Campus Access Control and Management System

Chapter · November 2016

DOI: 10.1007/978-3-319-27000-5_32

3 authors, including:

Nyuk Hiong Voon
Universiti Teknologi Brunei
5 PUBLICATIONS **33** CITATIONS

SEE PROFILE

Campus Access Control and Management System

Mei Jun Voon, Sy Mey Yeo, Nyuk Hiong Voon

School of Computing and Informatics,
Institut Teknologi Brunei, Jalan Tungku Link, Gadong, Brunei Darussalam.
Symey.yeo@itb.edu.bn

Abstract. Advanced centralised access control (CAC) systems are widely deployed on campuses as a means to provide security and track movements. There is concern that some campuses are not using such protective systems, hence this paper attempts to resolve this weaknesses in such institutions' by developing a simpler CAC system using the Radio Frequency (RF) and contactless smart card technologies. The scope of the developed system is not only limited to access control but also to utilise the gathered data to automate and potentially to support other processes of the institution, such as lecture scheduling and attendance tracking

Keywords: Access control, Radio Frequency, contactless smart card, multifunctional.

1 Introduction

Access control strategies have always been a necessity in university campuses. There has always been a need to limit access to sensitive areas and protect resources and assets in various scenarios and locations, including classrooms and special laboratories. Not only that, unfortunate incidents such as thefts, vandalism of campus property, cars being broken into [1], and even fatal assault case [2] had happened in local universities. This paper introduces a multifunctional centralised access control and management system using Radio Frequency (RF) and contactless smart card technologies. Campus security is the prime candidate for such technologies as the nature of campuses are easy access by a relatively high number of people in a place. The proposed system will benefit universities with no access control in place or are deploying standalone system in various strategic areas on their grounds. Standalone systems have limitations in their features and one main weakness is their ineffective ability to trace back individuals who gained access into the rooms, thus making investigations on campus grounds difficult. A background study to explore the various technologies such as barcodes, QR codes, Bluetooth, biometrics, RFID, contactless smart cards, and NFC, was carried out by reviewing relevant academic journals, papers and online technology articles. Research showed that the best possible technology to use for the implementation is the contactless smart card. The focus of this paper is to highlight the design and development of a Centralised Access Control (CAC) system for campus environment that is also capable of fully utilising its gathered data for other useful

adfa, p. 1, 2011.

tasks such as lecture attendance automation, room booking and scheduling, and real time occupancy validation.

The rest of the paper is organised as follows: Section 2 provides the background research of relevant leading technologies in today's CAC systems and their deployment in universities. Section 3 describes the research methodology. Section 4 gives an overview of the implementation of the prototype system. Section 5 identifies potentials of the developed system and Section 6 provides the conclusion.

2 Background research and related work

Ever since the concept of electronic access control system first appeared, it has been tested and implemented with various different technologies. Different approaches come with their own set of advantages and disadvantages. The following discusses prevailing technologies:

- Barcodes and Quick Response (QR) codes
  Both are technologies that require direct line-of-sight which could cause some delays especially when users have difficulty positioning the codes properly for scanning. Although they are low-cost access control solution, they are low-security technologies as the codes can be duplicated very easily.

- Bluetooth
  Several commercial products such as Kevo Smart Lock and EC Key which turn Bluetooth enabled devices into a key are already on the market. In 2014, HID Global announced the completion of a mobile access control pilot featuring Bluetooth Smart technology at Vanderbilt University [3]. The main concern of this approach is the battery consumption of the user credential. In order for users to travel fast and conveniently through the entry points, their Bluetooth are encouraged to be turned on and remain on discoverable mode at all times. This drains the battery of the mobile devices and backup plans should be considered in cases of mobile devices failure or devices running out of battery.

- Biometrics
  Biometrics provides highest form of security because it eliminates specific credential devices, thus providing access control that cannot be transferred unlike keys or cards. However, with the high security it provides, it comes with a high cost for implementation as well. Deploying biometrics for campus security in areas with large amount of users and high traffic might not be wise as its nature of authentication might cause bottlenecks at entry points.

