

SECURITY ACCESS CONTROL SYSTEM BASED ON
RADIO FREQUENCY IDENTIFICATION (RFID) AND
ARDUINO TECHNOLOGIES

AMMAR FAEZ BIN MOHAMAD AZUDIN

BACHELOR OF COMPUTER SCIENCE

UNIVERSITI MALAYSIA PAHANG

AMMAR FAEZ BIN MOHAMAD AZUDIN

BACHELOR OF COMPUTER SCIENCE

UNIVERSITI MALAYSIA PAHANG

UNIVERSITI MALAYSIA PAHANG

DECLARATION OF THESIS AND COPYRIGHT

Author's Full Name : **AMMAR FAEZ BIN MOHAMAD AZUDIN**

Date of Birth : **13 SEPTEMBER 2018**

Title : **SECURITY ACCESS CONTROL SYSTEM BASED ON
RADIO FREQUENCY IDENTIFICATION (RFID) AND
ARDUINO TECHNOLOGIES**

Academic Session : **2017/2018**

I declare that this thesis is classified as:

- CONFIDENTIAL (Contains confidential information under the Official Secret Act 1997)*
- RESTRICTED (Contains restricted information as specified by the organization where research was done)*
- OPEN ACCESS I agree that my thesis to be published as online open access (Full Text)

I acknowledge that Universiti Malaysia Pahang reserves the following rights:

1. The Thesis is the Property of Universiti Malaysia Pahang
2. The Library of Universiti Malaysia Pahang has the right to make copies of the thesis for the purpose of research only.
3. The Library has the right to make copies of the thesis for academic exchange.

Certified by:

(Student's Signature)

(Supervisor's Signature)

950913-12-5297
New IC/Passport Number
Date:

Dr Mohammed Falah Mohammed
Name of Supervisor
Date:



SUPERVISOR'S DECLARATION

I hereby declare that I have read this thesis and in my opinion this thesis/report is sufficient in terms of scope and quality for the award of the degree of Bachelor of Computer Science (Graphics & Multimedia Technology)

(Supervisor's Signature)

Full Name : DR MOHAMMED FALAH MOHAMMED

Position :

Date :



STUDENT'S DECLARATION

I hereby declare that the work in this thesis entitled “SECURITY ACCESS CONTROL SYSTEM BASED ON RADIO FREQUENCY IDENTIFICATION (RFID) AND ARDUINO TECHNOLOGIES” is the result of my own research except as summaries and cited which have been duly acknowledged.

(Student's Signature)

Full Name : AMMAR FAEZ BIN MOHAMAD AZUDIN

ID Number : CD15029

Date :

SECURITY ACCESS CONTROL SYSTEM BASED ON
RADIO FREQUENCY IDENTIFICATION (RFID) AND
ARDUINO TECHNOLOGIES

AMMAR FAEZ BIN MOHAMAD AZUDIN

Thesis submitted in fulfilment of the
requirement for the award of the degree of
BACHELOR OF COMPUTER SCIENCE (GRAPHICS & MULTIMEDIA
TECHNOLOGY) WITH HONOURS

Faculty of Computer System& Software Engineering
UNIVERSITY MALAYSIA PAHANG

JUNE, 2018

ACKNOWLEDGEMENTS

First and foremost, Alhamdulillah for all His blessing for giving me patience to complete my project successfully. I am also would like to thanks to my supervisor, Dr Mohammed Falah Mohammed for his encouragement, guidance and help in making this project possible. Besides, I also would like to express my appreciation towards my parents Mohamad Azudin bin Hussain and Rashadah binti Idris, family, not forget to my friends who have always been my supporter in order to finish my project titled “Security Access Control System Based On Radio Frequency Identification (RFID) And Arduino Technologies”.

I am very grateful towards all the lecturers of Faculty Computer Science and Software Engineering (FSKKP) who has been directly or indirectly helped me to prepare this proposal.

ABSTRACT

In this project, a study on the latest technologies that can be used to generate an automatic access control has been done. The aim was to create an automatic door access control system in order to solve the manual door access problem at Kolej Kediaman 2. Based on study and investigation, as mentioned in the literature review, Radio Frequency Identification (RFID) technology is chosen to be used in this proposed system based on Arduino. The RFID is an alternative technology with a potential that can replace the traditional manual door access. By using RFID technology and Arduino, the proposed system will enable students to automatically access the room using their ID card. Besides, this system also comes with warning SMS notification's feature using GSM Modem. The advantage of the proposed system is to avoid intruders from entering owner's room without owner's permission. The system has been tested and show the ability to solve the manual door access control problems.

