Jurnal Ilmu Komputer dan Informasi (Journal of Computer Science and Information)
13/1 (2020), 1-8. DOI: http://dx:doi:org/10:21609/jiki:v13i1:750

STUDENT ATTENDANCE SYSTEM USING WI-FI DIRECT AND TEMPORARY WI-FI HOTSPOT

Doni Setio Pambudi, Taufiqotul Bariyah

Department of Informatics, Faculty of Information Technology and Creative, Universitas Internasional Semen Indonesia, Kompleks PT. Semen Indonesia (Persero) Tbk. Jl Veteran, Gresik, 61122, Indonesia

E-mail: doni.pambudi@uisi.ac.id, taufiqotul.bariyah@uisi.ac.id

Abstract

Manual attendance recording throws away a lot of teaching and administration time from the university. Research on automatic attendance recording that has been done can be divided into biometrics and non-biometrics uses. Almost all methods require additional device that it is costly and inflexible for class changes. The proposed method solves the problems by utilizing the standard features of smartphones that are owned by all student, this method uses Wi-Fi direct for class broadcasting process and temporary Wi-Fi hotspot for verification process. The experimental results show that the proposed method produces the time needed for the initialization process is 14,980 ms and the verification process is 3,640 ms.

Keywords: *attendance recording, Wi-Fi direct, temporary hotspot*

Abstrak

Pencatatan kehadiran secara manual membuang banyak waktu mengajar maupun administrasi dari universitas. Penelitian di metode pencatatan kehadiran secara otomatis yang telah dilakukan dapat dibagi menjadi menggunakan biometrik dan tanpa biometrik. Hampir keseluruhan metode memerlukan peralatan tambahan sehingga menimbulkan biaya dan tidak fleksibel terhadap perubahan kelas. Metode yang diusulkan memecahkan masalah tersebut dengan memanfaatkan fitur standar di telepon pintar yang dimiliki oleh semua mahasiswa, metode ini menggunakan Wi-Fi direct untuk proses broadcasting kelas dan Wi-Fi hotspot sementara pada proses verifikasinya. Hasil percobaan menunjukkan bahwa metode yang diusulkan menghasilkan waktu yang diperlukan untuk proses inisialisasi adalah 14,980 ms dan proses verifikasi adalah 3,640 ms.

Kata Kunci: *pencatatan kehadiran, Wi-Fi direct, hotspot sementara*

1. Introduction

The number of attendance is one of the factors that determine success in the lecture process [1]. The attendance recording process is generally carried out by giving a signature on the attendance sheet that was provided during the lecture. This process wastes lecture time, assume that each student needs 30 seconds to fill in the attendance list, the class with 30 students will need 900 seconds or 15 minutes, if multiplied by 16 meetings each semester, then the time wasted per class is 4 hours or equivalent to more than 1 meeting. Manual recording also requires data entry to the system where if each meeting takes 1 minute to enter data, then the total time needed is almost 4.4 days for 400 classes.

Automatic attendance recording can be divided into two groups based on the media used for authentication. The first group used biometrics as an authentication medium by using parts of the body that were matched with data that had been previously registered, the advantage of this method is that the user does not need to carry other objects to authenticate other than himself. The second group uses media that facilitates user authentication, such as RFID tag, QR code, barcode, smartphone, access point, beacon.

The most popular media owned by students is smartphones, according to an anonymous survey that conducted on 400 students, 85.3% of students had 1 smartphone, 13.2% had 2 smartphones, and 1.5% had more than 2 smartphones. From a scale of 1 - 5 with the largest value indicating more important, the level of importance of smartphones is at level 5 (52.4%), 4 (33.9%), 3 (12.7%), 2 (1%). Furthermore, whether students will entrust their smartphone to friends for more than 2 hours to register attendance obtain results of 1.25% trust their friend and 98.75% is the opposite, most of them due to privacy concern.

From the survey above, smartphones have become basic needs of students and can be used as a media for verification of attendance because every student has it. In this paper, a method to verifying attendance is proposed using 2 types of smartphone's Wi-Fi, namely Wi-Fi direct for the initialization process and Wi-Fi hotspot for the verification process, there is no need for additional devices so no initial cost for implementation, flexible because we can change classrooms without additional effort, this method can also work even though there is no internet connection on the student side.