- Radio Frequency Identification (RFID) Tags
  An increasingly prevalent technology since 1970s as the technology becomes more affordable. One of its major advantages is the fact that it does not require line of sight and is capable of high read range, therefore making it one of the best candidates for object identification and tracking. However, using RFID tags that oper-

ates at high frequency and therefore having high read range will not be able to prevent tailgating. So ideally, tags operating at low frequency (LF) would be a better choice for access control systems.

- Contactless smart card
  Contactless smart cards employ radio frequency between card and reader which requires no physical insertion of the card as reading is done by passing it along the exterior of the reader. These cards conform to the ISO14443 standard, with variations of type A, B, and C. Equipped with the memory storage and ability to encrypt make these cards an ideal option for applications that require certain level of security. Santander's smart card is an example of using contactless smart cards for secure applications in educational institutions at a large scale [4].

- Near Field Communication (NFC)
  NFC is an emerging technology that has enabled smartphones to be used as user credential. A pilot program involving the deployment of NFC in access control system was done at Arizona State University in 2011 by HID Global [5]. But the lack of standardisation among cell phone carriers, handset manufacturers and security manufacturers is the biggest obstacle to the adaptation of the technology [6].

  A brief comparison of the discussed technologies is shown on Table 1.

Table 1. Comparisons between technologies

Technology	Cost	Security	Read Range	Power consumption
Barcodes and QR codes	Inexpensive	Very low	Line of sight required	None
Bluetooth	Lower than NFC	Medium	approx. 10 m (Class 2)	High
Biometrics	Very High	Very high	Contact	None
RFID tags	Low	Low	Variable, up to 100 m	Depends on type of tag
Contactless smart card	Low	High	< 10 cm	None
NFC	Higher than Bluetooth	High	10 cm or less	Low

To date, CAC systems are already in use by many campuses around the world. These systems usually employ multifunctional contactless smart cards as user credential. Aside from serving as official ID and access cards, they provide access to other on-campus services and facilities, and are also used as electronic wallets. ONEcards from University of Alberta [7] and TigerCard from Princeton University [8] are existing examples of such applications.

There has been several research projects [9], [10] which are focused on student attendance automation, and these authors have opted for using RFID technology for the implementation. Using a technology that is only capable of providing low security and high read range locks the proposed system out from the potentials of integrating various services that might require very secure transactions in the future, such as access controls and electronic cash applications. This project furthers the scope of these works by integrating not only smart attendance automation, but also lecture and room scheduling services to a CAC system, using a different approach by emphasizing on new use of the system's gathered data.

Ononiwu and Nwaji (2012) [11] had done similar research work. Their project was done with a low frequency RFID reader with a hardware motor unit to simulate an automatic door. A time attendance management system was also developed using visual basic.Net. The management system, however, was limited to only three major functions – showing attendance, adding and deleting users. The system did not provide for higher level of access control management; the door unit grant access to any registered users in the database and was also not designed for managing multiple doors. It did not have the ability to relate attendance to lessons as well.

3 Research Methodology

The research stage of the project involves reviewing relevant academic journals, papers, technology articles as well as commercial products, to study the various technologies used to develop modern digital access control systems in order to come up with alternate design options for the proposed system. Next, a relevant university is identified to conduct a survey to gauge the interests of multifunctional student smart card and access control system on campus, as well as the possibility of integrating NFC as user credential.

The short survey, consisting of twelve questions, is designed to solicit responses from university students, as they make up the largest portion of the system's end users. It is distributed randomly and a total of eighty-five university students responded; ranging from freshmen to seniors, across all departments of ITB. The rationale for picking ITB as the study bed is due to the fact that ITB fits the profile for universities which can benefit from such a system and also due to its proximity to the author.

An analysis is then conducted upon the gathered survey responses. The findings suggested high interests in the deployment of an access control system (75.3%) and use of multifunctional student smart card (84.7%), especially in electronic cash on campus (82.3%). More than half of the students (62.4%) also think that not being able to check their own attendance online is an inconvenience. The data also revealed that 60% of the students do not own an NFC device. These findings ultimately influenced the design rationale of the final product, which is based on the contactless smart card technology.

