2017 IEEE International Conference on Smart Technologies and Management for Computing, Communication, Controls, Energy and Materials (ICSTM), Veltech Dr.RR & Dr.SR University, Chennai, T.N., India. 2 - 4 August 2017. pp.3-6.

WLAN Attendance Management System

Vishal Naidu[1], Kumaresan Mudliar[2] and **Kailas Devadkar[3]**

Sardar Patel Institute of Technology, Andheri, Mumbai, India.
Email: [1]naiduvishal13@gmail.com, [2]kumaresh1112@gmail.com, [3]kailas_devadkar@spit.ac.in

***Abstract*— This paper is regarding the proposal of a whole new concept in the category of automatic attendance marking systems. The proposed methodology suggests making use of the fact that more than 99 percent of the student population of today's generation has a smartphone on his or her person, all of which are capable of using and sharing data via Wi-Fi technology. Use of such technology coupled with a background service on the host's smartphone to monitor the phones existing within the range and the amount of time they do so, will enable the host to mark the attendance of such population for which data regarding all students or attendees exist in the host's local database. The interesting feature of this implementation is that fooling the WLAN attendance will require attending the lecture itself, which would show significant decrease in the faulty-accept rates that is shown by the paper-pen attendance systems and would show much higher flexibility and ease of usage as compared to biometric systems.**

***Index Terms*— Attendance, Automatic, WLAN, Polling, Wi-Fi**

I. Introduction

The current world is at the brink of wireless revolution as we see wired solutions getting replaced by wireless ones wherever there's a possible performance-flexibility tradeoff, as managing wired technology is cumbersome, it takes more time to set up, and any faults in the wired medium are quite difficult to identify in some scenarios. Wireless technology on the other hand is hassle-free, works at a performance level much comparable to the wired solutions in the current technology standards, and provides much greater flexibility and management capability.

The same wireless revolution is what the paper-pen or biometric system would await. In today's world, almost all people having a presence in the digital universe carry a mobile phone on their person. A high percentage of people amongst the above carry phones that are so called 'Smartphones'[2] that have features comparable to a full-fledged desktop, plus the ability to carry it wherever one goes and to make calls, connect to different networks, share mobile-data with other phones, and more.

One of these features the smartphone provides and that can be used to adapt to an algorithm on a remote device that looks for a smartphone showing its presence in its wireless vicinity, is WLAN. [3, 4]

II. The Model Proposed

Figure 1 of the paper shows the flow diagram for the proposed model, indicating the working of the automatic attendance system, making use of multiple smartphone hardware or devices to mark the presence of a human being. The smartphone is considered as an integral part of a person's possession, and complying to the category, 'The things one carries when attending any session in an institution'.

Described below is the model, structured in a number of stages. Each of the stages indicate a different phase in the workflow that binds together different devices in the Automatic Attendance System. The current model is based on a smartphone application that carries out the script work that the stages mention.

A. The Unique ID

The unique identifier in this case is the (Google Plus Account) email address. Using biometric scan to tag the human to the phone is not feasible due to finger print sensors being available on devices much lower in numbers as compared to the complete digital smartphone population. Unique identifier provided by Google can be used to screen multiple copies of the same id across a session, to avoid the same attendee being marked twice.

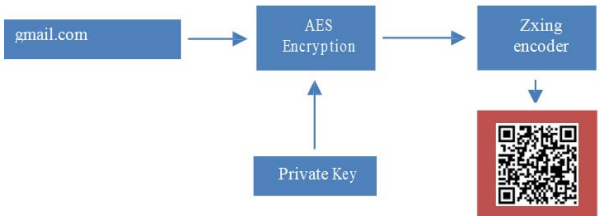

Fig. 1. The Unique Identifier generation process

978-1-5090-5905-8/17/$31.00 ©2017 IEEE

The QR-Code (use described in the next section) is created using the unique identifier made available by 'Google-Auth API' [5]. The same can be encrypted using AES and a key private to the developers of the application.[6]

B. Host Set-Up

The host smartphone is the center of the WLAN Attendance Marking System. The host uses the smartphone application to define the 'Session Tag' which is the class he creates. A class here is the container for storing data regarding the attendees. The attendee data addition process is a 'One-off', meaning it is done once for a set of attendees which can be later tagged onto different classes as well. Using encrypted QR-Code to transfer unique identifier from the attendee's phone to the host's phone will make the data entry process easier, faster and much secure as compared to manual entry. [7]

C. Encrypted SSID

The attendee's smartphone must contain the attendee version of the application to enable attending the session generated by the host possible. The unique identifier created in section A is one of the keys used to make a unique network identifier to make it visible in the host's session filter.