ABSTRAK

Dalam projek ini, satu kajian mengenai teknologi terkini yang boleh digunakan untuk menghasilkan kawalan akses automatik telah dilakukan. Tujuannya adalah untuk mewujudkan sistem kawalan akses pintu automatik untuk menyelesaikan masalah akses pintu manual di Kolej Kediaman 2. Berdasarkan kajian dan penyiasatan, seperti yang disebutkan dalam kajian literatur, Teknologi Pengenalan Frekuensi Radio (RFID) dipilih untuk digunakan dalam sistem yang dicadangkan ini berdasarkan Arduino. RFID adalah teknologi alternatif dengan potensi yang dapat menggantikan akses pintu manual tradisional. Dengan menggunakan teknologi RFID dan Arduino, sistem yang dicadangkan akan membolehkan pelajar mengakses bilik secara automatik dengan menggunakan kad ID mereka. Selain itu, sistem ini juga dilengkapi dengan ciri pemberitahuan SMS amaran menggunakan Modem GSM. Kelebihan sistem yang dicadangkan adalah untuk mengelakkan penyerang memasuki bilik pemilik tanpa izin pemilik. Sistem ini telah diuji dan menunjukkan keupayaan untuk menyelesaikan masalah kawalan akses pintu manual.

TABLE OF CONTENT

DECLARATION	
TITLE PAGE	
ACKNOWLEDGEMENTS	ii
ABSTRACT	iii
ABSTRAK	iv
TABLE OF CONTENT	v
LIST OF TABLES	viii
LIST OF FIGURES	ix
LIST OF ABBREVIATIONS	xi
CHAPTER 1 INTRODUCTION	1
1.1 INTRODUCTION	1
1.2 PROBLEM STATEMENT	4
1.3 OBJECTIVES	4
1.4 SCOPE	5
1.5 THESIS ORGANIZATION	5
CHAPTER 2 LITERATURE REVIEW	6
2.1 INTRODUCTION	6
2.2 EXISTING SYSTEMS	6
2.2.1 Vandal Resistant Slim Reader	6
2.2.2 UNIPASS-The Simple, Efficient Access Control Solution	8
2.2.3 DR2-Standalone Card and Pin	11
2.3 COMPARISON EXISTING SYSTEMS	13

2.4	SUMMARY	15
CHAPTER 3 METHODOLOGY		16
3.1	INTRODUCTION	16
3.2	RAPID APPLICATION DEVELOPMENT METHODOLOGY	17
3.3	ACTIVITIES IN THE RAD METHODOLOGY	18
3.3.1	Requirement Planning Phase	18
3.3.2	User Design Phase	19
3.3.3	Construction Phase	21
3.3.4	Cutover Phase	22
3.4	SOFTWARE DESIGN DOCUMENT	22
3.4.1	Flow chart	22
3.4.2	Context Diagram	24
3.4.3	Use Case Diagram	25
3.5	HARDWARE AND SOFTWARE	26
3.5.1	Hardware	26
CHAPTER 4 RESULTS AND DISCUSSION		35
4.1	INTRODUCTION	35
4.2	MODEL IMPLEMENTATION	35
4.3	THE IMPLEMENTATION OF CODING AND TESTING	40
4.4	RESULTS AND DISCUSSION	46
CHAPTER 5 CONCLUSION		48
5.1	INTRODUCTION	48
5.2	PROJECT CONSTRAINT AND CHALLENGES	48

5.3	FUTURE WORK	49
	REFERENCES	50
	APPENDICES	52

LIST OF TABLES

Table 2.1	A Comparison Between The Different Systems	14
Table 3.1	The Specification of Arduino UNO 3	27
Table 3.2	The Specification of MIFAIR RC522	30
Table 3.3	The Specification of 12VDC Solenoid Electromagnetic	31
Table 3.4	The Specification of Ethernet Shield	33
Table 3.5	The Specification of SIM900a GSM Modem	34
Table 4.1	Connected pins	39

LIST OF FIGURES

Figure 2.1	DM1 Installation Diagram (Soyal, DM1 Door access package, 2016)	8
Figure 2.2	Process of UNIPASS (IDtech, 2016)	10
Figure 2.3	DR2 Installation Diagram (Soyal, DR2 Door access package, 2016)	12
Figure 3.1	Rapid Application Development (RAD) Diagram	17
Figure 3.2	Process of RFID	19
Figure 3.3	Flow Diagram of Security Access Control System	21
Figure 3.4	Flowchart of the Security Access Control System	23
Figure 3.5	Context Diagram	24
Figure 3.6	Use Case Diagram of Security Access Control System	25
Figure 3.7	Arduino UNO	26
Figure 3.8	MIFAIR RC522 RFID Reader	28
Figure 3.9	Solenoid 12VDC Solenoid Electromagnetic	30
Figure 3.10	Single Relay Module	32
Figure 3.11	SIM900a GSM Modem	33
Figure 4.1	Arduino and GSM Modem	36
Figure 4.2	RFID and Arduino Circuit	37
Figure 4.3	Connection of Relay, Solenoid, and Power Supply	38
Figure 4.4	Complete Circuit and Design	39
Figure 4.5	Arduino Software IDE	40
Figure 4.6	Codes to Generates Notification	41
Figure 4.7	Codes for Relay	42
Figure 4.8	Main Code	45
Figure 4.9	Result in Logical Side	46