4 Implementation

An Internet Protocol (IP) reader is installed at every entry points on the campus and all of them are connected to a TCP/IP network via LAN cables. An Ethernet switch is used to connect all of them to a host computer. By scanning a MIFARE contactless smart card at the IP reader, the host computer will decide whether to grant or deny the user's request accordingly. Aside from handling authentication processes, the host computer is also responsible for running an attendance tracker (i.e. a scheduled PHP script) daily at midnight to mark attendances for all lessons that are conducted during the day time. The web-based management system runs on an online web server so all users can gain access through the Internet.

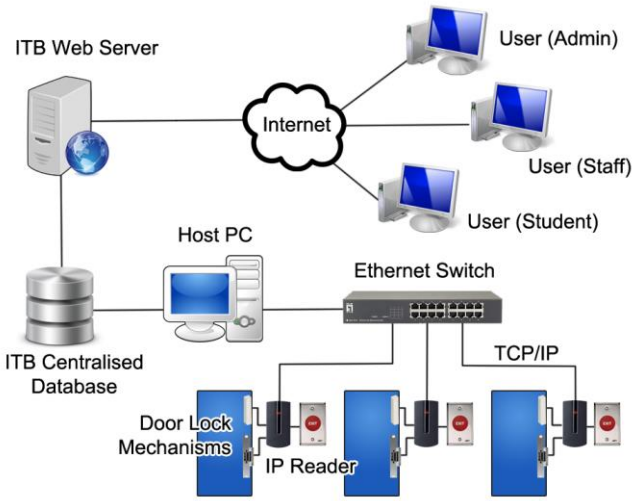

Fig. 1. Architecture Design of System for Intended Deployment

4.1 Access Control System

The access control consists of RFID reader which operates at 13.56 MHz and smart cards that conform to the ISO 14443A standard. The access control program is written in Java language and employs JDBC as middleware to facilitate the communication between the program and MySQL database when it is needed for authentication processes. The authentication processes verify that the presented card is authorised to the system, the user has sufficient privilege to enter the restricted area and the access request is made within the allowed hour of access.

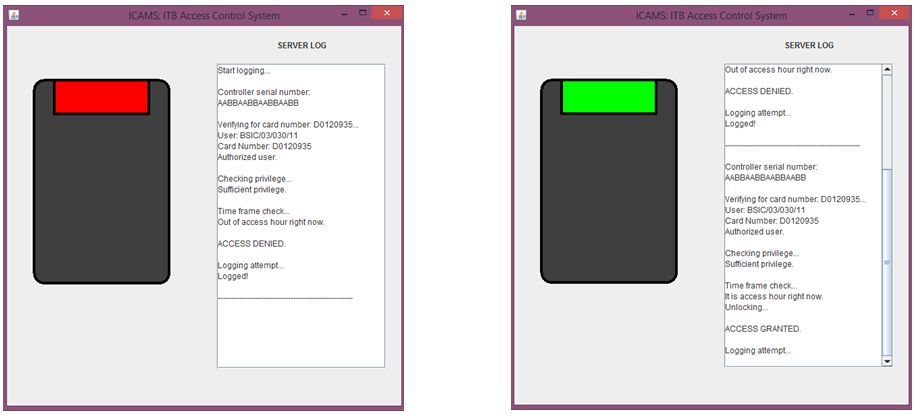

Fig. 2. Screenshot of the access control program: screen (1) shows a request denied due to request being requested outside of access hour and screen (2) shows an access request being granted because it met all the access criteria.

4.2 Features of the Management System

There are three categories of account types: - administrator, staff and student. The following describes all features available to the administrator account holders:

- Card management feature
  This feature allows staff to assign and deactivate access cards from students and staff members, as well as registering new blank cards into the system. To quicken the otherwise time-consuming card management procedures, the functions available under this feature are capable of smart and automatic card assignment or deactivation by batch. This help support high reusability of the student cards.

- Access management feature
  The purpose of this feature is to allow administrator to adjust reader's IP and access hour settings, user privileges by group or individual as well as tracking access logs.

- Semester management feature
  Administrators may provide details of the current semester (e.g. starting dates of semester breaks) as well as assigning staff members to handle lectures for modules of different courses. It is extremely important to provide these essential information accurately as these data will be used to assist auto lecture scheduling and lecture attendance tracking.

