iAttend: Secured Fingerprint Attendance System in the Cloud

Fahad Alsolami

Department of Information Technology
King Abdulaziz University, KSA

Summary
Private organizations and government offices have become more reliant on technology, particularly with employee attendance systems that result in a consistent and an efficient work environment. Recently, many private organizations and government offices use biometric authentication for their attendance monitoring systems. This increase the risk of these systems experiencing cybersecurity attacks, especially if the biometric authentication performs on raw data. Another problem arises when private organization and government offices deploy the attendance monitoring system locally, even though these systems require scalable computation and storage. This requirement results in the best recommendation being to deploy the attendance systems in the cloud, which have scalable computing along with low cost and ease of use. These challenges motivate our proposal: the iAttend scheme. iAttend scheme uses cloud computing, Bipartite token, and secret sharing scheme to introduce a secured fingerprint attendance system that monitors and manages employee attendance in private organizations and government offices. The iAttend scheme hides an employee's ID and share of every day attendance inside an encoded fingerprint. Then iAttend scheme distributes these shares over multiple clouds. Each day, to validate attendance, an employee provides his/her fingerprint data for authentication using encoded fingerprint data. If it is authenticated, iAttend scheme releases one share of the employee's attendance with his/her ID. This share proves employee attendance and is saved in the employee's record with employee's ID. Finally, at the end of the payment round, in this case assumed to be a month, the iAttend scheme calculates all shares to compute the total attendance record of each employee for the month.

Key words:
Attendance, Cloud, iAttend, biometric authentication

1. Introduction

With the spread of many government offices, private companies, and startup companies, management and control of the workstation environment is a challenge. Many papers in literature discuss how to manage and control the work environment. First, work attendance is found to be influenced by motivation and work abilities [1]. Second, self-management has a positive effect on employee attendance [2]. Other studies examine the relationship between stressful job demands and attendance, finding that there is an interaction between control and physical demands [3]. Also, the relationship between organization politics and employee attendance is important and should be considered [5]. Finally, applying flexible scheduling programs for employees reduces absenteeism [4]. Even though the above models and suggestions improve work efficiency, they do not close the gap to resolve the problem. To work on fully addressing the gap, many electronic monitoring systems have been proposed such as electronic system and biometric system.

Recently, many private organizations and government offices rely on technology such as attendance monitoring system or biometric authentication to improve work efficiency. Card identification is used as an attendance monitoring system to allow a user to register attendance time and to allow additional information to be saved [8]. Another electronic attendance system to manage the employee attendance time is a radio-frequency identification (RFID) system [10]. This RFID reader is connected to a central computer that controls all activities. Additionally, biometric data is used for employee attendance authentication. Fingerprint data is integrated with access control for identification and attendance [13]. Iris recognition is proposed for a wireless attendance system [12]. Also, face recognition is presented as a quick and convenient method for tracking student attendance in classrooms. Some of the attendance system use biometrics to improve the authentication, but this has put these systems under greater threat of cybersecurity attacks, especially if the biometric authentication performs on raw data as biometric data are targeted for compromising issues in terms of privacy and security [20].

To overcome the obstacles of both cybersecurity attacks against biometric data and unscalable local storage, we propose the iAttend scheme. The iAttend scheme is a secured cloud-based fingerprint attendance system designed for managing the employee attendance that ensures high security and privacy. In the enrollment process, iAttend scheme transforms an employee fingerprint image to an encoded form using the revocable fingerprint biotokens (Biotope) [21]. Then, iAttend scheme uses a secret sharing scheme [23] to split the attendance secret into multiple shares where each share represents each day's attendance. iAttend scheme hides each share of attendance with the employee's ID inside encoded fingerprint data using a Bipartite token [22]. Finally, iAttend scheme distributes all shares of a secret into multiple clouds so that no single cloud stores the threshold of shares required to reconstruct the secret. During the

