Optimizing and Implementation Contactless Tag-Reader System for Smart Classroom and Laboratory Access

Rida Ariyanti¹, Elyas Palantei², Intan Sari Areni³
1,2,3 Electrical Engineering Department, Hasanuddin University, Makassar, Indonesia

E-mail: ridaariyantizainal@gmail.com, elyas_palantei@unhas.ac.id, intan@unhas.ac.id

Abstract. Advances in wireless technology support smart card technology became contactless technology. Wireless technology allowed users to access or controlling. However, existing contactless smart cards have limited coverage with low security levels. Therefore, this research perform optimization on user access further with better security assurance. This research implemented in classroom and laboratory access. Hardware that used consists of Smart cards and Raspberry Pi that serves as a host and card reader that could be interconnected with the microprocessor. On the smart card stored user data (registration number and name) and on the Raspberry server stored user data that could access the class or laboratory. User’s data on smart cards were stored on chips that act like RAM (Random Access Memory). The chip was embedded in the Smart card in the same function as storage media. Raspberry that had function as server and microprocessor that provide access to registered users. This study produced classroom access system by using smart card with distance > 5cm with automatic access system for user registered on system. It was according to this research proposed about security and historical data. Reader in this research use wireless transmission system. Historical data stored on the server (Raspberry pi) which records the time in and out, and the duration of time while in the room. Additional technology in the classroom access system is equipped with an automatic door close system for double security in the classroom. The advantages of this system was using server and microcontroller in one package so that in terms of cost is cheaper than the smart card access technology available today.

1. Introduction

Smart cards were cards with chips as data storage that can be used for network access systems, storing values and other data[1]. Smart card technology were supported by the advancement of wireless communication technology made smart cards became contactless to facilitated user in access or controlling. Open data transmission over a wireless system process have a security challenge, namely user authentication and privacy [2]. Previous research on contactless smart cards focused on file access for printing data and evaluation in tags [4], [5], which then developed file access on cloud storage systems [6] but there was no guarantee of user safety. Research then develop in 2016 to ensure the security of data with remote systems and used dynamic (changing) ids and remote servers verify the legitimacy of users through open and unsafe communication channels [8]. The research has focused on authentication but has not access the system by using microcontroller. Therefore, the
authors do research that implemented in everyday life in the academic field, namely access
classroom and laboratory. Classroom and laboratory access systems that use smart cards with
optimizations at a range of objectives to enable users for access with an high-class security
algorithm, which is an automatic closed door. The host computer (in research using Raspberry)
and card reader can be interconnected with the microprocessor [3].

The structure of this paper is related research on part 2. The system model presented in the next
part 3 of the results is discussed in part 4 and finally the conclusions in part 5.

2. Related works
The researches and implementation of smart cards has grown from year to year. Previous research had
been conducted using contactless and IC smart cards as a medium for identity authentication,
analyzing conditions and ways for cloud print systems, and researching key printer driver technology,
data encryption, identity authentication to print centers by Wu Yun [4].

Another research was focused on smart cards with contactless interfaces. Using Mifare DESFire
able to found some weakness of smart card that can cause vulnerability if protocol were not
implemented properly. This method can be used by researchers to evaluate the security of protocol
implementation on some types of smart cards [5]. Another research about Unified RB-DAC
method Approach With Secure Authentication Using Smart Card Architecture for file access on
cloud computing using smart cards. RBAC was a system where all users could access the specified
data for a particular need, but can not specify the data allocation for each user. The RABC system
incorporates the ACL (Access Control List) & ACM (Access Control Matrix) concept of the
DAC with RBAC to improve the integrity of data in RBAC. Thus to achieve this, ACLs were add
for all objects (data) and ACM for all objects in the system [6]. Related research Authentication of
remote users with mechanisms by which servers verify the legitimacy of users through open and
unsecured communication channels. The Password authentication using smart cards has become
one of the commonly adopted methods for password protection during transmission by Zhengxian
Gao, et al. [7].