Other features include:

- Schedule Management feature (for staff accounts)
  Pre-schedules, reschedules or cancels lectures efficiently. Pre-schedule is capable of smart auto lesson scheduling for staff according to provided criteria (e.g. lecture day and number of lectures) by making use of the important semester dates provided by the administrators to avoid scheduling lessons on public holidays and semester break. Lesson schedules viewable by involved students through their personal accounts.

- Real time occupancy validation (for staff accounts)
  Allow staff to validate the occupancy of a specific location in real time, in cases of last minute cancellations of booking schedules which are not reflected in the system. Staff can also see the current and upcoming booking details of that room.

- Attendance feature (for both staff and student accounts)
  For staff, an overview of class attendance for lectures that have been conducted up-to-date is presented by each module they are teaching. The report can also be exported in Excel spreadsheet format. For student, they may view their accumulated lecture attendance for all modules they are registered in.

Fig. 3. User is requested to login at the index page (1) before they can access to the home page (2) of the system. Features that are available to the user changes accordingly to the user's account type. The administrator accounts are allowed to adjust various system settings and configurations, and perform administrative management. The staff accounts (3) are essential for schedule management. Attendance tracking for whole class and individual student are accessible by both staff and student accounts respectively.

5 Results and Analysis

Rather than implementing a specific system for attendance registration as suggested by many previous research projects [12],[13], the developed system marks attend-

ance by making use of the access logs by running the attendance tracker script the end of the day. Since the database contains all lesson schedules arranged by staff members as well as students' registered modules, the attendance tracker identifies a list of lessons that were conducted during the day before identifying the lists of students that are involved for each lesson. Then for each student, the attendance trackers tracks if they have created any access logs at the lesson venue between one hour before and after the lesson starts to mark their presence for the class. Employing an attendance tracker at the end of the day to automate attendance marking is efficient and also makes good use of the server during its most idle time because access traffic on campus would be low to almost none during midnight.

The highlight of the developed CAC system is in its infrastructure design to maximise the use of its gathered data, hence enabling its scope to reach beyond just campus security, including not only smart lecture attendance, but also room booking, validation of room occupancy, facility management, and other data possibilities; Since this is analysing data already gathered, there should be no significant operational costs increment.

Fig. 4. Data simulation of the validation of occupancy feature: User checks for real-time occupancy of lecture room 1F.25 at 8 AM. The system checks for the door ID of that room is '1' (1) and identify if there is a lesson scheduled at that time. Schedule stored in database reveals that CISWIR module is scheduled at 8 AM that day (2). System then checks for the details of the lecturer who booked the room (3), and found out that CISWIR is taught by staff with ID of '2', who goes by the name of 'Dyg Yeo Sy Mey', holding the ID card with number '44330259'. The system then proceeds to validate the immediate occupancy of the room by checking if the teaching staff member is already in the room by going through the access logs (4). In this example, the staff member has made an access at 8.06 AM to the room, and therefore the system deduces that the room is already occupied. If no access log was found, the system would deduce that the room is not occupied so it is free to be used by the requesting user.

Fig. 4 illustrates the validation of room occupancy by analysing live data. Since all details of lessons (i.e. venue and time) are necessary to be kept in database to support smart lecture attendance, these data can also be used to illustrate occupancy timeslots of lecture rooms. This offers a good overview at one glance to staff members, making

room booking a more convenient process. The availability of rooms, especially laboratories equipped with special facilities, can also be confirmed in real time by the use of access logs. The system validate the occupancy by going through the access logs of a specific room to determine if the teaching staff who booked the room for the timeslot beforehand is already present at the venue. This feature would be useful in the event of any last minute lesson cancellations which are not reflected in the system.

The access logs can also be utilised to support facility management. Maintenance workers or teams (e.g. air conditioning technicians, I.T. technicians) can be given another account to distinguish them from other users of the CAC system. The system can then track when was the last visits these maintenance workers came to perform maintenance work around the campus, and remind the administrators when it is time for the next maintenance work to be scheduled.

The potential of this system can be expanded beyond the examples given above. The introduction of multifunctional student smart card also opens up opportunities for integrating other services on campus such as integration with the library management system, canteen food voucher management system, campus parking management services and e-payment management services.