2. Related Work

Recent years, several attendance verification methods have been proposed and developed. Attendance recording using biometrics has advantages over the other methods because it can ensure that user is present in the classroom. All types of biometrics can be used to authenticate users including fingerprint, face, iris, hand geometry, ear, palm print, palm vein, speech, signature [2].

The most commonly used biometric for attendance recording is fingerprint. Portable microcontroller equipped with fingerprint sensor is used to retrieve fingerprint data [3-5], this device contains registered fingerprint data and attendance records are transferred to the computer for further processing via usb or sd card. This microcontroller can be equipped with communication module such as GSM module, Wi-Fi module or LAN module so it can communicate with server that allow data to be integrated and accessed through mobile applications [6].

Face recognition requires a camera placed at the entrance [7], front of the classroom [8-10], or using smartphone camera [11], it is also possible to combine other media to narrow the scope of face recognition so that it only compares with certain users [12-13]. In [13] student can record their attendace using their smartphone by scanning the QR Code on the monitor in front of the class and capturing their face, this solution only works if student connected in a university Wi-Fi network.

In general, the steps that must be taken in attendance recording using biometrics are data retrieval, pre processing, feature extraction, matching. Combination of microcontrollers and sensors is also found in biometrics using iris, where the eye sensor is combined with a microcontroller connected to a PC using a wireless module [14] or using a webcam connected to the PC [15-16], the latter method is also used in biometric using ear [17] or using palm vein [18] where photos taken with the camera [17] or infrared camera [18] are processed on a connected PC.

QR code and barcode are examples of attendance recording without using biometrics, codes generated by the system is then scanned using the reader [19] or the application on the lecturer smartphone [20-21]. Smartphone add flexibility to attendance recording methods, eliminate queues when processing attendance using a reader or done by the lecturer, by using a smartphone, students can authenticate themselves.

Bluetooth beacons are placed in certain positions in the class so the system can determine the position of the student [22-23], student use their smartphone scaning for available beacons in the class then submit data to the server, the data that is broadcasted can also contain secret codes to improve system security [24].

Another method that uses the features available on all smartphones is via Wi-Fi, the student's position can be detected through Wi-Fi signal strength received by the student's device [25], user authentication can also be done by detecting the mac address of the student connected to the access point [26]. By giving the ssid names with an encrypted token, the limit of users who can connect to access points can be removed because student device do not need to be connected to the access point in order to be authenticated [27].

Almost all methods in previous research require additional devices for implementation such as microcontrollers, sensors, smartphones with specific specifications. Our proposed method eliminate the costs needed for the implementation of the attendance recording system but still maintains the ease of use, flexibility because we can change classrooms without additional effort and validity of student attendance verification by limiting the distance of students from the lecturer.

3. Proposed Method

Our proposed method uses 2 types of Wi-Fi which is Wi-Fi direct as broadcast medium and temporary Wi-Fi hotspot as authentication medium. We do not use standard Wi-Fi direct but we use Wi-Fi direct service, standard Wi-Fi direct cannot contain additional information.

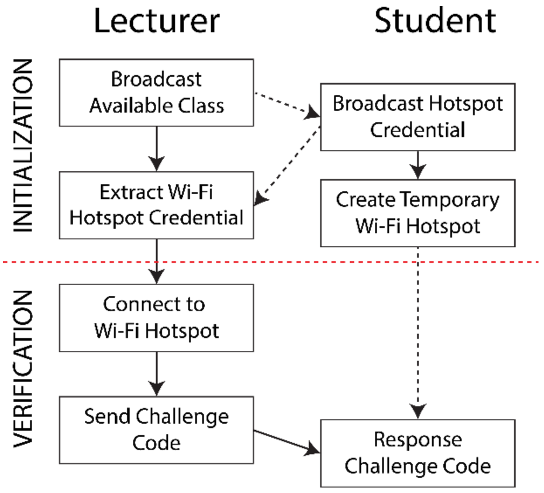

Lecturer
Student
INITIALIZATION
VERIFICATION
Broadcast Available Class
Broadcast Hotspot Credential
Extract Wi-Fi Hotspot Credential
Create Temporary Wi-Fi Hotspot
Connect to Wi-Fi Hotspot
Send Challenge Code
Response Challenge Code