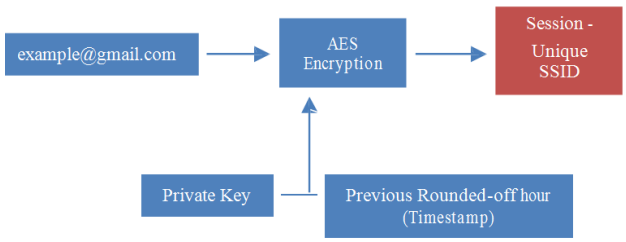

Fig. 2. The session-unique SSID generation process

The reason 'Previous rounded-off hour' is used here is to make sure that the AES encrypted value for the unique identifier keeps changing across sessions. This feature will make sure that a person cannot use the same SSID to create an identity using which he or she can spoof the presence of that person on the Attendance Polls conducted by the host. [8, 9]

D. The Scanning Process

The application running on the host smartphone is responsible for deploying the scanning algorithm. The host phone runs an instance of the application in the form of a background service on session start. This service would follow the Polling Algorithm [10,11] described below, to mark the attendees as present or absent based on the results of the polls. The polls conducted will be automatic and will be timed at an interval chosen by the host user, and the session length will decide how many polls take place till the end of the session.

Working of the scanner service includes first getting the data for all the attendees registered for the class from the database and making a temporary hash table for the same. The unique_id_hash will be a value we get by following the steps from stage C. The hash table format will be as follows:

After the above process completes, the service keeps hashes of all the attendees' unique IDs ready in the hash table. Now, the service will start the Wi-Fi scan, filtering the SSIDs that match with the keys present in the hash table. For every scan that takes place, within the decided session length, the attendee's phone's Encrypted SSID, if matches one of the stored keys from the hash table, the polls of that particular object for the table is updated i.e. (+1).

Algorithm for Scanner service

// All values stated in round brackets are example variables

// initiated

// Original variable and data may vary

1. Get class id (X) from calling activity
2. Read the 'Registered Attendees' table
3. Create an array (RegList) of all the attendees that registered for class X
4. Create hash table (AtndHashTable)

   (unique_id_hash, (attendee_database_id, polls_present))
5. For each (Atnd in RegList)
   a. Encrypt Atnd using private key
   b. Add the encrypted value as key to AtndHashTable
   c. Add 0 as polls for the above value added to the hash table
6. (TotalPolls = 0)
7. Set (SessionLength) and (PollingInterval)
8. Calculate (EndTime = CurrentTime() + SessionLength)
9. While (CurrentTime() < EndTime)
   a. Start Wi-Fi scan
   b. Receive scan result
   c. For each (Val in ScanResult)
      i. If (AtndHashTable contains(Val)) AtndHashTable[Val](Polls + 1)

d. Wait (PollingInterval)

e. TotalPolls + 1

10. For each (Attendee in AtndHashTable)

a. If (Attendee(Polls) > (50% of TotalPolls))

i. Attendee(Present) = true b. Else

i. Attendee(Present) = false

11. Update 'Attendance Logs' table using

a. All Attendee such that

Attendee(Present) == true

III. The Application

The application that the proposed system would run on can be brought into action using Android Application Development using Java, Windows Universal Application on C# or Objective C for an IOS [12] build. The current implementation is achieved using Android, and screenshots for the working build of the application are pasted below:

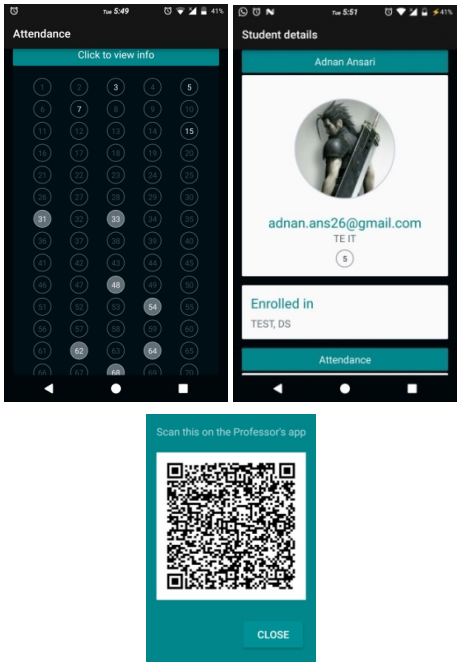

Fig. 3. Application instance screenshots

1. Attendance log for test session
2. Student data retrieved from the database and Google-Auth
3. Generated QR-Code

The application was designed to show a table of all the roll numbers available in the students list. All the roll number indications shown in 'Bright Gray' were those students who were 'Registered and Present', all those without the shade were 'Registered but Absent'. All those that appear dull are 'Unregistered' students.

