ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 2, Issue 4, April 2013

Automatic Wireless Attendance Recording and Management Using Near Field Communication (NFC)

Kumari Lavanya[1], Midhila NM[2], Eveline Blessy[3], [4]B.Karthik
[1,2,3] ECE Department, Bharath University
Selaiyur, Chennai-73, India
[4]Assistant Professor, Bharath university
Selaiyur, Chennai-73, India

Abstract- **In this world of automation, there is a continuous need for the constant evolution and up gradation of the existing mechanisms. There is an urge for automation wherein people do less work and machines do more. This project aims at providing a user friendly and automated way of attendance entry and data management with the help of dedicated recorders placed at classrooms and labs. It also helps to avoid large registers, manual calculations, false entries etc. In places such as colleges, schools and large industries there is a continuous need for monitoring the presence of workforce – their in and out time etc. These details are marked in a register and the whole data is collected for each and every department and for every hour. Further there is a manual calculation that involves for salary calculation, number of days present or absent etc. The project proposes a system wherein any staff after entering into the classroom can record the attendance of the students in an electronic register. This register communicates with the PC placed at office rooms and the students' details, time of attendance, staff details are all recorded in the PC. The PC does the rest of the job and no manual calculation or error occurs. It sends the students attendance report to their parents as SMS using GSM. The teachers can login to their respective id to check the student's attendance status and save it. The project proposes a novel way of identification system that is tamper proof and is easily usable by everyone concerned. For that it uses NFC technology that is known for communication between multiple tags at a specific time. This particular feature of NFC makes identification and processing very easy as the signals are completely wireless and has a collision free algorithm to transmit and receive signals from multiple units. The staff can use a dedicated card for identifying themselves at the recorder. This prevents misuse by the students. Further the details of the staff are also recorded along with the attendance details. Further if any class is left without teacher for a particular period of time, it is also recorded and suitable authorities are alerted. Thus with the help of this the whole process of attendance management can be automated and it reduces lots of hardships and manual calculations. Further any detail regarding any person can be obtained within a few clicks at any time.**

Keywords: **Near Field Communication (NFC) technology, Education related business processes automation, Secure and reliable person identification, contactless card technology, embedded system with wireless access**

I. INTRODUCTION

Near Field Communication (NFC) is an upcoming technology with a great potential for many application that were either not possible earlier. It is give a higher platform for attendance system where the no. of students is very high and it is not possible to take attendance manually. NFC is one technology that can bridge the gap between wired communication and conventional wireless communication technologies like Bluetooth and Zigbee etc. it is with reduced cost and complexity with increase in efficiency of education. NFC is particularly useful in applications where a wired communication might not be possible, but existing wireless technologies are also not suitable. In order to ensure a healthy participation from the students in the lecture rooms such incentive process was introduced like making the students presence at

lectures as perquisite of the examination. However, taking manually attendance reports during lectures can be tedious and hard to maintain task which consumes valuable in-class time.

II. REQUIREMENTS

In this section we present an overview on the basic requirements of the monitoring system outlining the security requirements at the end of the section. During the identification of the requirements we had taken into account two main goals. The first goal is to provide reliable enough attendance data which can be used to sanctioning the students. According to the university ethical codex if a student does not visit a predefined percentage of the lectures he fails the possibility to enter the exam at the end of the semester. The second goal driven by both the availability of the NFC technology and also the spreading of NFC enabled mobile equipments in the market is to prepare the system to be used with NFC enabled mobile phones as well as NFC capable smart cards.

Functional requirements

The fundamental consideration is that the student has to prove his presence in a given time window before and after each lecture. If the student meets the above requirements his presence at the lecture is confirmed. As an average lecture at the university is held for more then two hundred students it is necessary to provide an easy and straightforward opportunity for presence indication. To meet this requirement an average registration process should consume less than 2 seconds. Furthermore the monitoring system should provide high robustness and reliability as the main output the attendance report is used for allow or deny the possibility to the students to absolve the specific curse. In the start-up period around 1000 students participated in the automatic attendance monitoring. The students had 8-10 lectures on a week which take place in 10 lecture room in two different buildings. An average lecture is held for 200 students. Taking into account the size of the lecture rooms a lecture can be held for maximum 500 students. As the time passes more and more students and lecture rooms will be involved in the attendance monitoring procedure. The above specification outlines a highly distributed environment where even in one lecture room the collimation of the attendance checking process is expected. Furthermore the monitoring system should provide an efficient way for implementing extra services in the future. Such a service for example could be an interface where the students can follow his/her attendance status. The system could be extended in the future by functions aiding the examination process at the university as well. This extension means services for aiding the examination registration process, aiding the student identification before examination or providing an interface where the students can examine his/her test results.