LIST OF ABBREVIATIONS

ABBREVIATION	TITLE
KK2	Kolej Kediaman 2
RFID	Radio Frequency Identification
SMS	Short Message Service
RAD	Rapid Application Development
IDE	Integrated Development Environment
LED	Light Emitting Diode
LAN	Local Area Network
CCTV	Closed Circuit Television
CAC	Common Access Card
PIN	Personal Identification Number
AC	Alternating Current
DC	Direct Current
GSM	Global System for Mobile
ID	Identification
USB	Universal Serial Bus

CHAPTER 1

INTRODUCTION

1.1 INTRODUCTION

Nowadays, the living cost of the citizens is increasing in tandem with the improvement of technology and economy. Therefore, some people tried several ways in order to secure their life even though sometimes it violates national regulations and norms of life. Based on that, the security level of many human life's aspect have been improved that covers different topics including personal security for example Mini Foaming Defence Spray UK (UK, 2014). This security product is designed for females to defence them if they got confronted. They just need to spray out to the attacker's eyes and then they got time to get away from the attacker.

Besides, there is also car security like Viper LCD 2-Way Security System. This system has 2-way security which protect the vehicle. The electronic technologies used in this system including Stinger® DoubleGuard® shock sensor, Revenger® six-tone siren and Failsafe® Starter Kill (Viper, 2009). For home security there is an example of system which is Vivint Smart Home. The system works when there is fire, smoke, or carbon monoxide that can threat house owner's life. User are just need to click a one-touch callout button on the control panel then it will automatically direct contact with monitoring teams (Vivint, 2012).

Even in university residential college also have security system. For example, in University of Yale, there is central alarm station that provides 24-hour monitoring of the University's integrated security system such as fire, burglar, duress alarms, and video. The central alarm station also receives request for security services likes residential college alarms (University, 2006).

Therefore, many organizations come out with different technology of authentication and security to meet regulatory demands of compliance. For example, IDtech company release UNIPASS Access Control System which a security system for door's access. The system used a biometric technology which is fingerprint recognition access control system (IDtech, 2016). Another existing system is DR2-Standalone Card and Pin. The system which is released by Soyal's company is build for accessing the door that used both card and PIN. The technology used is Radio Frequency Identification (RFID) (Waxton, 2016).

Based on these two systems, there is different in technology used. Each technology has their advantages and disadvantages. Biometric technology used only for user's biometric identification for example fingerprint, eyes and voice recognition and on the other hand RFID technology used for recognition of user's cards or tags. Although there is various optional authentication, the focus of this work will be on RFID (Radio-Frequency Identification) technology which more user convenience that provides better authentication. The reason why RFID technology is chosen because users do not have to bring a key with them anymore and the problem of missing key also can be solved. Another reason why RFID technology is chosen because it has large capacity which can store many of users and codes (Astc, 2016).

Radio Frequency Identification (RFID) is a technology that uses radio waves in order to identify individual items automatically. The objective or function of RFID system is basically to carry data in transponders for example a tags and then it will retrieve data (Pandey, 2016). Nowadays, the technology of RFID is one of the most technologies that being accepted by the industry. RFID technology is commonly used a method which are storing a serial number and other information on a microchip that has antenna attached. The components of typical RFID are including at least three components which are an antenna, transceiver, and transponder (tag) (Rouse, 2006). In RFID technology, there is a reader that uses the radio frequency signal to tracking tags. Next, the information will sends by the reader to the end user by client software. This client software basically embedded in the microprocessor (Ishabakaki, 2015).

RFID technology currently have been applied in many aspect of life in different applications for example in library system to improves the efficiency of circulation operations and also to enhance the process of individual's checkout and check-in

(Thrasher, 2013), storage system to track the returnable items (Långström, 2013), attendance system to record the data when the employee enter or exits the office and calculate the total of person staying in the office by using an RFID card (Chudasma, 2014), as well as, in access control system which is cover different areas like Biometric Access Control System Proximity Access Control System (Agarwal, 2012). The focus of this work is on the security door access control system.

The other component that used in this project is Arduino. Basically, Arduino is known as an open-source platform that used specially for developing various kind of electronics projects. Arduino can be divided to two things which is consist of a physical programmable circuit board and a piece of software which is called IDE (Integrated Development Environment) that function on computer. The computer code is wrote and upload to the physical board by using this IDE (Arduino, 2003). The Arduino IDE (Arduino program's name) contains an editor that able us to write sketches in simple programming language. It will convert to C language and then compiled using avr-gcc. The microcontroller on the Arduino board will be able to understand and execute because this process produced binary code. First, connect the Arduino board to a computer using USB cable then IDE is used in order to compile and upload the board to the program (Fabio, 2006).

There are several systems that has been used Arduino likes Arduino Alarm System. This alarm system uses a motion sensor to detect movement and emit a high pitched tone. It also emits visual display consisting of flashing LED lights. The other one example is Arduino Light Sensor which is a device that functioning as to detect light. This system is using Light Dependent Resistor (LDR) and then will be controlled using Arduino (Administrator, 2016).

The reasons why Arduino is used in this project for example it is simple, clear programming environment. For beginner, it is easier to use the Arduino software (IDE), as well as, it is good cross-platform device as the IDE able to runs on typical operating systems such as Linux, Macintosh OSX and Windows. In addition, Arduino boards are relatively inexpensive compared to other microcontroller platforms as it can reduce the cost of materials while completing this project (Arduino, 2003).