Manuscript received November 5, 2018
Manuscript revised November 20, 2018

matching/attendance process, iAttend scheme requires each employee to provide his/her fingerprint data daily. If authentication is successful, iAttend scheme releases the share of a secret with the employee's ID and saves them in the employee's record in an encrypted mode. At the end of the month, iAttend scheme calculates all shares, computes the secret, and counts all number of days to send this information to the financial department for payroll processing. In sum, these processes are conducted in encoded mode to provide security and privacy for the fingerprint data and for the underlying information (attendance shares). Moreover, iAttend uses threading to speed up these processes, allowing for significant performance gains when compared to the two baselines.
The rest of this paper is organized as follows: in section 2, we briefly describe previous related work. The objectives of iAttend are given in section 3. Our proposed iAttend algorithm is presented in section 4. In section 5, the description of the experimental design is given. The experimental evaluation and results are provided in section 6. Finally, the conclusion is drawn in section 7.

2. Background

2.1 Using Electronic Attendance System for Employee Attendance

To improve the efficiency of the daily work in private organizations and government offices, many use electronic systems, such as an identification card system. These systems are intensively studied in literature. Jones et al [7] invents an attendance monitoring system that provides daily attendance, attendance history, vacation schedules, and responsibilities. Their system has advantages such as attendance awareness, staff reliability, and the ability to support the needed number of employees. Bennett [8] invents a system for registering the time attendance of employees. Also, while a user uses an identification card, and the system records a video during the bar code scanning. Additionally, the system allows a user to input additional information and save it. Chalker et al [9] proposes a system to automate attendance time for employees that is connected to a central processor to determine the payroll system. Meanwhile, radio-frequency identification (RFID) systems have been introduced to monitor employee attendance; Chiagozie et al [10] proposes an RFID system to manage employee attendance time. This RFID reader is connected to a central computer that controls all activities. In addition, Singhal et al [14] proposes an attendance system that uses FRID and GSM network for a safe, secure, and easy approach. Finally, Bhalla et al [11] presents a software application installed in the teacher's smartphone that can connect to students' smart phones using the Bluetooth. This allows a present student to send his/her MAC address to the teacher's smartphone for attendance confirmation.

2.2 Using Biometric in Employee Attendance System

To improve authentication in attendance systems, many private organizations and government offices use biometric data. Biometric data have been discussed in literature as a highly effective authentication tool. Rao et al [6] proposes an attendance monitoring system based on fingerprint authentication. They use a minutia points technique for fingerprint verification. Second, Roy et al [13] invents a biometric access control where the system takes a fingerprint from a user and identifies it against database. Third, Akinduyite et al [18] presents a fingerprint authentication system to administrate employee attendance to improve the workplace environment. Finally, Olagunju et al [19] proposes a fingerprint monitoring system for employee attendance. Kadry et al [12] proposes a wireless attendance system based on iris recognition which uses Daugman's algorithm. Kar et al [16] presents a face recognition system for students' attendance where the system integrates face recognition technology with personal component analysis. Each time a student enters, the system does face recognition and saves the entry time. The system has a log for clock entry and clock exit time.

3. The iAttend Objectives

The main goal of iAttend scheme is to introduce a secure fingerprint attendance system in the cloud. In this section, we explore the objectives of iAttend scheme in terms of authentication, security and privacy, and scalability and performance.

3.1 Authentication Objective

Since biometric data is considered a highly effective authentication tool, iAttend scheme uses fingerprint data for authentication. The iAttend scheme requires each employee to enroll his/her fingerprint data with his/her ID. Each day, an employee provides his/her fingerprint data to log his/her attendance. If the authentication is successful, iAttend scheme confirms that the person who provides his/her fingerprint is the right person. Thus, iAttend scheme verifies each employee authentication.

3.2 Security and Privacy

Security and privacy are the most important objectives, not only for private organizations and government offices, but also for users and employees. Therefore, iAttend scheme does not use raw fingerprint data for authentication; all authentication processes are performed over encoding fingerprint data. For the daily attendance process, iAttend

uses revocable fingerprint biotoken (Biotope) [21] to authenticate over the encoded form. Moreover, iAttend uses a sharing secret scheme [23] to encrypt the daily attendance share and hide it inside the encrypted fingerprint data using bipartite tokens [22]. In sum, these technologies are applied in the core algorithm of iAttend scheme to provide the highest security and privacy, not only for attendance system for organizations, but also for users/employees themselves.