Based on the previous research, this research was an optimization. Previous research had
evolved using smart cards with contactless reader, but with limited distance and low
security. The Improvement in this research was using the server and mikrokontroller in one
package. In the field of academics, classroom or laboratory security is very important, so the system
was develope by adding applications for the history user who uses the room, hours of entry, hours out
and duration of users are in the room.

3. System Model

3.1. System Design
Raspberry Pi is a micro module computer that has a digital output port input such as microcontroller
board. Excess Rasberry Pi compared to other microcontroller board that has a port / connection for
display in the form of TV or PC Monitor, USB connection for Keyboard and Mouse and has 26 pin I /
O digital [8].
**Figure 1.** Algorithm Classroom and Laboratory Access

| Function | Pin Number | Pin Number | Function |
|----------|------------|------------|----------|
| 3.3 V    | 1          | 2          | 5 V      |
| 12C0 SDA | 3          | 4          | DNC      |
| 12C0 SDL | 5          | 6          | GROUND   |
| GPIO 4   | 7          | 8          | UART TXD|
| DNC      | 9          | 10         | UART RXD|
| GPIO 17  | 11         | 12         | GPIO 18  |
| GPIO 21  | 13         | 14         | DNC      |
| GPIO 22  | 15         | 16         | GPIO 23  |
| DNC      | 17         | 18         | GPIO 24  |
| SP10 MOSI| 19         | 20         | DNC      |
| SP10 MISO| 21         | 22         | GPIO 25  |
The Function of GPIO in Raspberry

| Function     | Pin Number | Pin Number | Function     |
|--------------|------------|------------|--------------|
| SP10         | 23         | 24         | SPC10        |
| SCLK         |            |            | CE 0 N       |
| DNC          | 25         | 26         | SPC10        |
|              |            |            | CE 1 N       |

Room access system has several steps in development, namely:

- Input the information on a smart card (name, student/teacher identification number).
- Entry of a data base on the server which users can access which consists of the name and identification number.
- Access system programming with the detail time in, time out, duration. It proposed to accessing historical data can be displayed on screen. As a microcontroller, Raspberry was connected to the solenoid then the door can automatically open when the authentication process were completed.

GPIO pins can be configured as inputs. Connection of GPIO to a voltage higher than 3.3V was destroy GPIO blocks in SoC [9]. In addition to the input output on some pins GPIO has functions as serial communication such as I2C, SPI and serial communication UART [10].

3.2. System testing

The Figure 1. shows the Algorithm on classroom and laboratory access systems. Users who had been registered on the system and stored on the server access by using tag on the reader. Further authentication process whether the user can access or not. In accordance with the programmed procedure, if the user were not registered, the door would not open and there was a warning that the user were unidentified. Meanwhile, if the user were registered, the door that uses a selenoid and connected to the microcontroller / Raspberry will automatically open.

Figure 2. Testing System Diagram
Figure 2 shows a system test consist of 3 test scenarios were measuring the tag distance on the reader, the access system of the room where the moment after the user accessed the room, the door would be closed automatically. The last scenario was accessing historical data stored on the server. The data in the form of time in, time out and duration of users were in the room. This allowed the administrator or Person in charge to monitor the room. The security of the room will be ensured with additional features that automatically close the door when the user takes too long to enter the room.

4. Formatting the text

The system testing process were verifying the distance between the reader and the tag.

Figure 3. Accesses denied

Figure.3 shows system testing that users who did not have access to the system will not enter the room and the door will not open.