In this project, the RFID reader module uses the SPI protocol for communication with the Arduino board. The Arduino board need to connect with the RFID reader module then the coding process will take place in Arduino IDE software in order to connect the RFID with Arduino. This Arduino IDE contains all the software which will run a computer in order to program and communicate with an Arduino board (Mukherjee, 2016).

1.2 PROBLEM STATEMENT

Nowadays, there are many students who stay in residential college complaints that the security level of their room or house is not very satisfied. This is due to the theft case that often happens for example in Kolej Kediaman 2. One of the factor why this incident keep occur is because lack of security of door's access control. The manual access door that currently used in college is actually not really secure as they are easily broken into. Besides, students need to carry around those keys and sometime the keys will likely to be lost. Other problem while using manual door access is students need to store a duplicate or spare key somewhere on their property like many homeowners currently do. However, this method still does not guarantee safety as most criminals are used to looking around to find a spare key. In addition, the quality of the door knob is low of usability and easy to be damaged by others. Lastly, there is no unique identification of the user for each of the door knob on manual door access.

1.3 OBJECTIVES

The aim of this project is to design a secure automatic door access system for Kolej Kediaman 2. While the objectives are

1. To study and analyse the current control access system.
2. To propose an automatic control access system based on Arduino and Radio Frequency Identification (RFID) technologies.
3. To further enhance security level of system by triggering SMS to the owner using GSM Modem.

1.4 SCOPE

The scopes for this project are:

1. The system is developed for residents in Kolej Kediaman 2 Universiti Malaysia Pahang.
2. The user need a mobile phone to receive the notifications from the GSM Modem.
3. The GSM modem must attached with sim card that already reloaded with credit to trigger a notification message.
4. The warning notification will automatically send to the owner of the room.

1.5 THESIS ORGANIZATION

Chapter 1 is discuss in the introduction of the project. In this chapter will shows a rough overview about the RFID concept and why the system is going to purposed. Moreover, in this stage, the problem statement, objective and scope of the entire project are defined here.

Chapter 2 is discuss on Literature review in the 3 existing systems. Then will brief about the problem that Kolej Kediaman 2 facing and will brief about the proposed system.

Chapter 3 is discuss about the flow of the system process and the selected methodology that will be used in this project. On the other hand, the software and hardware specification also will explain here in more details. Besides, the flowchart, use case digram also explained here.

Chapter 4 is show about the development of the project. Besides, this chapter also will describe about the steps of the system implementation. The testing and coding implementation will be elaborated here.

Chapter 5 is discuss about the final result of the project. Other than that, the conclusion for entire development will be discussed here and will explain the challenges of this system.

CHAPTER 2

LITERATURE REVIEW

2.1 INTRODUCTION

Over the years, access control systems have become more and more advanced. Security access control system serves security by giving flexible control over who is allowed to enter the room. These access control systems basically invented as security purposes. Access control system recognizes authenticates and authorizes entry of a person to enter into the room. At the same time, the security of the room will ensured as it gives complete protection.

In this project, we will provide an overview of some security access control system and technology that used to improve the security process in them. There are three examples of existing systems that currently in market is studied and examined. The limitations and restrictions of these systems also will be determined here. Additionally, after finding all the limitations on these systems, the results obtain from study could show the answer to find a solution to the issues that had been found. Based on the demands in terms of electronic security management is constantly evolving, the RFID technology is a solution to minimize the risk involved in authorized access to the room or building.

2.2 EXISTING SYSTEMS

In this section, a review on different security access control system belongs to different companies is highlighted. The techniques and technologies also use different types of access control systems like biometric, RFID and door controllers.

2.2.1 Vandal Resistant Slim Reader

Vandal Resistant Slim Reader or also known as DM1 is a door access control system that developed by Soyal. DM1 is a device that provides vandal resistant function and water splash proof (Soyal, DM1 Door access package, 2016). The technology used in this system is RFID technology as it used card reader as medium to access the door.

On 2 April 2015, DM1 was released under the Silver Black Series. This product was implemented with SoyalEtegra Access Control Management System that allows personnel maintenance. Besides, the product allowed users remotely the view within the LAN. Furthermore, this product give comfort to the user as the access card reader is designed with a slim body which make it easy to fit into narrow door frame. In addition, DM1 can perform monitoring and CCTV picture capturing.

However, there are some weaknesses in this product. The first problem is there is only one method to access the room at a time. For example, if users choose the card as a medium to unlock the door, then the reader will set up to read the card only. On the other hand, if the users choose the tag to be a medium to unlock the door, the reader will set up to read the tag only. Thus, at this point the card could not be used as a key anymore. Consequently, users must have in their mind first which method they want as medium to unlock the door to access the room.