3.3 Scalability and Performance

Since the iAttend scheme relies on fingerprint data for authentication and secret sharing scheme [23] to generate a daily attendance secret, iAttend scheme uses cloud computing and storage for scalability to compute and store the big data it relies on. Additionally, iAttend scheme uses threading to match and process the daily attendance in parallel to achieve a significant performance gain.

4. Design of iAttend Scheme Algorithm

In this section, we show the details architecture of iAttend scheme for both enrollment and matching operation

4.1 Enrollment Operation

To create a gallery fingerprint database iAttend scheme first takes a fingerprint image from each employee. Second, iAttend scheme applies the NIST Bozorth matcher algorithm [24] to create the minutia points, minutia point files, and pair-table. Third, iAttend scheme uses the revocable fingerprint biotokens (Biotope) [21] to encrypt the fingerprint data (pair-table). Then, iAttend scheme creates a secret (user ID) for each employee and uses a secret sharing scheme [23] to split the secret into multiple shares where the total shares are equal to the total days in a month. iAttend scheme hides each share of a secret inside the encrypted fingerprint data of employee using a Bipartite token [22] where we have a biotoken for each share equal to the total days in each month. Indeed, iAttend scheme creates a secret for each month and splits this secret into multiple shares equal to the total days in a month. Finally, iAttend scheme distributes all biotoken shares of each month over multiple clouds so each cloud does not store the threshold shares needed for recovery. For the next month, iAttend scheme creates a new biotoken for each employee without taking his/her fingerprint data again. Figure 1 shows the details of enrollment operation.

4.2 Matching Operation

During the matching operation, which occurs when daily attendance is submitted, each employee must provide his/her fingerprint data. First, iAttend scheme takes the employee fingerprint image and follow the steps as in enrollment process. iAttend schemes creates the minutia points, minutia point files, and the pair-table. Second, iAttend scheme converts the plain text pair-table into an encrypted form by applying revocable fingerprint biotokens (Biotope) [21]. Then, iAttend scheme matches the encrypted probe fingerprint data (pair-table) against one share of a gallery encrypted fingerprint already stored in the cloud. If there is a true match, iAttend scheme confirms the attendance time for the employee by releasing the attendance share of the day and storing it in the employee's record. iAttend scheme

