Comprehensive-Factor Authentication in Edge Devices in Smart Environments: A Case Study

Chalee Vorakulpipat, Ekkachan Rattanalerdnusorn, Sasakorn Pichetjamroen

National Electronics and Computer Technology Center (NECTEC), Thailand

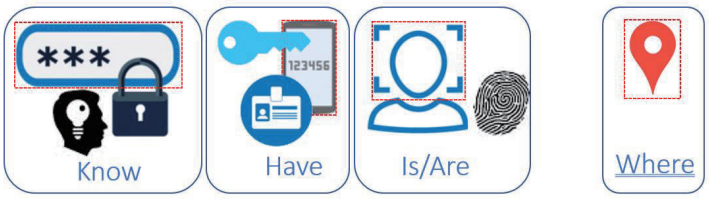
ABSTRACT

The objective of this paper is to introduce a scheme of comprehensive-factor authentication in edge computing, focusing on a case study of time attendance in smart environments. This authentication scheme deploys all possible factors to maximize security while maintaining usability at a specific smart context. The factors used include three classic elements: something you know, something you have, and something you are, plus an additional location factor. The usability issue involves the ability to reduce time used and to minimize the human actions required throughout the authentication process. The results show that all factors should be authenticated at once in background, and a user can successfully complete the authentication process by performing one or two actions simultaneously. Since user role in a smart environment can be more complicated than roles in other smart offices, role classification at an early stage is highly recommended. The case study reveals that the same setting can require varying levels of security and usability for each user.

Keywords—multi-factor authentication, security, usability, smart environment, case study

OBJECTIVES

Multi-factor authentication has been widely used in many information systems to ensure the accuracy of user identity. It is said that the more factors taken into account, the more accurate the results. However, in real use, deploying too many factors can cause difficulty of use such as increased time and cost. Our proposed **"Comprehensive-factor authentication"** is defined as an authentication method that uses all possible factors while maintaining real-world usability. The study demonstrates a case of a mobile-based time attendance system in a smart office using four factors, including password, MAC address, biometric data (facial data), and location. An employee can use a mobile phone (Bring-Your-Own-Device: BYOD) to check in at any area in the office, using all four authenticating factors in a few seconds. This method promotes both security and ease of use. However, the use of mobile-based system may not be applied in all smart environments due to some restrictions.



User Identification Methods

COMPREHENSIVE-FACTOR AUTHENTICATION

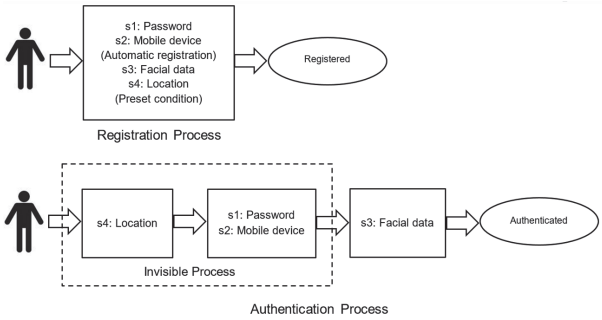
This section proposes a comprehensive-factor authentication scheme designed for smart environments that have unique characteristics. The comprehensive-factor approach contains all possible or necessary factors, while low effort in terms of ease of use, time consumed, and seamlessness must be taken into account. In cases where the system is BYOD-based, the factors should include login/password from Lightweight Directory Access Protocol (LDAP) (from personnel database), MAC address of mobile phone, facial data for face verification, and location from GPS or a WiFi locator. All of these factors must be authenticated seamlessly, allowing a user to finish check-in in a few seconds without too much effort.

Comprehensive-Factor Authentication in a Time Attendance System

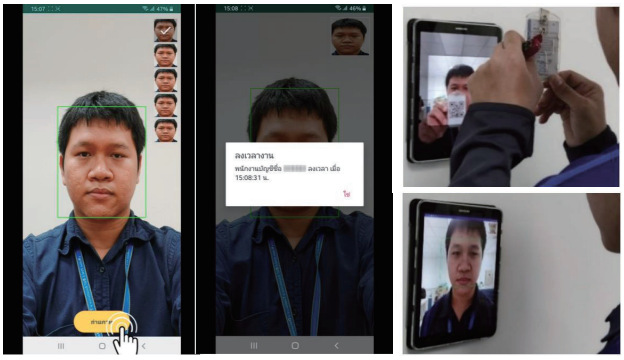
EXPERIMENTS

The proposed scheme is divided into two processes:

- **Registration:** A user registers all the factors including password (from LDAP or Active Directory), mobile device (IMEI/MAC-automatic registration), facial data (for face verification), and location (GPS/WiFi locator-preset condition)
- **Authentication:** A user uses a mobile device to check-in/check-out. All four factors registered above are authenticated in a few seconds.



Registration and Authentication



Screenshots

Factors/Attributes	Results
Something you know (Username/Password)	100% Accurate (similar to our existing Intranet system)
Something you have (Device)	100% Accurate (once a device is registered, other user cannot use the registered device on behalf)
Something you are (Face verification)	98% Accurate (two persons who are twin cannot be differentiated)
Somewhere you are (Location)	100% Accurate (employees who are outside the desired area including a location outside the technology park, not on the desired floor at the desired building and through VPN)
Average time used to check-in	Less than two seconds
Attempt for spoofing	Attempt for spoofing is possible, and it depends on the security strength of each factor. In our experiment, MAC spoofing be done in general as mentioned earlier. However, the hacker does not know the target's MAC unless it is willingly given by the targeted user. However, the hacker still needs to acquire the target's identity of the other factors, and has to borrow the target's device. In this scenario using BYOD, people today feel reluctant to lend their own mobile device, even for a short time.

Results

REFERENCES

1. Vorakulpipat, C., Pichetjamroen, S., & Rattanalerdnusorn, E. (2021). Usable comprehensive-factor authentication for a secure time attendance system. *PeerJ Computer Science, 7*, e678.
2. Zhang, T., Yang, L., & Wu, Y. (2019). Evaluation of the Multifactor Authentication Technique for mobile applications. In *Intelligent Computing-Proceedings of the Computing Conference* (pp. 696-707). Springer.
3. Wang, R., Madden, K., & Wang, C. (2022). Low-effort user authentication for kiosk systems based on smartphone user's gripping hand geometry. In *CHI Conference on Human Factors in Computing Systems*.
4. *Chalee Vorakulpipat, Ekkachan Rattanalerdnusorn, "Evolutionary Consideration on User Authentication: Security, Privacy and Safety", IEEE IT Professional, 23(5), 38-43, 2021.*

ACKNOWLEDGEMENTS

This work is the output of ASEAN IVO project (https://www.nict.go.jp/en/asean_ivo/index.html) entitled "Agricultural IoT Based on Edge Computing", and financially supported by NICT (http://www.nict.go.jp/en/index.html).