The basic process on how to access the room is firstly user needs to scan their card in front of the reader. After the card is verified successfully by the reader, the electromagnetic door will automatically release the door. At the same time, a single beep will be heard as notifier to user that the card was successfully being identified. On the contrary, double beep will sound out if there is unauthorized issue because of the card is rejected by the reader. With the result that, the data from verified identity will save to the PC for record purpose. The picture below shows how the installation of DM1:

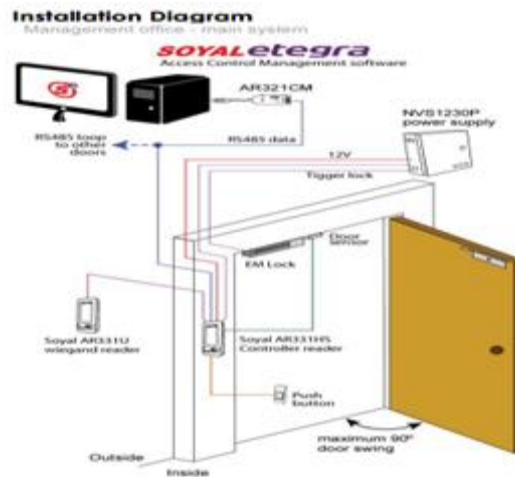


Figure 2.1 DM1 Installation Diagram (Soyal, DM1 Door access package, 2016)

2.2.2 UNIPASS-The Simple, Efficient Access Control Solution

UNIPASS Access Control System developed by IDtech company is a product or system that capable to identify a person, time based on the situation under circumstances for an unlimited of people. This system is customized based on the user requirements. Basically, UNIPASS is an access control system that using biometrics technology (IDtech, 2016). Recognition technology that implemented in this systems is a fingerprint recognition access control system. In this system, user able to allow and set the validation of the authorized tags based on predefined zones and time. The authorization of the system usually according to the peoples timetables and days. In addition, the advantage of UNIPASS is still can be incorporated in offline state. It also can be accessed by an unlimited number of sites, controllers, reader and credential holders.

There is different type of authentication recognition technology recently. For this UNIPASS system, a biometric authentication is used as recognition that determined the authority of the users depend on user behavioural characteristic or specific physiological. Fingerprint recognition can be divided into two modules which are identification module and verification module.

Enrollment phase is present in this system as to enroll individuals in the biometric system. User must go through the enrollment phase to complete these two modules. In the enrollment phase, the individual's biometric characteristic will be scanned using

fingerprint scanner in order to get the input from user. Next, the process of identification and verification will take place. The identification or also can be called authentication process is about to identify who is the user and at the same time used to establish user's identity. Conversely, verification process is about to affirm identity of user. Hence, there is two major process which are used to accepting and rejecting the user's identity. So, the biometric system process need to starts with enrollment after that followed by identification and verification process. In the enrollment phase, user will scanned their characteristic using biometric reader for getting a raw digital data. To facilitate matching, the raw data will processed by feature extractor in order to generate a compact but costly representation, also called as template.

Enrollment : This phase function as to recognize a specific person. User must have identity card then the biometric will link to identity specifies on the identification document. The next step is user needs to provide their biometric characteristics for instance iris, hand or fingertips to acquisition device. Then, the distinctive features will be located and the samples are extracted and encoded. Later, it will be stored as template for comparison in the future. Generally, there is various ways in collecting biometric sample. For example, collected it as an image or maybe recording. Template normally based on the technology. Besides, generation of a template are also influenced by distance, pressure, minute changes in positioning, environment and other factor.

Identification : In this phase, the identification of user will occur here. The process runs by comparing the trial template with the stored reference template in order to find a match. This identification process is declared as one-to-many matching because the user's biometric will be compared with others multiple biometric templates in the database. Currently the two types of identification system available are positive and negative which are the positive one is about to make sure that the biometric characteristic is already enrolled in the database. The expect result for this search is there is a match. The other one which is negative identification systems are used as to ensure that an individual's information is not exist in a database. The results expectation for this search is a no match.

Verification : In this phase, the verification is used to verify that an individual is claiming to be. After the users provide an identifier, then the biometric characteristic is

presented, generating a trial template that is based on an algorithm. Then, the trial template will be compared with user's reference template that already exist in the system in enrollment phase before. This process function as identify whether the template is matched or mismatched. Contrary to identification method, verification was referred as one-to-one matching. The figure 2.2 below is the process of UNIPASS.

Biometric technology also has its own limitation. If the user's finger have sweat or injured, it will hard for biometric reader to do the identification. In addition, the system can make mistakes with the dryness or dirtiness of the finger's skin. This is because the system cannot read the finger's information due mismatch with exist information that stored in the system.