Figure 4. Accesses denied
Figure 4 shows system testing that users who have access to the system will enter the room and the door will open. Based on the proposed concept of this research, the access room system using the tag is shown in Table 2.

| Distance (cm) | Readable by System | Not Legible by System | Door open (Yes / No) |
|---------------|--------------------|-----------------------|---------------------|
| 0.5           | √                  | -                     | Yes                 |
| 1             | √                  | -                     | Yes                 |
| 1.5           | √                  | -                     | Yes                 |
| 2             | √                  | -                     | Yes                 |
| 2.5           | √                  | -                     | Yes                 |
| 3             | √                  | -                     | Yes                 |
| 3.5           | √                  | -                     | Yes                 |
| 4             | √                  | -                     | Yes                 |
| 4.5           | √                  | -                     | Yes                 |
| 5             | √                  | -                     | Yes                 |
| 5.5           | √                  | -                     | Yes                 |
| 6             | -                  | √                     | No.                 |
| 6.5           | -                  | √                     | No.                 |
| 7             | -                  | √                     | No.                 |

In access distance tested the distance of tag to reader as shown in Table 2. Explains that the system could be accessed with a maximum distance of 5.5 cm. The 100% security class system works by denying access for unregistered users.

Additional applications on this system were historical data about time in, time out and duration of users in the room can be recorded on the server. Thus, when needed the data can be accessed from the server. This is very important considering the security of the room such as classes and laboratories need a special security system. Thus, the optimization of the system related to the security of the room is added to the closed door automatically system algorithm when the user has authenticated.

5. Future research direction and Conclusion
The function of the reader in reading the tag, works well on the reader reading distance to the tag can reach 5.5 or > 5 cm. Software testing shows the system works based on proposed where the user registered on the system will be able to access the room and the door opens automatically. If the authentication process fails / the user is not registered, the door will not open and the access warning appears rejected. As the advantages of this system, data stored on the server in the form of historical time in time out, long in the room and logs of users who access can be seen on the display / monitor server. Future research will be done about detecting users within 100 m of the reader.
Acknowledgments
This research support by Cyber Tech Community, Electrical Engineering of Hasanuddin University.

References
[1] M. Wassim Raad, Tarek Sheltami, M. Sallout, “A Smart card Based Prepaid Electricity System”, IEEE [Pervasive Computing and Applications, 2007. ICPCA 2007. 2nd International Conference].
[2] Alavalapati Goutham Reddy, Eun-Jun Yoon, Ashok Kumar Das, Kee Young Yoo, “Lightweight Authentication With Keyagreement Protocol For Mobile Network Environment Using Smart Cards”, IEEE [The Institution of Engineering and Technology 2016].
[3] Agnes C. Noubissi, Julien Iguchi-Cartigny, Jean-Louis Lanet, “Hot Updates for Java Based Smart cards”, IEEE, 2011 [ICDE Workshops].
[4] Wu Yun, “Research of Cloud Print Key Technology Base on Identity “. IEEE, 2012 [Third World Congress on Software Engineering].
[5] Matej Kacic, Petr Hanacek, Martin Henzl, Ivan Homoliak, “A concept of behavioral reputation system in wireless networks”, IEEE, 2013 47th International Carnahan Conference on Security Technology (ICCST).
[6] B. Linkesh, S.Durga, E. Chowdary, Unified RB-DAC Approach With Secure Authentication Using Smart card Architecture, IEEE [2014 3rd International Conference on Eco-friendly Computing and Communication Systems].
[7] Shanu Gaharana, Darpan Anand, “Dynamic ID Based Remote User Authentication In Multi Server Environment Using Smart cards: A Review”, IEEE, 2015, International Conference on Computational Intelligence and Communication Networks (CICN).
[8] Zhengxian Gao, Shou Hsuan Stephen Huang, Wei Ding, “Cryptanalysis of Three Dynamic ID-Based Remote User Authentication Schemes Using Smart cards”, 2016, IEEE International Conference of Online Analysis and Computing Science (ICOACS).
[9] Qihao He; Bruce Segee; Vincent Weaver, “Raspberry Pi 2 B+ GPU Power, Performance, and Energy Implications”, IEEE, 2016 International Conference on Computational Science and Computational.
[10] Vamsikrishna Patchava, Hari Babu Kandala, P Ravi Babu, “A Smart Home Automation technique with Raspberry Pi using IoT”, IEEE, 2015, International Conference on Smart Sensors and Systems (IC-SSS).