

A Secure Four-factor Attendance System for Smartphone Device

Tinthid Jaikla*, Sasakorn Pichetjamroen*, Chalee Vorakulpipat*, Achara Pichetjamroen**

*National Electronics and Computer Technology Center, Pathumthani, Thailand

** Department of Electrical Engineering, Faculty of Engineering, Kasetsart University, Bangkok, Thailand

tinthidj@gmail.com, sasakorn.pichetjamroen@nectec.or.th, chalee.vor@nectec.or.th, fengaap@ku.ac.th

Abstract—A time attendance system is implemented in many organizations to track the attendance or presence of employees and reduce employee absence. Most attendance systems use a one-factor authentication method such as RFID tags or fingerprints. However, the limited number of authentication factors causes security issues with these attendance systems. Although multi-factor attendance systems have been presented to solve this problem, their usability has not been satisfactory. This paper introduces a four-factor attendance authentication system that uses smartphones. The proposed system uses fingerprints, mac addresses, wireless networks, and face images as authentication factors, which can improve the security of the attendance system. Moreover, the process for the proposed system can increase the system usability.

Keywords—four-factor authentication, attendance system, security, usability, smartphone, face recognition, wireless network

I. INTRODUCTION

In many organizations, a time attendance system is used to reduce employee absenteeism in the workplace. Most traditional attendance systems use a smart card-based method to authenticate employees, such as RFID. However, a smart card-based method is a one-factor authentication. Other people can easily use the employee's card to check-in. Therefore, the employee can check-in to work without entering the workplace. Biometric authentication has been presented to solve this problem, in which employees are required to scan their fingerprint at the attendance hardware. However, fingerprint scanning requires time to read the employee's finger and match the fingerprint to identify the employee. This process can create a long queue. Employees will waste time waiting for others to complete the attendance process [1–3].

A multi-factor attendance system can be used to solve the security issues of one-factor attendance authentication systems. However, this security improvement usually decreases the usability. For example, with a multi-factor attendance system that uses attendance hardware, employees need to enter a password, scan an RFID tag, and then scan their fingerprint. This process is more secure than using a single RFID tag or fingerprint. However, it is not practical in real-world use cases. Therefore, system usability needs to be considered while improving system security.

This paper proposes a four-factor attendance system that uses smartphones to improve the attendance authentication security. Moreover, the usability is not decreased by this method.

II. RELATED STUDIES

Various related studies have been conducted to make an attendance system work securely and efficiently using more than one factor in the attendance process. One study [4] used fingerprint and RFID techniques to record the attendance times of students. However, attendance hardware was still used in the attendance process, which required a hardware installation cost and maintenance cost. There is a need to improve the usability of this system because students need to queue up in front of the RFID reader and fingerprint reader. Another study [5] presented a multi-factor attendance authentication system based on smartphone capabilities. Fingerprints, secure Android IDs, and GPS coordinates were used in the authentication process. An anti-fake location module was implemented to prevent the use of a fake GPS location. Moreover, this system implemented an anti-emulator module to prevent the use of a fake device. Furthermore, other researchers [6] also used a smartphone's mac address as an employee smart id. The employee's fingerprint was used as biometric data, but their system used a wireless network to determine whether employees were in the building instead of using GPS.

Based on these studies, fingerprints are the most commonly used biometric data in authentication attendance systems. The trend of using BYOD (Bring Your Own Device) for identification is increasing. However, smartphones do not have the same hardware and capabilities for implementing the same authentication method. For example, some smartphones do not contain a fingerprint sensor. Therefore, the use of a smartphone's capability in an attendance system should be addressed. Moreover, the implementation requirements of the attendance system also need to be considered. The implementation cost depends on the number of requirements.

III. PROPOSED SYSTEM

A. Attendance Factor

Most organizations have their own intranet network that is accessible only to their employees; therefore, we can use the intranet username and password from the organization's database (e.g., LDAP, Active Directory) as a "what you know" factor. Employees do not need to

remember an additional password or PIN to use in the attendance system. Thus, an organization can save the cost of implementing a new password authentication system for its attendance system.

Typically, RFID tags are used in an attendance system. However, this requires additional hardware such as an RFID reader. When using an RFID attendance system, the organization needs to consider the costs that occur, such as the maintenance cost, installation cost, and tag cost. Therefore, we attempted to find something that everybody has to reduce the operation cost. A smartphone was our choice because smartphones are part of our daily life, and everybody has a smartphone. Moreover, we can use a smartphone's mac address as a unique identifier so that the smartphone can be used as a "what you have" factor.