Security requirements

As pointed out earlier in this article the system should meet strict security requirements to provide a reliable attendance report. Based on this report the student are allowed to take the exam at the end of the semester a student is allowed to take the exam and complete the curse only if he appeared at more than a predefined percent of the lectures. To meet this goal the following major requirement groups were identified which the system should satisfy.

Reliable identification: The system should accept identification and register the presence only if the student is personally present. To meet this requirement the system should prevent that one can register on behalf of another student or more students. As the students may be interested in misleading the system it may be a student's interest to register his presence at a lecture in the system without personal appearance the application of paraphrases or any transferable tokens are insufficient.

Reliable data storage and transfer: The system should provide a reliable way for storing and transferring the registration data. Especially such situations where registration data can be lost should be avoided.

Data integrity and consistency on every components: It is essential to preserve the integrity of the registration data. If the registration data becomes corrupted then the result will be inappropriate to decide whether a student is accomplished the prerequisites of a curse. Based on the requirements introduced so far we have implemented a distributed and highly autonomous system for monitoring the student's attendance at lectures present at the university.

III. IMPLEMENTATION AND RESULT

Although a number of automatic attendance solution are known, from our point of view these systems has a several bottlenecks. From the previous requirements it is clear that the contactless infrastructure should be involved in the attendance monitoring system. The contactless technology (i.e. RFID, NFC) could ensure secure and fast identification based on redistributed tags. As these tags are easily transferable among the students, an attendance system based on pure contactless technology can be easily circumvented. To eliminate the above weakness we can apply biometric identification along with the contactless technology. In our solution the personal data for biometric identification are stored distributively and serves as a binding between the appeared person and the student identifier used for registration. For biometric identification we can choose the fingerprint identification as it is wildly used and it is among the cheapest ones. Although the central storage of personal biometric data raises both procedural and legal issues these can be avoided by storing it distributively in our system the biometric identifiers are stored on the student cards. To eliminate the security risk which comes from the distributed storage, highly reliable and secure student cards are used *System architecture.*

System architecture:
The implemented system is based on a number of distributed terminals managing the registration process and a central server collecting the registration logs from the terminals and implementing the presentation layer. The third main component of our system is the NFC capable student card used for registration at a terminal.

Student card: Every student involved in the attendance monitoring gets an NFC capable student card for attendance registration at lectures. There are many types of NFC cards from a number of different vendors available on the market and we choose the card which is most secure due to its excellent safety features. In addition these cards provide services for managing multiple NFC application independently on one card. The latter feature comes in handy as we expect to implement additional NFC based services in the future. The student card contains a student identifier which is used for registering the student's presence at lecture in the attendance reports. The card can contain two different fingerprints from the student which will serve as a binding between the identifier and the real person itself. This binding prevents one from using other student's card for registration. The benefit of this approach is that no one of the components in our system stores sensitive personal data other than the student card. This eliminates the necessity of storing thousands of fingerprints in our system while the card is accepted as secure enough for storing sensitive data. The chosen card can have 4k memory that is far enough for storing the student identifier and the two fingerprints. The card personalization is done by an administrator using a special terminal. The administrator verifies the identity of the student based on the ID card. Finally the administrator sends the student card issuance event to the back office. As the penetration of NFC capable mobile equipments is continuously increasing on the market we plan to involve these equipments into our system to replace the student card in the future. Although the NFC technology utilized in our system supports the option of involvement of NFC enabled mobile phones, the replacement of cards by mobile devices is not a trivial issue. While NFC chip-sets integrated in mobile equipments supports the emulation of classical Mifare cards in the operation system layer the DesFire emulation is not commercially available yet. We should like to use both DesFire cards and mobile equipments in our system in parallel. To meet this expectation the terminals has been built and prepared to support the different NFC reading procedure. Terminal The terminal serves as the main interface between the student and the attendance monitoring system. Its main part is the graphical interface the NFC capable card reader. The student can register the attendance by waving the student card in front of the terminal. The terminal reads the student id and the fingerprints if implemented from the card and registers the event. The terminal either accepts the attendance automatically or asks the student for biometric identification. If the biometric identification succeeds the attendance became registered, in other case the student has to register himself in person at a defined checkpoint. If the student fails with the biometric identification and does not appear in person at the checkpoint it results in retaliation. The number and the locations of the terminal can be dynamically changed inside the attendance monitoring system. Each terminal works autonomously and independently from the other