Figure 1. Flow of the proposed method

The flow of attendance recording process can be seen in Figure 1, the proposed method divided into two steps, initialization process and verification process, all process run without user intervention. The initialization process consists of several steps to prepare the verification process by sharing hotspot credential used in the verification process. This process starts when lecturer presses the start button on the selected course in the application then the application broadcasts the selected class. On the other hand, the student choose the available class by pressing the attendance button, where the list of available classes is the class that matches the list taken by the student and the class being broadcasted by the lecturer. The student application provides response to selected class by broadcasting encrypted credential from temporary Wi-Fi hotspot that has been created. On the lecturer side, after broadcasting class data, the application creates a listener to listen for attendance recording request, when the request is received then the application decrypts the credential information. Both broadcasting processes use Wi-Fi Direct Service.

The verification process is used to check whether the application connected to the lecturer is a legitimate or not. The lecturer application connects to the Wi-Fi hotspot with the credentials obtained from the previous step. When the application is connected to the Wi-Fi hotspot, the lecturer application sends a challenge code that must be answered by the student application, if the answer is correct then the student is considered to be present at the lecture. Reverification process can be added after random time to improve validity and reduce attempts to attack using Wi-Fi / radio waves properties (range and penetrating object) or to prevent students from leaving class after recording attendance.

Why Wi-Fi

The main focus of the proposed method is to maximize flexibility and minimize costs while still maintaining the security and validity of the verification process, the process must also be as easy as possible without user intervention. We try to eliminate the need for additional devices that must be installed in each classroom, causing some methods impossible to implement, therefore the possible method to use is Bluetooth, Wi-Fi, 2D code (QR code or barcode), NFC phone and GPS. We remove web and mac address-based methods because it is difficult to limit the user’s location without additional devices or efforts.

Flexibility means how the attendance verification process can adapt to a variety of changes, such as changing classrooms and changing schedules, consider that the university has at least dozens of classrooms and some have hundreds or thousands, it is also possible to teach outside the classroom.

2D code has a security hole where students can take photos and send to friends who are not in class, while NFC phone is less popular because only mid-upper tier phones are equipped with these feature so the only available options are Bluetooth and Wi-Fi. The GPS-based method is ignored because it is very easy to spoof the device location with fake gps application and it is hard to get a GPS signal inside the building. Likewise when the location has been obtained it will be difficult to determine on which floor the user is due to GPS altitude error always bigger than horizontal error [28-29].

Bluetooth is better at limiting user’s distance because smartphone’s bluetooth (category 2) has maximum range of 10 meters, while smartphone’s Wi-Fi have a maximum range of 100 meters. Bluetooth also has an advertising feature on bluetooth LE supported devices but only latest smartphone is supported. Bluetooth and Wi-Fi direct need paired device to make a connection. It is very easy to pair two devices, user only need to tap the pair button in the popup dialog but if we multiply that action with number of students then it becomes an inconvenience. Temporary Wi-Fi hotspot is the solution for the previous problem. Wi-Fi direct services are used to broadcast initial information and Wi-Fi hotspots are used to establish connection for the verification process.

Encryption Key

For every class taken by students the system will create different encryption keys stored on the server. This key is used to encrypt the credential of the temporary Wi-Fi hotspot during the initialization process, key consists of random character k with minimum length n multiply by number of academic week w that reflects the number of lectures that must be recorded as seen in equation 1. Figure 2 show example of generated key with n = 8, the first 8 characters is key for academic week 1 and so on, 8 characters is certainly not a safe key, here is only used as an example.

$$k_{length} = n * w \tag{1}$$

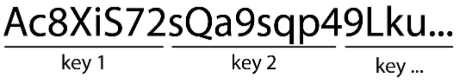


Figure 2. Example of generated key with n = 8

In the explanation above all encryption keys are generated at the same time, this is to accommodate students who do not have an internet connection, so only need an internet connection to download all keys only once at the beginning of the semester, a safer approach is to generate the key needed during the initialization process. Keys are obtained by the lecturer application during the initialization process by downloading all the keys from the server for the course in that week which is used by students who are members of the class. In addition to the encryption key also requires a challenge code that is random characters that have sufficient length (more than or equal to k_{length}).