The proposed system is validated by a small group of 6 students and 2 staff members. The prototype consisted of only one USB RF reader connected to a laptop which was running the Java program to simulate the door locking mechanism and log for data collection. The reader was set with the serial number that was assigned to a specific door on campus. Students were distributed with a contactless smart card and asked to interact with the system. The staff members were also asked to perform various tasks on the management system with their own accounts. Feedbacks from the testers were used as inputs to refine mainly the user interface of the system. The testing session validated that the system was performing as expected, and was able to handle the good amount of data that was collected in the database properly.

6 Conclusions

Implementing a CAC system can bring in numerous benefits to a university, including making the campus a smarter and more secure space. This paper has discussed on how to maximise the utilisation of the data gathered by a CAC system to integrate several useful features and services quite efficiently in terms of its stored data. The fact that the management system is web-based makes it very flexible as additional functions can be incorporated into the system with ease. Selecting smart cards as user credentials is not only a security strategy to reduce tailgating, but also to allow for future applications that require secure transactions. A multifunctional smart card would surely relief the burden of students and staff having to carry several different cards at the same time. The system, however, is still quite simple and therefore prone to trickeries such as proxy attendance and tailgating issues. The system could be bolstered with facial recognition and biometrics to address such weaknesses.

Acknowledgements. This paper is developed by an undergraduate (first author) from a final year project in the Bachelor of Computing, School of Computing & Informatics, Institut Teknologi Brunei.

References

1. Ismail, H. 2012. Handbag reported stolen from UBD student's car. *Borneo Bulletin*. [Online] 8th March. [Accessed: 10th July 2015]. Available from: http://www.brusearch.com/news/107443.
2. Hamit R. 2014. Students want UBD to strengthen security. *The Brunei Times*. [Online] 23rd December. [Accessed: 10th July 2015]. Available from: http://bt.com.bn/frontpage-news-national/2014/12/23/students-want-ubd-strengthen-security.
3. Security Today. 2014. HID Global, Vanderbilt University pilot uses mobile access control featuring Bluetooth smart technology. [Online]. [Accessed: 11th July 2015]. Available from: http://security-today.com/articles/2014/10/06/hid-global-vanderbilt-university-pilot-uses-mobile-access-control-featuring.aspx.
4. Santander UK. n.d. Santander smart card in the UK. *Satntander UK* [Online] [Accessed: 11th July 2015]. Available from: http://www.santander.co.uk/uk/santander-universities/smartcard.
5. HID Global. 2012. HID Global completes NFC mobile access control pilot at Arizona State University. [Online]. [Accessed: 11th July 2015]. Available from http://www.hidglobal.com/press-releases/hid-global-completes-nfc-mobile-access-control-pilot-arizona-state-university.
6. Gray, R.H. 2011. Is NFC the future of access control? [Online]. [Accessed: 11th July 2015].Available from: http://www.campussafetymagazine.com/article/nfc-the-next-step-in-access-control/P2.
7. University of Alberta. n.d. ONEcard. [Online]. [Accessed: 11th July 2015]. Available from: http://onecard.ualberta.ca/.
8. Princeton University n.d. Welcome to Tigercard! [Online]. [Accessed: 11th July 2015]. Available from: http://www.princeton.edu/tigercard/.
9. Saparkhojayev, N. and Guvercin, S. 2012. Attendance Control System based on RFID-technology. *International Journal of Computer Science Issues*. **9** (3). pp.227-230.
10. Patel, R., Patel, N. and Gajjar, M. 2012. Online Student's Attendance Monitoring System Classroom Using Radio Frequency Identification Technology: A Proposed System Framework. *International Journal of Emerging Technology and Advanced Engineering*. **2** (2). pp.61-66.
11. Chiagozie, O.G. and Nwaji, O.G. 2012. Radio Frequency Identification (RFID) Based Attendance System with Automatic Door Unit. *Academic Research International*. p.163-182.
12. Arulogun, O.T., Olatunbosun, A., Fakolujo, O.A. and Olaniyi, O.M. 2013. RFID-Based Students Attendance Management System. *International Journal of Scientific & Engineering Research*. **4** (2).
13. Man, M. and Law, Y.K. 2007. TITO: Utilizing MYKAD Touch N Go features for Student Attendance System. *Proceeding of 1st International Malaysian Educational Technology Convention 2007*. pp.114-120.