ones. However the terminals have a wireless communication interface for periodically checking the timetable status on the back office and sending the attendance report. This communication channel is not considered as a permanent and reliable one. In order to resolve this problem the terminals get the timetable and identification policy once in a semester and after that it manages the attendance checking process autonomously during the given period. The timetable contains the lectures held at the specific room while the identification policy contains the rules for every lecture. These rules contain the student list and as the biometric identification is applied randomly, this rule contains the biometric identification policy as well. Every terminal in the same lecture room gets exactly the same identification policy descriptors thus if a terminal requires biometric identification form a student at a specific lecture all other terminals at the same room will require the biometric identification. Obviously after the initial distribution of the timetables and identification policies further modifications can be make on the schedule during the semester. The terminals store the attendance logs for a whole semester but when the back office is available via the communication channel it uploads the logs. The uploading procedures are initiated by the terminal periodically.

Back office: The back office generates the timetable and identification policies for the terminals and collects and stores the attendance data. Timetables contain the lecture dates for a specific terminal while the identification policy describes whether a biometric identification is required form a specific student at a specific lecture. Both the timetable and the identification policies are generated for a whole semester and distributed to the terminals before the starting. During the semester the timetables and identification policy descriptors can be modified by the back office as well. The other main role of the back office is to collect the attendance data from the terminals and generate the attendance report for the university staff. The attendance data is collected periodically every day. As the terminals has far enough storage space for storing attendance data for the whole semester, even after successful transition to the back office the attendance data remains stored on the terminal as well. After collecting the attendance data the back office generates the attendance report for every student and provides an interface for visualizing it.

IV. CONCLUSION

We have implemented the above described autonomous student attendance monitoring system at the university. The monitoring has been lunched at the beginning of the last semester involving around 1100 first year students and 8 curses in 7 different lecture rooms. The system operated during the whole semester almost without any failure. 100 students were prohibited from accomplishing certain courses. During the introduction period of the monitoring system, there was not any successful and registered attack against it. Two weeks after the installation the students accustomed to use the system properly and the registration process became an essential activity.

V. REFERENCE

[1] G. Fordos, T. Doktor, B. Benyo, and B. Sodor, "Building a contactless university examination system using nfc," in Proc. IEEE Intelligent Engineering Systems (INES), 2011 15th IEEE International Conference on, Szlov´akia, 2011, pp. 57–61.

[2] A. Vilmos, G. Fordos, B. Sodor, L. Kovacs, and B.Benyo, "The stolpan view of the nfc ecosystem," in Proc. IEEE WTS 2009, 8th Wireless Telecommunications Symposium, Prague, Czech Republic, May 2009, p. 5, paper 1569183809.

[3] B.Sodor, G.Fordos, L. Kovacs, A. Vilmos, and B. Benyo, "A generalized approach for nfc application development," in Proc of WIMA, 2010.

[4] M. D. Garris, E. Tabassi, C. L. Wilson, R. M. McCabe, S. Janet, K. Ko, and C. I. Watson, User's Guide to NIST Biometric Image Software (NBIS). National Institute of Standards and Technology, 2006.

[5] Gemalto, Worlds First: Gemalto Integrates DESFire Transport Card into NFC Mobile Phone. John Wiley & Sons, 2007.