Initialization Process

Before the initialization process starts, the lecturer and student must tap the start button. The lecturer application will create Wi-Fi direct service contain information such as action, class code and week number w_i, the latter data correlates with the key used during the encryption process. Broadcast data can be modified as needed but it is better to keep the data to a minimum, according to specification, the best size for txt record is below 200 bytes, but it can hold up to 1,300 bytes [30], Silvennoinen also conducted tests using several devices and obtained approximately 900 bytes of data sent [31].

Figure 3 contains an example of data broadcast by the lecturer application, line 1 is action data contains information about the current state, init means the application is receiving a request for verification, the next line is class code which is the unique code of the selected class, while the last is current week number information.

```
init
1AB670F9
2
```

Figure 3. Example data broadcast by the lecturer application

The student application starts service discovery and listens to services with init action and contain class code that have been taken by the student, if the application finds the service then the application creates a Wi-Fi direct service with data containing action, class code, student code, hotspot name, user name, password, we combine and encrypt student code and data after that with encryption key w_i, at the same time the application creates a temporary hotspot with the same access. Figure 4 is an example of data broadcast by the student application, the first line is the state of the action, where the example shows that it is requesting a verification process. Action is important because Wi-Fi Direct receives all data broadcast by any device. Therefore, we need data that can be used to distinguish between devices.

```
verification
1AB670F9
AF231CDE……..
```

Figure 4. Example data broadcast by the student application

On the other hand, the lecturer application starts the process of discovering Wi-Fi direct services that match the class code and have verification action. When finding the appropriate service, the application decrypts the combined data to connect to the hotspot created by student application using key w_i.

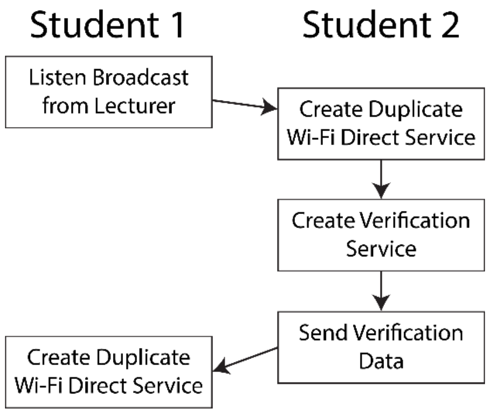

Student 1
Student 2
Listen Broadcast from Lecturer
Create Duplicate Wi-Fi Direct Service
Create Verification Service
Send Verification Data
Create Duplicate Wi-Fi Direct Service

Figure 5. Flow of how to be verified without being in classroom

Verification Process

This step is very simple but very important in this method because it eliminates the security hole from the previous step, when the initialization process read the broadcast data, it cannot ensure that the data is sent by a legitimate user. Figure 5 shows how students can be verified without being in the classroom, this looks rather complicated, but with simple client-server program (h_1 and h_2) it can be easily done.

The student 1 who attends the lecture sends Wi-Fi direct data scanned to the student 2 using h_1 who is outside the class or even at home, the student 2 application (h_2) then creates identical Wi-Fi direct service with the data provided. The Official student application will respond by creating a service for verification, this service information is forwarded by h_2 to replicate the same service for verification with the official lecturer application. Therefore, the proposed method use a challenge code to verify student attendance, challenge code is a random character with fix length created after encryption key generation.

The verification process starts with the lecturer application connect to the Wi-Fi hotspot using connection parameters decrypted from the previous step, then the application sends a challenge code to the student application which must be replied with the correct answer in order to get verified, data sent from both the lecturer and student application must be encrypted with key w_i. The lecturer application can find out the challenge code because when making an encryption key request, the server also provides a challenge code along with the answer.

4. Experiment and Analysis

Non-biometric method do not require an accuracy test because as long as the data can be read, we can identify who the user is. In this experiment we measured the time required from the attendance recording process.

Time Measurement

The time required by this method according to Figure 1 is divided into 2 processes which is initialization and verification, the initialization process is done simultaneously while the verification process are done one by one, we ignored time to challenge because it is not significant.

The advantage of using Wi-Fi is Wi-Fi direct and Wi-Fi hotspot can be used together, so we use 2 separate processes that run together. As we can see in Figure 6 verification process is done one by one, so that it will wait for the previous verification to be completed before it can proceed to the other students.