In addition to using the smartphone as a "what you have" factor, we can use a smartphone to scan biometric data such as a fingerprint or iris. However, in any given organization, we cannot expect everybody's smartphones to have security modules like a fingerprint scanner and iris scanner. For example, some budget smartphones do not provide a fingerprint sensor. For this reason, a method must be implemented that can work in everybody's smartphone. Therefore, we decided to implement face recognition because every smartphone has a camera. The face recognition can achieve the "what you are" factor.

Lastly, for the "where you are" factor, GPS is widely used to determine a smartphone's location. However, GPS is not designed to find elevation data. Therefore, the GPS cannot determine the smartphone's floor location when we are in a tall building. Unfortunately, many companies are located on a designated floor with limited space. For example, an organization may be located on the 10th floor. An employee can perform an attendance action from the 1st floor if the attendance system uses the GPS system as a location service. Because of this problem, we decided to use a networking device to determine the employee location. Employees are required to connect their smartphones to the organization's network. The attendance system knows the employee's location and floor by collecting information from the networking devices.

B. System Design and Implementation

This attendance system was implemented at NECTEC (National Electronics and Computer Technology Center), Thailand. The attendance server was installed in the organization's intranet network. The attendance server will obtain user information from the organization's network to use in the user's credential validation. The database is used to store the mac address of an employee's smartphone and the employee's face. To recognize the employee's face, a deep learning module is implemented. The employee's face will be collected separately from those of other employees. We can separate the employee's face using their employee id from the organization's management system. Therefore, one-to-one face verification can be used to verify the employee's face.

The attendance application was developed for Android devices. The employees are required to connect to the organization's network to use the application. The application will send the employee information (mac

address, face image) to the attendance server. Figure 1 shows the system design of the proposed system.

C. Attendance Process

The attendance authentication process is an important part of the attendance system. Increasing the factors in the authentication process can increase the gap between system security and usability. Poor process management will decrease the system usability. The proposed system was designed to simultaneously improve the system security and usability. Employees only use their smartphone to perform an attendance action. This attendance system consists of two processes: the registration process and authentication process.

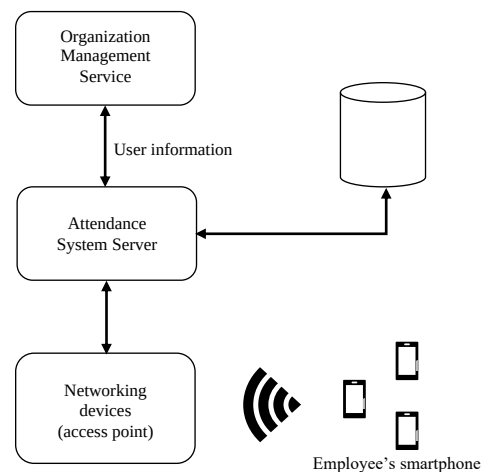


Figure 1: System Architecture

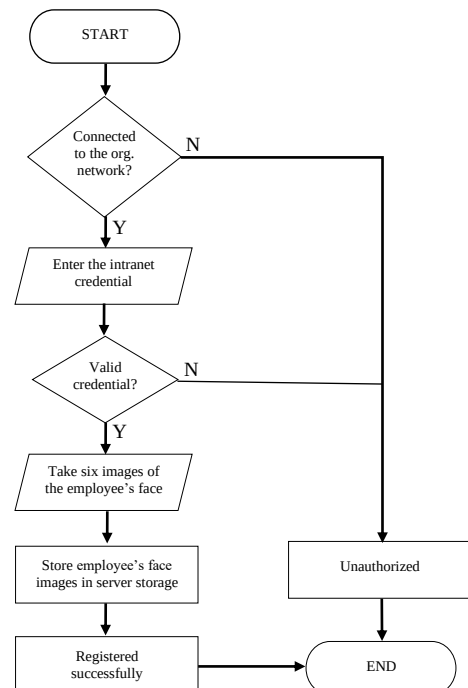


Figure 2: Registration Process

In the registration process, the employee is first required to connect to the organization's network. Then, the employee needs to enter their username/password to access the attendance application. The application will send the credential information to the attendance server for validation. After the employee accesses the application, they are required to register their face in the system. Each employee must take six photos of their face. The employee's face images will be stored in the database using the employee id as the identify key. These photos will be used as biometric data to verify the employee's identity. A flowchart of the registration process is shown in Figure 2.