Clicking on any one of the buttons in the form of roll numbers will give a page displaying information about the student registered for that roll number.

The screenshot shown of a dialog in the 3rd image is that of the QR-Code that is scanned on the host phone at most once to be able to tag to any class or session.

IV. Features and Advantages

1. Improved security because of attendee look-up for more than once in the entire session
2. Proves much more reliable as compared to traditional paper-pen-signature method for attendance maintenance
3. The current method would not require tiresome biometric scans which would require buying more 'Fingerprint Scan Terminals' to speed up the attendance process
4. No additional cost incurs because the only apparatus the WLAN Attendance System needs is a Wi-Fi capable smartphone
5. Would reduce the time wasted in verifying attendance at the end of the session, because the verification is fully automated
6. Would be more battery optimized. The reason being that CPU intensive connection protocols are not called intermittently. Instead frequent Wi-Fi look-ups are used
7. SSIDs encrypted using an 'Ever-changing' key can reduce the faulty-positive rates by a great magnitude
8. 'FirstConnect' is an add-on decided for the system, requiring the host phone to connect and set a 'HandsUp' schedule on the attendees' phones to reduce the Wi-Fi lookup population in case some phone hardware doesn't allow such large number of phones to be tracked at once
9. Attendance for those who have missed/misplaced their phones can be managed using 'Exclusions', a feature in the application used to set singular attendances manually.

V. DISADVANTAGES

1. If the host fails to activate the Scanner service when the session starts he has to make one of the two choices stated below:
   a. Start service immediately reducing the session length
   b. Mark the attendance manually
2. Encryption is a trade-off between performance and security [13]
3. If the host himself forgets his phone, he won't be able to mark the attendance for that session

VI. CONCLUSION

The WLAN Attendance System is a system created to give rise to a hassle-free attendance management system for professors at the college levels who struggle with attendance on paper and/or any case of faulty-acceptance, also known as a

'Proxy' as signed by a fellow attendee. Solving these problems using the Wi-Fi technology available on every smartphone in today's digital world becomes easy.

Thus, we have created an application that demonstrates the use of the above-mentioned technologies to mark attendance in an easy, wireless and digital mode.

REFERENCES

[1] Wireless Technology source: *http://home.deib.polimi.it/capone/rmd/materiale_tarr/2- wpan/ComMag01.pdf*

[2] Asma Patel, Esther Palomar, "Privacy Preservation in Location-Based Mobile Applications: Research Directions", Availability Reliability and Security (ARES) 2014 Ninth International Conference on, pp. 227-233, 2014.

[3] Mobile Privacy, 2011, [online] Available: http://www.gsmworld.com/our- work/public-policy/mobile_privacy.htm.

[4] Wireless Lan source : https://en.wikipedia.org/wiki/Wireless_LAN

[5] Google API source : https://en.wikipedia.org/wiki/Google_Developers

[6] Ensuring Uniqueness: Collecting iris biometrics for the Unique ID Mission, [online] Available : http://uidai.gov.in/UID_Pdf/working_ Papers/UID_and_iris_paper_final.pdf

[7] Toktam Hemmati, Mohammad Hossein Yaghmaee Moghadam, "SIP- based vertical handover scheme with bicasting", Advanced Communication Technology (ICACT) 2014 16th International Conference on, pp. 19-22, 2014.

[8] S.M.K.M. Abbas Ahmad, Dr. E.G. Rajan, Dr. A. Govardhan, "Robust and Secured WEP Protocol For Wireless Ad Hoc Network", International Journal of Recent Trends in Engineering, Volume 2 November, 2009, pp 248- 252, Academy Publishers, Finland.

[9] Diffie, W. and Hellman, M.E. New directions in cryptography, IEEE Transactions on Information Theory November 1976, IT- 22, 644-654

[10] M. Kamran, "A framework for dynamic bandwidth allocation algorithms in TDM Ethernet passive optical networks", Proc. International Symposium on High Capacity Optical Networks and Enabling Technologies, Nov., 2007.

[11] H. Song, B. W. Kim, B. Mukherjee, "Multi-thread polling: a dynamic bandwidth distribution scheme in long-reach PON", IEEE J. Select. Areas Commun., vol. 27, no. 2, pp. 134-142, Feb. 2009.

[12] J. Andrus, A.V. Hof, N. AlDuaij, C. Dall, N. Viennot, J. Nieh, "Cider: Native execution of iOS apps on Android", 19th International Conference on ArchitecturalSupport for Programming Languages and Operating Systems, pp. 367-382, March 2014.

[13] J. K. Mandal, Arindam Sarkar, "An adaptive genetic key based neural encryption for online wireless communication (AGKNE)", Recent Trends in Information Systems (ReTIS) 2011 International Conference on, pp. 62-67, 2011.