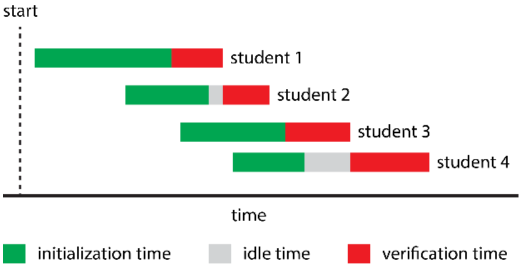


Figure 6. Time frame of how initialization and verification work

$$Total\ Time = \max(t_i) + \sum t_v \qquad (2)$$

If we assume that the initialization time ends at the same time, then the time needed for attendance recording can be seen in equation 2, where t_i is initialization time and t_v is verification time.

Experiment

In this experiment, time measurements were taken from 7 devices to detect Wi-Fi direct and connect Wi-Fi hotspot compared to distance, both tested without obstacles and through the wall.

Table 1 shows that distance does not affect Wi-Fi direct detection time, as long as the Wi-Fi direct signal is still within range, the data from Wi-Fi direct can still be received. The time above is for measuring the broadcast from lecturer to student, from there it can be estimated that the time needed by the initialization process is 2 times from the time above. The maximum time for this first experiment is 7,490 ms.

TABLE 1
DISTANCE COMPARED TO INITIALIZATION TIME

d	Time of each device (ms)						
(m)	1	2	3	4	5	6	7
1	1,911	1,303	4,094	3,776	6,496	6,584	1,432
3	3,526	1,579	1,920	2,531	2,820	2,647	1,505
5	650	380	2,780	5,149	922	7,490	466
7	4,104	956	2,251	447	1,579	3,307	2,638
9	6,402	557	3,890	6,013	1,244	5,894	1,346
11	2,594	1,780	3,086	3,476	2,836	-	2,240
13	820	658	2,162	1,546	2,065	4,836	1,620
15	905	1,241	1,227	5,411	2,766	7,030	2,175
17	-	670	2,701	3,871	1,559	4,235	4,143

Table 2 measures how the effect from the wall on detection time and range, the results obtained indicate that the presence of a wall affects the received signal, the results of the experiment show the number of devices that cannot detect Wi-Fi Direct signals exceeding the results of previous experiments. The maximum time for this second experiment is 14,085 ms.

TABLE 2
DISTANCE COMPARED TO INITIALIZATION TIME THROUGH THE WALL

d	Time of each device (ms)						
(m)	1	2	3	4	5	6	7
1	4,593	1,681	1,129	2,835	5,187	-	1,174
3	3,212	11,575	1,532	2,369	940	4,462	2,077
5	289	-	1,983	-	-	-	-
7	2,807	14,085	342	2,733	3,263	3,883	1,934
9	2,403	203	3,147	3,083	5,908	1,394	2,927
11	1,900	335	1,142	328	2,487	2,793	1,779
13	-	-	6,382	6,533	-	-	-
15	2,441	-	-	-	3,182	-	-
17	2,419	-	-	12,773	2,018	-	-

The next experiment measured the time needed to connect to the Wi-Fi hotspot. The results of Table 3 and Table 4 can be concluded that the average time needed increases if passes through the wall, but in contrast to the two previous experiments, it still can be received within range that failed with he previous experiment. The maximum time needed to connect to the Wi-Fi hotspot in experiments 3 and 4 is 3,640 ms and 9,610 ms

TABLE 3
DISTANCE COMPARED TO VERIFICATION TIME

d	Time of each device (ms)						
(m)	1	2	3	4	5	6	7
1	1,520	1,460	1,640	1,580	2,260	2,160	3,350
3	1,640	1,710	1,580	2,090	2,170	3,240	3,290
5	1,770	1,830	1,580	1,970	3,130	3,640	3,270
7	1,650	1,710	2,040	1,510	2,260	2,390	2,820
9	2,220	1,650	2,030	1,770	2,260	3,580	3,370
11	1,910	1,910	2,430	1,710	2,390	2,260	3,460
13	1,840	2,000	2,090	1,970	3,310	3,640	3,320