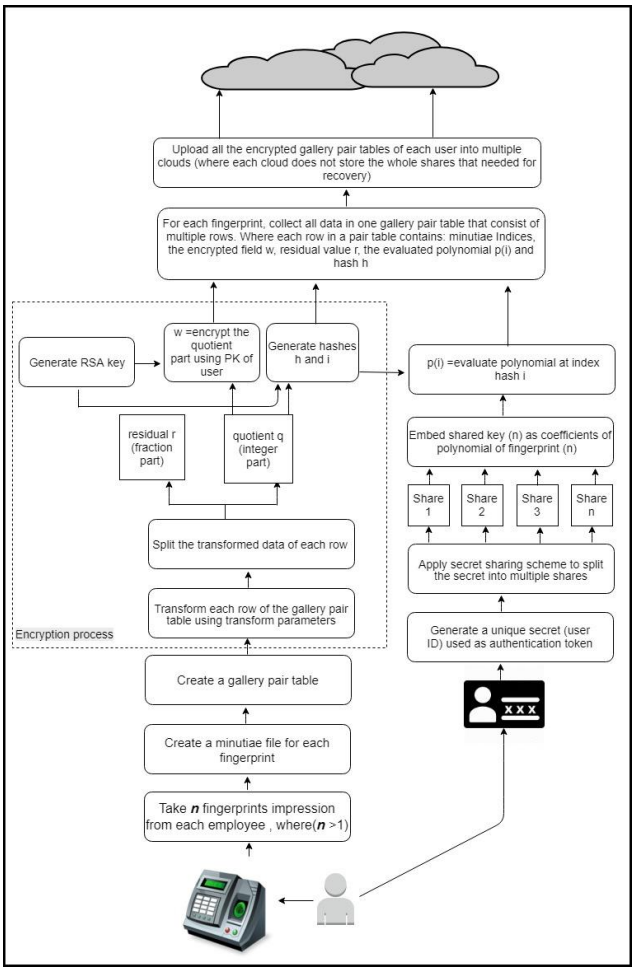

Fig. 1 Enrollment operation of iAttend scheme

does this process each day when an employee submits his/her attendance. iAttend scheme performs this process in an encrypted form and in parallel. Finally, at the end of the month, iAttend scheme applies a secret sharing scheme [23] to compute all shares, to obtain the secret, and to count days of employee attendance. iAttend scheme sends this information to the financial department to execute the

employee's payroll for the month. Figure 2 shows the details of matching operation.

5. Experiment Design

Our experiment is designed to have a real-life employees' attendance scenario, as seen in a private organization or a government office, where each employee must sign daily for the whole month to prove his/her attendance. We create a secret for each month and for each employee where we split this secret into multiple shares equal to the total days in each month. For each day, successful attendance means one share is released and stored in the employee's record. At the end of the month, our scheme computes the whole shares to get the secret, which contains the counter of how many days in the month required employee attendance. We use the AWS Amazon clouds for our experiment using eight clouds: North California, North Virginia, Ohio, Paris, London, Ireland, Sydney, and Tokyo. For this experiment, during the enrollment operation, iAttend scheme uses the fingerprint dataset (FV C2002Db2 a) [25]. Then, iAttend scheme uses the programming languages C++ and Python to upload the gallery fingerprint data in the cloud. The uploading operation happens in parallel by utilizing threading. To match probe fingerprint data against those gallery stores in the cloud, iAttend scheme connects Amazon Web Server S3 with Amazon Web Server EC2 instance using the Python boto library. We run our experiment twenty times and compare our results with the two baselines Bipartite Biotoken algorithm [22] and Cloud-ID-Screen [26]. We compare our scheme to the Bipartite Biotoken algorithm [22] because we use the same encryption algorithm. Additionally, we compare our scheme to Cloud-ID-Screen [26] because they use the AWS clouds for their experiment.

6. Experimental Evaluation

We aim to prove that if we encrypt, hide, and distribute the attendance secret of all employees among the total days of a month, we can use threading for parallel fingerprint matchin to have significant performance while getting comparable accuracy comparing to the two baselines. Our null hypothesis Ho is that the two baselines are better than iAttend scheme in performance (matching time) and in accuracy.

