smart Spaces, and Next Generation Networks and Systems.
- [10] Singh, Gurminder, and Baldev Krishan. "Wireless access point with fingerprint authentication." U.S. Patent Application 10/965,422, filed May 18, 2006.
- [11] Jaiswal, S., Bhadauria, D. S. S., & Jadon, D. R. S. (2011). Biometric: Case Study. *Journal of Global Research in Computer Science*, 2(10), 19–48.
- [12] Habib, Kashif, and Wolfgang Leister. "Context-aware authentication for the internet of things." In *Elev. Int. Conf. Auton. Auton. Syst. fined*, pp. 134-139. 2015.
- [13] Makhtar, M., Rosly, R., Fadzli, S. A., Shamsuddin, S. N. W., & Jamal, A. A. (2016). Geo-Fence Technique, 11(5), 3391–3395.
- [14] Mello Maia, E. D., Alan Wyatt, S., Hooper Somuah, H., John Saretto, C., & Shane Lynch, D. (2013). *U.S. Patent No. US8618932B2*. Washington, DC: U.S. Patent and Trademark Office.
- [15] Nag, Abhijit Kumar, Dipankar Dasgupta, and Kalyanmoy Deb. "An adaptive approach for active multi-factor authentication." In *9th annual symposium on information assurance (ASIA14)*, p. 39. 2014.
- [16] Kawale, Ajinkya. "Fingerprint based locking system." *International Journal of Scientific & Engineering Research* 4, no. 5 (2013).
- [17] Sherer, W. Paul, and Danny M. Nessett. "Medium access control address authentication." U.S. Patent 6,115,376, issued September 5, 2000.
- [18] Ghogare, Shraddha D., Swati P. Jadhav, Ankita R. Chadha, and Hima C. Patil. "Location based authentication: A new approach towards providing security." *International Journal of Scientific and Research Publications* 2, no. 4 (2012): 1-5.
- [19] Soni, Prachi, and Monali Sahoo. "Multi-factor authentication security framework in cloud computing." *International Journal of Advanced Research in Computer Science and Software Engineering* 5 (2015).
- [20] Cho, YounSun, and Lichun Bao. "Secure access control for location-based applications in WLAN systems." In *2006 IEEE International Conference on Mobile Ad Hoc and Sensor Systems*, pp. 852-857. IEEE, 2006.