TABLE 4
DISTANCE COMPARED TO VERIFICATION TIME THROUGH THE WALL

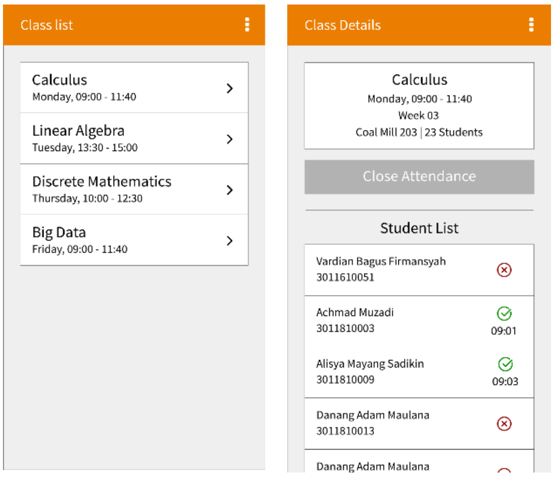
d	Time of each device (ms)						
(m)	1	2	3	4	5	6	7
1	2,030	1,720	6,670	2,490	3,490	3,500	3,360
3	2,360	1,850	2,950	1,900	2,330	3,390	3,350
5	2,160	3,010	2,130	2,300	3,510	3,270	2,360
7	5,570	1,790	2,560	1,580	2,420	2,340	7,560
9	8,010	1,970	1,690	2,490	3,500	2,230	2,230
11	3,020	2,090	2,090	2,320	3,430	2,440	2,480
13	2,750	3,010	8,500	2,360	3,550	9,150	2,460

Experiments by passing through the wall is done to determine the maximum limit of distance that can be detected and how fast the connection is, if the distance is too far then student can intentionally not be in class but try to do attendance recording. Table 2 shows the maximum distance 11 meters for the connection to run smoothly. This distance can ensure students are in the classroom because the size of the classroom is most likely exceeds that distance. We also test how far the signal from the Wi-Fi hotspot can be detected with a result of 20 meters.

From the experiment above, the estimated time needed for attendance recording if the class contains 30 students is:

$$2 \text{ x } 7{,}490 + 30 \text{ x } 3{,}640 = 124{,}180 \text{ ms} = 125 \text{ s}$$

Manual attendance system average execution time for 30 students is approximately 900 seconds or 15 minutes as against 125 seconds for the proposed system. It can be shown from the illustration of the attendance calculation above and thus, it can be seen that the system using wi-fi direct is better and faster than the use sheets of paper.



Calculus
Monday, 09:00 - 11:40 >

Linear Algebra
Tuesday, 13:30 - 15:00 >

Discrete Mathematics
Thursday, 10:00 - 12:30 >

Big Data
Friday, 09:00 - 11:40 >

Calculus
Monday, 09:00 - 11:40
Week 03
Coal Mill 203 | 23 Students

Student List

Vardian Bagus Firmansyah
3011610051 ☒

Achmad Muzadi
3011810003 ✓ 09:01

Alisya Mayang Sadikin
3011810009 ✓ 09:03

Danang Adam Maulana
3011810013 ☒

Danang Adam Maulana

Figure 7. Interface of lecturer application

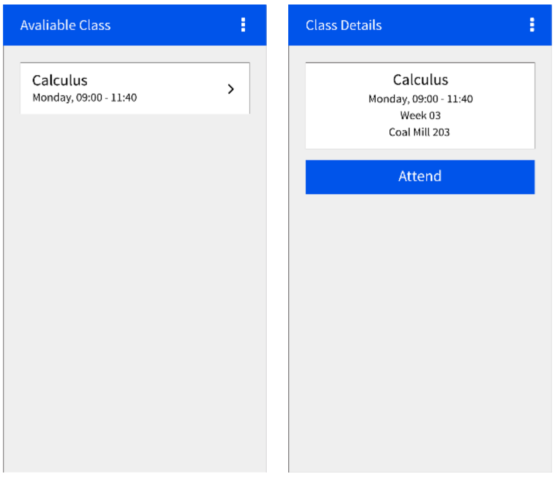


Figure 8. Interface of student application

Graphical User Interface (GUI)

The Graphical User Interfaces (GUI's) of the proposed system shown in Figure 7-8. Figure 7 illustrates the proposed system application interface for the lecturer side, while Figure 8 illustrate the system application interface for students. Figure 7 (left) shows the interface of the courses list taught by the lecturer. Lecturer can choose the course to be taught, then the lecturer will be taken to the next interface Figure 7 (right) where the details of the course and 'Open Absensi' button will be displayed. Figure 7 (right) also shows the update students' name list which have been successfully attended class after lecturer clicked 'Open Attendance' button (this button changes to 'Close Attendance' when clicked).