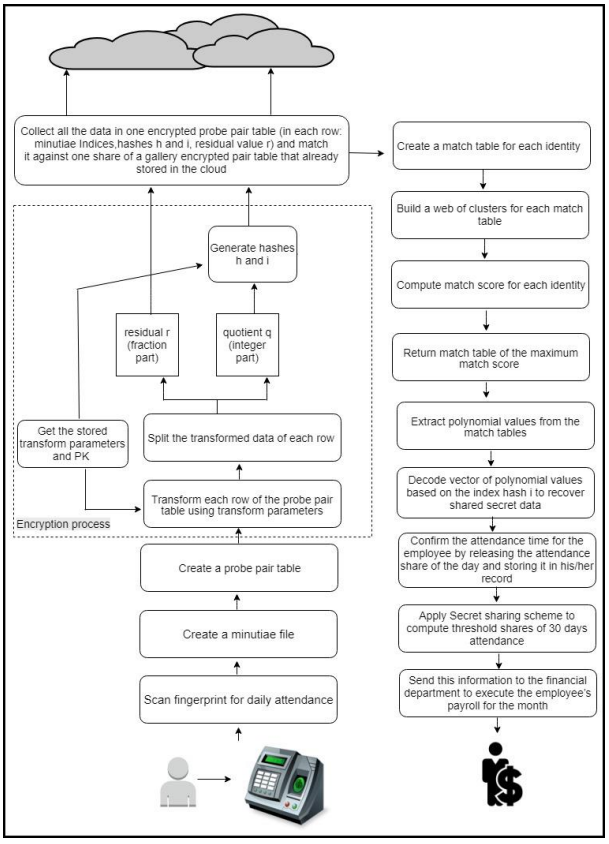

Fig. 2 Matching operation of iAttend scheme

6.1 Accuracy Experiment

As an accuracy experiment, we run our experiment (N:N) to evaluate the false accept rate (FAR) and the genuine accept rate (GAR) for our scheme iAttend and both baselines Bipartite Biotoken algorithm [22] and Cloud-ID-Screen [26]. We then compare the results from our scheme and both baselines to check if these result reject the null hypothesis and prove our claim. Figure 3 shows the ROC curve demonstrates where our iAttend scheme achieves a comparable accuracy with a GAR equal to 97 and FAR equal to 0. This promising result rejects the null hypothesis and proves our claim.

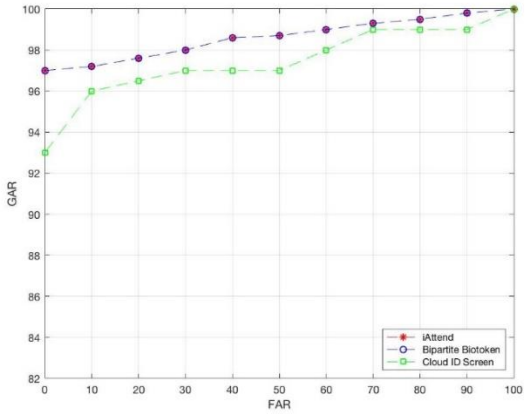

Fig. 3 The ROC curve shows the accuracy between three schemes: iAttend, Bipartite Biotoken and Cloud-ID-Screen.

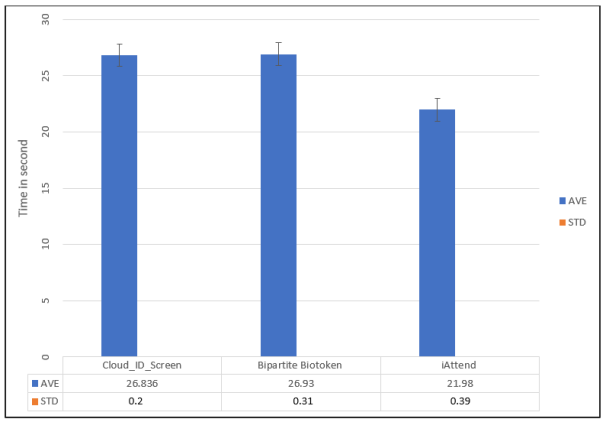

Fig. 4 The speed result comparing the performance of iAttend scheme against the two baselines

6.2 Performance Experiment

As a performance experiment, we run (1:N) experiment to evaluate the matching time speed for iAttend scheme and both baselines Bipartite Biotoken algorithm [22] and Cloud-ID-Screen [26]. Then, we compare the matching time processing between our scheme and both baselines. The matching time operation shows that the iAttend scheme achieves a significant improvement over the two baselines. This promising result rejects the null hypothesis H0 and proves our claim that the iAttend scheme matching time is faster than the two baselines.

7. Conclusion

This paper introduces iAttend scheme as a daily attendance system for private organizations and government offices. The iAttend scheme is a cloud-based system that uses the revocable fingerprint biotoken, Bipartite Biotoken algorithm, and secret sharing scheme. Thus, iAttend scheme provides scalability to process big data in the cloud. Moreover, iAttend scheme provides security and privacy by performing all attendance processing over encrypted form. For future work, we are going to deploy our scheme over smart devices platforms to increase convenience and usability.

References

[1] R. M. . Steers and S. R. Rhodes, “Major influences on employee attendance: A process model.,” Journal of applied Psychology, vol. 63, no. 4, p. 391, 1978.