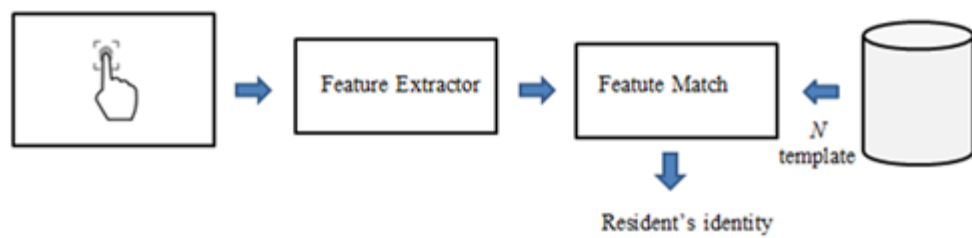


Figure 2.2 Process of UNIPASS (IDtech, 2016)

2.2.3 DR2-Standalone Card and Pin

CAC which is also known as Common Access Card is a card that similar like credit card based on their size. This smart card is used for allowing rapid authentication and also serve high security for all type of access. With installing secure CAC application, it can access the information stored. In addition, a Personal Identification Number (PIN) also needed in order to access the stored data with system access to the secure CAC.

If the person has authorized to the system, then he can perform an identification process. The example is like only the person who has authorized is allow to access or review the information data in the card if the card contains user's information. Besides, the CAC technology give safety features for example sound criteria for personnel identification and also resistance to exploitation and identity deception. Despite that all positive criteria, there is still some lacking that can be found in the system for instance the chip may be get damaged and the card might be lost.

A PIN is a number allocated to an individual and used to validate electronic transactions. On the other word, it also known as password. It connect user and the system for authentication. The DR2 system is not allow a pin number embedded in the card but the pin is only entered manually by user or owner of the card (Soyal, DR2 Door access package, 2016). Nowadays there is a lot of usability of PIN like bank transaction, log in to restricted website, internet transaction and of course for door access too.

While using PIN system, user needs to enter the PIN first then the device or a system can be used. Usually password or pin contain different type of characters including numbers, letters or symbols that can be range of 12 to 14 characters. The higher the password length the higher the level of security. However, if users are using password for their door access card, it will burden them as they need to remember the password which are contain multiple characters.

This DR2 Access Control System which produced by Soyal company is released on 1 May 2009 (Soyal, DR2 Door access package, 2016). The system is build for accessing the door that used both card and PIN. DR2 system is very famous among user as it is low budget application. This DR2 product is recommended for user who want to

install auto access control to their door as it was designed to allow high security function but cost effective.

The process of accessing the door is begin with user needs to flash the card in front of the reader. If the system is able recognize the card, a blink of green LED will appear and one beep sound will be heard. On contrary, red LED will blink with two beep sound as mention to user that there is an invalid reading. If the car is accepted and verified, then they may enter the pin number on the keypad. Upon identity verification, the electromagnetic door will automatically open and allow the door to be opened. However, user need to push the exit button from the inside of the room first manually in order to lock the door during the exit.

There are few weaknesses in the system for example it is need to keep a hard copy list of the name, user number, and card number programmed into the reader for future maintenance. While using this system, a software need to be added so that all user profile can be stored in PC. The function of this software is for allowing easy add, edit or delete of user profile. The Figure 2.3 below shows the diagram of the DR2.

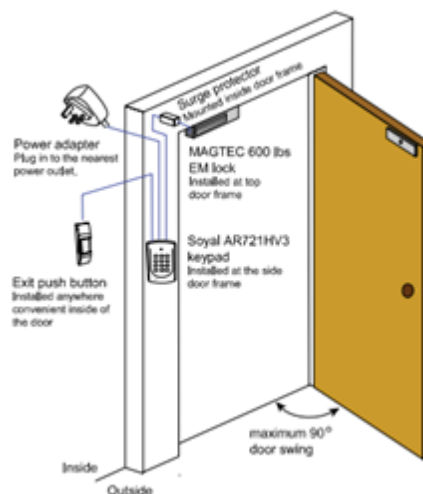


Figure 2.3 DR2 Installation Diagram (Soyal, DR2 Door access package, 2016)

2.3 COMPARISON EXISTING SYSTEMS

The three existing systems which are DM1-Vandal Resistant Slim Reader, UNIPASS–The Simple, Efficient Access Control Solution, and DR2-Standalone Card and Pin have been studied and compared. Based on these three systems, there are some differences that can be summarize as shown in the Table 2.1.

	Features and Accessing Operation	Challenges and Limitation	Type of Alarm Notification
DM1 – Vandal Resistant Slim Reader	<ul style="list-style-type: none"> - Firstly, user need to choose the method to access the door whether using pin or card. - Access the door by scanning the card or pin in front of the door - If the data is verified, it then will send to the PC 	<ul style="list-style-type: none"> - Only user with authorized access are allowed - The alarm will sound as warning if stranger or unauthorized user tries to access 	<ul style="list-style-type: none"> - If successfully recognized by the reader a single beep sound will be heard - If not recognized by the reader a double beep sound will be heard
UNIPASS – The Simple, Efficient Access Control Solution	<ul style="list-style-type: none"> - User access the door by scanning fingerprint - Then, the raw data will be compared by the system with stored or existing data - The system 	<ul style="list-style-type: none"> - Not effective as the system difficult to detect if user’s finger are injured or wet - A fault result will occur due to the condition (dryness or 	<ul style="list-style-type: none"> - Automatic dispatch of reports by e-mail

	include from the enrollment phase, identification phase and verification phase	dirtiness) of user's finger skin	
DR2 - Standalone Card and Pin	<ul style="list-style-type: none"> - First, user need to scan the card the reader - Then, user may enter the pin to access the door - Used multiple of characters for password security - The exit button need to pushed manually by user in order to lock back the door 	<ul style="list-style-type: none"> - Only user with authorized access are allowed - 8 characters is the minimum of password length . - User need to memorize variety of characters for the password - The alarm will sound as warning if stranger or unauthorized user tries to access - Manually programmed the reader through the keypad 	<ul style="list-style-type: none"> - Green LED will blink with one beep sound to notify that the card is successfully recognized - Red LED will blink with double beep sound to notify that the card is successfully recognized