Figure 8 (left) shows the list of the classes currently open and also shows the class information and 'Attend' button for student to start attending the selected class (right picture). An updated list of student names that have been recorded for attendance validation will be displayed on the lecturer interface Figure 7 (right).

5. Conclusion

This paper proposes a method of automatic attendance recording which is divided into initialization process using Wi-Fi direct and verification process using Wi-Fi hotspot. The initialization process works by broadcasting class data by the lecturer smartphone which is responded to by student data and encrypted temporary Wi-Fi hotspot access by student smartphone. Attendance forgery can be eliminated by verifying students connected via temporary hotspot with challenges in the form of unique codes that have been prepared for each class meeting. From the results of the experiment it can be seen that the time needed for the initialization process is 14,980 ms while the time for the verification process is 3,640 ms, with this results it is estimated that the time needed to complete attendance recording for class of 30 students is 125 seconds.

Acknowledgement

This research has been made possible by the LPPM UISI under the scheme of "Hibah Riset Bersaing". We extend our gratitude for the support.

References

[1] A. Lukkarinen, P. Koivukangas, T. Seppala, "Relationship between class attendance and student performance" *In Proceeding of HEAd´16*, pp. 341-347, 2016.

[2] M.F. Zanuy, "Biometric security technology," *IEEE Aerospace and Electronic Systems Magazine*, vol. 21, pp. 15-26, 2006.

[3] N.I. Zainal, K.A. Sidek, T.S. Gunawan, "Portable Anti Forgery Recognition for Attendance System Using Fingerprint Based Biometric," *ARPN Journal of Engineering and Applied Sciences*, vol. 11, pp. 396-403, 2016.

[4] N.I. Zainal, K.A. Sidek, T.S. Gunawan, H. Mansor, M. Kartiwi, "Design and Development of Portable Classroom Attendance System Based on Arduino and Fingerprint Biometric" *In Proceeding of ICT4M 2014*, 2014.

[5] B.K.P. Mohamed, C.V. Raghu, "Fingerprint Attendance System for classroom needs" *In Proceeding of INDCON 2012*, pp. 433-438, 2012.

[6] L. Kamelia, W. Darmalaksana, E.A.D. Hamidi, A. Nugraha, "Real-time Online Attendance System Based on Fingerprint and GPS in the Smartphone" *In Proceeding of ICWT 2018*, 2018.

[7] S. Chintalapati, M.V. Raghunadh, "Automated Attendance Management System Based-on Face Recognition Algorithms" *In proceeding of ICCIC 2013*, pp. 1-5, 2013.

[8] A. Raghuwanshi, P.D. Swami, "An Automated Classroom Attendance System Using Video Based Face Recognition" *In Proceeding of RTEICT 2017*, pp. 719-724, 2017.

[9] M. Fuzail, H.M.F. Nouman, M.O. Mushtaq, B. Raza, A. Tayyab, M.W. Talib, "Face

Detection System for Attendance of Class Students," *IJMSE*, vol. 5, pp. 6-10, 2014.

[10] N.D. Veer, B.F. Momin, "An automated attendance system using video surveillance camera" *In Proceeding of RTEICT 2016*, pp. 1731-1735, 2016.

[11] S. Budi, O. Karnalim, E.D. Handoyo, S. Santoso, H. Toba, H. Nguyen, V. Malhotra, "IBAtS - Image Based Attendance System: A Low-Cost Solution to Record Student Attendance in a Classroom" *In Proceeding of ISM 2018*, pp. 259-266, 2018.

[12] M.S. Akbar, P. Sarker, A.T. Mansoor, "Face Recognition and RFID Verified Attendance System" *In Proceeding of iCCECOME 2018*, pp. 168-172, 2018.