The authentication process confirms the identity of the employee before check-in to the organization. Because this is a multi-step process, the employee should be able to perform these steps as easily as possible. First, the employee must connect their smartphone to the organization's intranet network to confirm their location. We can then determine which floor the employee is on, or the building in a case where the organization has multiple buildings. By using the wireless network to determine the location, the security is improved, because the employees can only connect to the network when they are in the area of the wireless signal. Therefore, a fake location is prevented. Second, the username/password for the organization's intranet is required in the authentication process. This will be the second authentication factor after the location factor is confirmed. Employees can choose to save their log-in session for the next time they use the application. This will increase the usability for the authentication process because entering their username and password every time they use the application is a waste of time. If the username and password are invalid, the employee cannot perform the check-in/check-out function. After the employee successfully logs in to the application using their intranet credential, they can perform a check-in/check-out function. To perform these actions, the application will open the smartphone's front camera and take a photo of the employee's face to compare with the employee's face photos in the attendance server. The mac address of the smartphone is also sent to the attendance server to check the "ownership" factor. After these four factors are validated, the employee will be able to successfully check-in and check-out. Figure 3 shows the registration process of the proposed system.

IV. DISCUSSION

The four-factor attendance system discussed here was designed to increase an attendance system's security. The use of a wireless network allows an employee to check-in from anywhere in the organization's area. Moreover, the attendance system can accurately determine which floor the employee is on. The use of a smartphone's front camera for face verification solved the smartphone limitation problem of using a fingerprint as an authentication factor. Table 1 shows the difference in authentication factors between the proposed system and related systems.

A comparison between a related system that use multi-factor attendance authentication and the proposed system that uses four-factor authentication is given in Table 2.

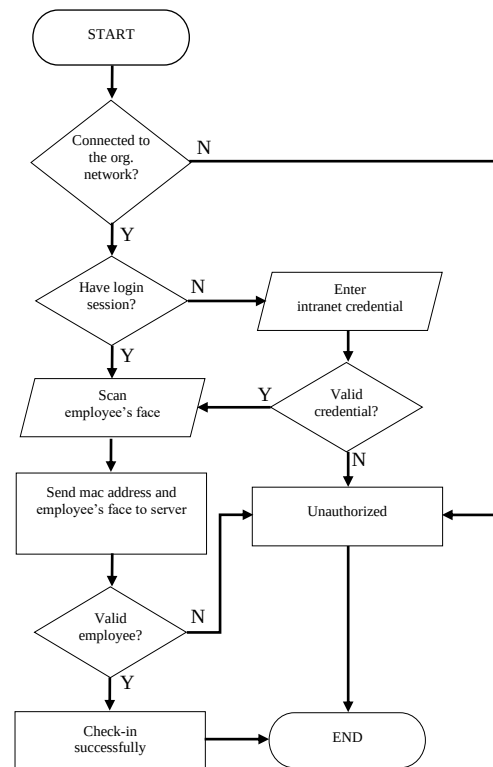


Figure 3: Authentication Process

TABLE I. COMPARISON OF AUTHENTICATION FACTORS BETWEEN RELATED WORKS AND PROPOSED SYSTEM

Factor Method	Knowledge	Ownership	Biometric	Location
[4]	-	RFID	Fingerprint	-
[5]	-	Smartphone (Android ID)	Fingerprint	GPS
[6]	-	Smartphone (Mac address)	Fingerprint	Wireless Network
Proposed System	Intranet password	Smartphone (Mac address)	Face recognize	Wireless network

TABLE II. COMPARISON OF EXISTING SYSTEM AND PROPOSED SYSTEM

Requirement	Existing System	Proposed System	Description
Able to use in all smartphone devices	✗	✓	Every smartphone has front camera
Able to determine the building floor of attendance employee	✗	✓	Use access point location
Has more than three factors	✗	✓	-
Reduce implementation cost	✗	✓	Integrate with existing organization intranet