Table 2.1 A Comparison Between The Different Systems

2.4 SUMMARY

Kolej Kediaman 2 at present used manual key for lock and unlock the door. The key is made by metal that have incisions cut to fit the wards of a particular lock, to open or close the door. As we know, the key is actually the traditional way and only operate in offline state.

The benefit while individual use this traditional method is they no need to use electrical supply if compared to nowadays advance technology method. This method is the cheaper way compare to the method that technology invented. Besides, the key is easy to bring and also easy to take care of. However, the key of course has their own weakness for example users may lost their key due to misplace because they need to bring the key together everywhere they go.

Based on today's rapidly developing technology, various methods have been invented to reduce the user's burden of life. Therefore, there are many technologies available for protection purpose likes a password or PIN and access card. The example of technology that related to this project is a security system to access someplace using access card. However, the technology that was established does not completely safe because sometime hackers or unauthorized user still can intrude our room. For example, if we set the password for our access door, intruders still can crack our password. Although, using a strong password also not solve the problem as user need to remember those characters because strong passwords are normally not mean anything to the user.

Therefore, for this project, the features of security access system that used is RFID technology. This technology is more suitable compare to fingerprint or password access because it is more safe and more convenient for students. Another reason why RFID technology is chosen because users do not have to bring a key with them anymore and the problem of missing key also can be solved. As conclusion, in order to find the solution to this problem, the Security Access Control System with warning SMS notification will be developed.

CHAPTER 3

METHODOLOGY

3.1 INTRODUCTION

Methodology is important in the development of this system. The function of methodology in this system is as guideline for developer to plan, structure and control the system development process. The software process model for this project development is discussed in this chapter. Besides, this chapter also will tell about the development methodology and the specification of hardware and software which are required for the project's development and implementation.

In this project, the methodology that will be utilized is Rapid Application Development (RAD). Basically it focuses on the design, prototype, research and related hardware and software for the whole project's development. There are some advantages of using RAD methodology which is its convenient and flexibility. Thus, if there are some issues during the phases occur, then it helps to make the system easier to modify. RAD is best used for developing system based on existing prototype. The key to this methodology is to reuse the prototype hence, reduce the duration of development process and testing. Moreover, it provides system that offer minimal maintenance cost. The involvement of user in the analysis and design stage also improve the good quality of final product.

3.2 RAPID APPLICATION DEVELOPMENT METHODOLOGY

To ensure the project is successful, the right and suitable methodology should be considered. The methodology that will be used to develop this system is Rapid Application Development (RAD). Basically, RAD is a software development methodology. Iterative development and constructed technique are the things that involve in RAD. Figure 3.1 shows the process of RAD methodology.

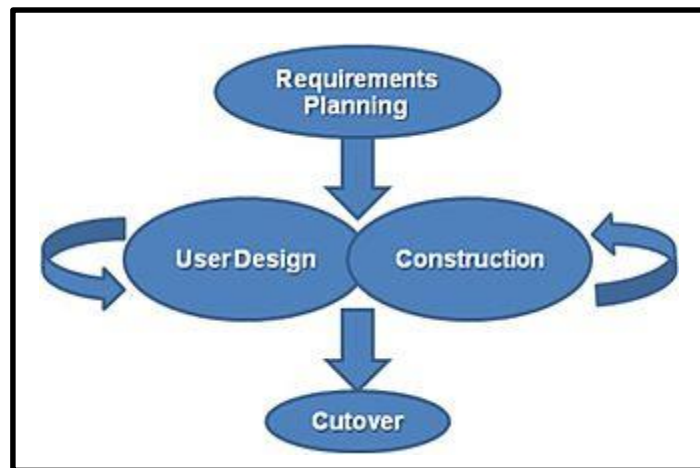


Figure 3.1 Rapid Application Development (RAD) Diagram

By using this method, a clear idea on what should be or should not be built in this system will be obtained. If there are any problems regarding the system, it can be solved first before any implementation is done. Hence, the system can be developed faster and at the same time consuming with low cost. The analysis, design, build and test phase was combined by RAD in the traditional SDLC into the iterative process in order to produce efficient development technique. RAD basically has 4 phases which are requirement planning, user design, construction and cutover.

Requirement planning is a phase that require the end user determine what the function of the system. In this phase, the objective and scope of Security Access Control System will be identified and clarified. The requirement for the system will be discussed and also define the project methodology, technique and tools.

The next phase is user design. In this phase, user needs to participate with the developer as to create the system's prototype. The user will participate under guidance provided by the developer. The prototyping process is created to assist in requirement specification and design.