[13] D. Sunaryono, J. Siswantoro, R. Anggoro, "An android based course attendance system using face recognition," *Journal of King Saud University*, vol. 31, 2019.

[14] S. Kadry, M. Smaili, "Wireless attendance management system based on iris recognition," *Scientific Research and Essay*, vol. 5, pp. 1428-1435, 2010.

[15] A. Khatun, A.K.M.F. Haque, S. Ahmed, M.M. Rahman, "Design and Implementation of Iris Recognition Based Attendance Management System" *In Proceeding of ICEEICT 2015*, 2015.

[16] T.W. Hsiung, S.S. Mohamed, "Performance of Iris Recognition using Low Resolution Iris Image for Attendance Monitoring" *In Proceeding of ICCAIE 2011*, pp. 612-617, 2011.

[17] J.B. Jawale, A.S. Bhalchandra, "Ear Based Attendance Monitoring System" *In Proceeding of ICETECT 2011*, pp. 724-727, 2011.

[18] S. Bayoumi, A. Aldayel, M. Alotaibi, M. Aldraihem, S. Alrashed, S. Alzahrahi, "Class Attendance System Based-On Palm Vein as Biometric Information," *JTAIT*, vol. 77, pp. 266-272, 2015.

[19] H. Subramaniam, M. Hassan, S. Widyarto, "Bar Code Scanner Based Student Attendance System (SAS)," *TICOM*, vol. 1, pp. 173-177, 2013.

[20] A.A.A. Rahni, N. Zainal, M.F.Z. Adna, N.E. Othman, M.F. Bukhori, "Development of The Online Student Attendance Monitoring System (SAMS^{TM}) Based on QR-Codes and Mobile Devices," *Journal of Engineering Science and Technology*, Special Issue on UKM Teaching and Learning Congress 2013, pp. 28-40, 2015.

[21] D. Deugo, "Using QR-Codes for Attendance Tracking" *In Proceeding of FECS 2015*, pp. 267- 273, 2015.

[22] R. Apoorv, P. Mathur, "Smart Attendance Management using Bluetooth Low Energy and Android" *In Proceeding of TENCON 2016*, pp. 1048-1052, 2016.

[23] M.S.M. Azmi, M.H.M. Zabil, K.C. Lim, R.F.R. Azman, "UNITEN Smart Attendance System (UniSas) Using Beacons Sensor" *In Proceeding of IC3e 2018*, pp. 35-39, 2018.

[24] S. Noguchi, M. Niibori, E. Zhou, M. Kamada, "Student Attendance Management System with Bluetooth Low Energy Beacon and Android Devices" *In Proceeding of NBiS 2015*, pp. 710-713, 2015.

[25] M. Zheng, S. Li, H. Fan, "Classroom Attendance Detection using a Wi-Fi Positioning Algorithm" *In Proceeding of CSREAP 2016*, pp. 243-247, 2016.

[26] M. Alfarizi, R. Primananda, R.A. Siregar, "Implementasi Smart Identification Menggunakan Perangkat Smartphone dengan Raspberry PI (Studi Kasus: SMAN 2 Balikpapan)," *JPTIIK*, vol. 2, pp. 2899-2906, 2018.

[27] M. Choi, J.H. Park, G. Yi, "Attendance Check System and Implementation for Wi-Fi Networks Supporting Unlimited Number of Concurrent Connections," *International Journal of Distributed Sensor Networks*, vol. 2015, 2015.

[28] GPS Gov, GPS Accuracy, Official U.S. government information about the Global Positioning System (GPS) and related topics, https://www.gps.gov/systems/gps/performance/accuracy, retrieved April 5, 2019.

[29] C. Bauer, "On the (In-)Accuracy of GPS Measures of Smartphones: A Study of Running Tracking Applications" *In Proceding of MoMM2013,* pp. 335-341, 2013.

[30] IETF, RFC 6763 - DNS-Based Service Discovery, IETF Tools, https://tools.ietf.org/html/rfc6763, 2013, retrieved April 5, 2019.

[31] J. Silvennoinen, Wi-Fi Direct and Dns-Sd Txt record size measurements, Dr. Jukka's mobile Blog, http://www.drjukka.com/blog/wordpress/?p=127, 2015, retrieved April 5, 2019.