V. CONCLUSION AND FURTHER WORK

This proposed system can be used to perform an attendance process securely. The system can provide important security factors such as “what you have,” “what you know,” “what you are,” and “where you are.” The organization can confidently trust an attendance employee’s identity. The proposed system can be easily implemented in an existing organization’s network. The attendance application increases the usability of the system. However, today, face recognition systems are vulnerable to fake face attacks (spoofed faces). An interactive method is proposed to avoid fooling the system using fake facial data such as photos and 3D-printed face masks. Encrypting the data during storage and transmission is still important to preserve confidentiality. Furthermore, edge computing can reduce server resource consumption. An employee’s face can be stored in the secure storage of the device, and then the recognition process can be performed in the device. Also, this four-factor system could be integrated to others application such as the forecasting, distributed learning and optimization data in the aspects of electricity markets included various types of renewable energy resources and lithium-ion battery [7]. The high security for all data communication is necessary to avoid cyber-attack and operation failure.

REFERENCES

- [1] T. S. Lim, S. C. Sim, and M. M. Mansor, “RFID based attendance system,” *2009 IEEE Symp. Ind. Electron. Appl. ISIEA 2009 - Proc.*, vol. 2, no. Isiea, pp. 778–782, 2009.
- [2] M. Kassim, H. Mazlan, N. Zaini, and M. K. Salleh, “Web-based student attendance system using RFID technology,” *Proc. - 2012 IEEE Control Syst. Grad. Res. Colloquium, ICSGRC 2012*, no. Icsgrc, pp. 213–218, 2012.
- [3] O. Shoewu, A. Idowu, “Development of attendance management system using biometrics,” *The Pacific Journal of Science and Technology*, vol. 13, no. 1, pp. 300–307, 2012.
- [4] A. Ahmed, O. M. Olaniyi, J. G. Kolo, and C. Durugo, “A multifactor student attendance management system using fingerprint biometrics and RFID techniques,” *CEUR Workshop Proc.*, vol. 1830, no. December, pp. 69–74, 2016.
- [5] S. B. Utomo and B. Hendradjaya, “Multifactor authentication on mobile secure attendance system,” *Proceeding - 2018 Int. Conf. ICT Smart Soc. Innov. Towar. Smart Soc. Soc. 5.0, ICISS 2018*, pp. 1–5, 2018.
- [6] H. Adal, N. Promy, S. Srabanti and M. Rahman, “Android based advanced attendance vigilance system using wireless network with fusion of bio-metric fingerprint authentication,” *2018 20th International Conference on Advanced Communication Technology (ICACT)*, Chuncheon-si Gangwon-do, Korea (South), 2018, pp. 1-2.
- [7] Somakettarin, N. and Pichetjamroen A., “Characterization of a Practical-Based Ohmic Series Resistance Model under Life-Cycle Changes for a Lithium-Ion Battery” *Energies*, vol. 12 no.3888, 2019.



Tinthid Jaikla received his Bachelor's Degree in Computer Engineering from Chiang Mai University, Thailand in 2015. He works as a research assistant at National Electronics and Computer Technology Center (NECTEC). He is currently studying MSc Cyber Security at the University of Southampton, United Kingdom. He is interested in network security, web application security, cloud computing and distributed computing.



Sasakorn Pichetjamroen received M.S. and B.S. degrees in computer engineering from King Mongkut's Institute of Technology Ladkrabang. She is currently a research assistant at the National Electronics and Computer Technology Center (NECTEC), Thailand. She has been involved in several projects in information security and particularly AI and Image Processing. Her current research focuses biometrics for security.



Chalee Vorakulpipat received his PhD in information systems from the University of Salford, UK. He is currently the head of Information Security Research Team at the National Electronics and Computer Technology Center (NECTEC), Thailand. He has been involved in several projects in information security (including ThaiCERT), national e-science, mobile device management, social networking, context-aware computing, e-health, and mobile application development. He has over fifty refereed publications in these areas. He also serves as a subcommittee member on issues regarding national information security of Thailand. He holds professional certificates including CISSP, CISA, PMP, and IRCA (ISMS Lead Auditor).



Achara Pichetjamroen received the B.S. (1st class honors) and M.S. degrees in Electrical Engineering from King Mongkut's Institute of Technology Ladkrabang (KMUTL), Thailand in 2007, and the Ph.D. degree from Osaka University, Japan in 2009. She is now a lecturer at Kasetsart University, Thailand. Her research interests include Smart grid technologies, electrical transmission system, power electronics and battery management system.