[2] C. A. . Frayne and G. P. Latham, “Application of social learning theory to employee self-management of attendance.,” Journal of applied psychology, vol. 72, no. 3, p. 387, 1987.

[3] D. J. . Dwyer and D. C. Ganster, “The effects of job demands and control on employee attendance and satisfaction.,” Journal of Organizational Behavior, vol. 12, no. 7, pp. 595–608, 1991.

[4] D. R. . Dalton and D. J. Mesch, “The impact of flexible scheduling on employee attendance and turnover.,” Administrative Science Quarterly, pp. 370–387, 1990.

[5] D. C. . Gilmore, “Organizational politics and em- ployee attendance.,” Group & Organization Management, vol. 21, no. 4, pp. 481–494, 1996.

[6] S. . Rao and K. J. Satoa, “An attendance monitoring system using biometrics authentication”. International Journal of Advanced Research in Computer Science and Software Engineering 3.4. 2013.

[7] W. . Jones and J. Rickenbacker, “Attendance monitoring system.,” U.S. Patent Application, vol. 10, no. 337.

[8] M. J. . Bennett, “Time and attendance system and method therefor.,” U.S. Patent, vol. 5, 8 1996.

[9] O. H. . C. Jr and R. J. Spooner, “Automated time and attendance system.,” U.S. Patent, vol. 4, 4 1982.

[10] O. G. . Chiagozie and O. G. Nwaji, “Radio frequency identification (RFID) based attendance system with automatic door unit.,” Academic Research International, vol. 2, no. 2, p. 168, 2012.

[11] V. . Bhalla, “Bluetooth based attendance management system. ,” International Journal of Innovations in

Engineering and Technology (IJIET) Vol 3.1 (2013): 227-233.

[12] S. . Kadry and M. Smaili, "Wireless attendance management system based on iris recognition.," Scientific Re- search and essays, vol. 5, no. 12, pp. 1428–1435, 2013.

[13] R. B. . Roy and J. C. Sadlon, "Biometric access control and time and attendance network including configurable system-on-chip (CSOC) processors with embedded pro- grammable logic.," U.S. Patent, vol. 7, 9 2008.

[14] Z. . Singhal and R. K. Gujral, "Anytime anywhere-remote monitoring of attendance system based on RFID using GSM network.," International Journal of Computer Ap- plications, vol. 39, no. 3, pp. 37–41, 2012

[15] N. . Kar, "et al. "Study of implementing automated attendance system using face recognition technique."," International Journal of computer and communication engineering, vol. 1, no. 2, p. 100, 2012.

[16] Kar . Akinduyite, "CHRISTIANAH OLANIKE, et al. "Fingerprint-based attendance management system."," Journal of Computer Sciences and Applications, vol. 1, no. 5, pp. 100–105, 2013.

[17] E. A. A. . Olagunju and T. O. Oladele, "Staff Attendance Monitoring System using Fingerprint Biometrics.," International Journal of Computer Applications, vol. 179, no. 21, pp. 8–15, 2018.

[18] K. N. . A. K. Jain and A. Nagar, ""Biometric template security," EURASIP," J. Adv. Signal Process, vol. 113, pp. 1–113, 1 2008.

[19] W. J. S. . Boult and R. Woodworth, "Revocable finger- print biotokens: Accuracy and security analysis.," Computer Vision and Pattern Recognition, 2007.

[20] W. J. Scheirer and T. E. Boult, "Bipartite biotokens: Definition, implementation, and analysis," in International Conference on Biometrics, 2009, pp. 775–785.

[21] A. . Shamir, "How to share a secret.," Communications of the ACM, vol. 22, no. 11, p. 612613, 1979.

[22] "User's guide to non-export controlled distribution of nist biometric image software,," 2004.

[23] A. K. J. . D. Maltoni and S. Prabhakar, "Handbook of fingerprint recognition,," 2009.

[24] B. A. . Alsolami and T. Boult, Cloud-ID-Screen: Secure fingerprint data in the cloud. Identity, Security, and Behavior Analysis (ISBA), 2018 IEEE 4th International Conference on. IEEE,2018.