For construction phase, the Security Control Access System will be developed and also implementing the elementary modules. Here, all the codes will be generated to the prototype. To enhance the performance of generated code, code optimizer may be used. In this phase, the end user ID will involve as the testing will take place all the way through the process of construction.

The last phase of RAD is cutover. In cutover phase, it will present the new system to the end user. Here, comprehensive testing, end user training and implementation the system will occur. This phase is basically consist of implementation and maintenance phase.

3.3 ACTIVITIES IN THE RAD METHODOLOGY

3.3.1 Requirement Planning Phase

Requirement planning phase is very important in RAD methodology as it covered everything that need to prepare before the project development is started. There are many aspects that must be analysed and defined in this phase including project scope, objective, project planning, hardware and software that used and also project description. The process had been done in this stage is firstly find all the information about the current system. All process must be done in a time that been plan from beginning.

Therefore, in this phase, the Gantt chart is created. This Gantt chart shows the overall schedule of the project development and function as to ensure the project development delivered on time. Furthermore, this Gantt chart will assist in order to plan, manage and track the task development. The project schedule's detail refers to Appendix A.

3.3.2 User Design Phase

After identify all the tools and requirement needed from previous phase, hence the analysis is made. While using this RAD methodology, in order to minimize the time consuming for completing this project, analysis and design are combined together.

In analysis phase, the information that needed for this system was analysed to make sure that the goals of the system are achieved. The current existing systems in the market also must be studied in finding the solution of project's problem. Therefore, it helps in order to design and enhance the proposed system and also to reach the project's objectives.

In design phase, the RFID technology that used in this system will go through some steps to establish the access control process. These steps are shown like the Figure 3.7 below.

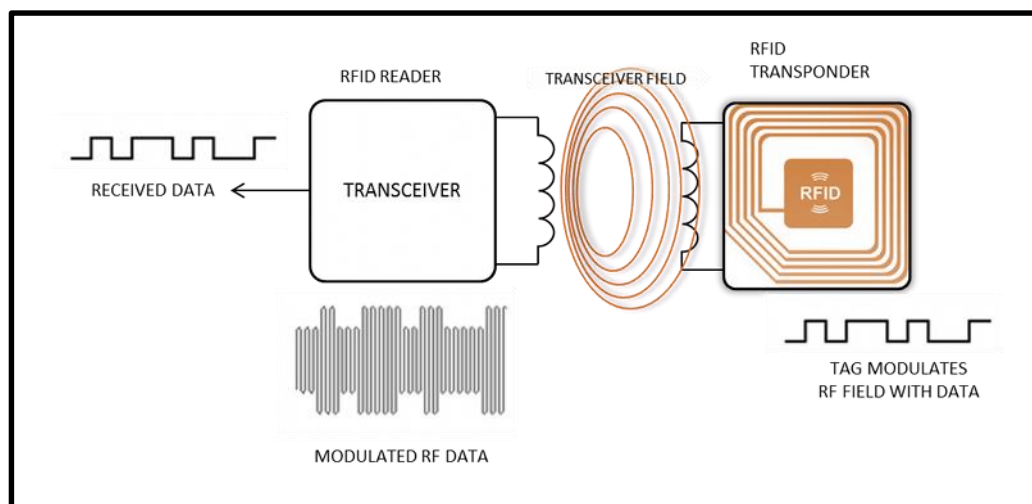


Figure 3.2 Process of RFID

RFID is a technology that used radio waves in order to transmit the identity of the individual. This RFID used waves as to recognize and capture the data stored in a card or tag. The typical RFID consist of two main components. The first one is the tags or transponder and the other one is reader or interrogator. For the RFID tags, it consists of two main parts which are 12 byte unique ID Microchip that used to store and process the

information. The second one is the antenna that used to receive and transmit the signal. For the reader hardware, it is used to detect radio waves and receive the signal from the tag whenever the tag is brought or scan around the reader's range.

For the reader to read the information in the tags, the reader will emit a signal to the tag through an antenna. Then, it will convert the energy into radio frequency waves. Next, after the tag is read by the reader, the antenna from the tag draws in energy from the radio waves. The energy moves from the antenna belong to tag to the IC then will power the chip which produced a signal back to the waves. The ID or information that embedded in the tag will read by the reader whenever the RFID tag is brought near the specific range of the reader. Thereafter, these information and ID will pass onto a controller or processor.

Nowadays, several types of RFID tags have been used in many aspect. In this project, in order to develop the Security Access Control System, the passive RFID tag is used. Passive tags did not have power source so this tag need to derive the power from the incident electromagnetic field that generated by the reader. The passive tag used the radio waves from the reader to relay its stored information back to the reader. However, the passive RFID tag operates in different frequency. Based on the system that will be developed, the 125-134 KHz of frequency is used because it is the lower frequency. The range for lower frequency is about 1–10 cm (Smiley, 2016). This type of lower frequency is better for this system as it is long wavelength but has a short read range.

Whenever RFID system operate with low frequency, the range covered is short and also the rate of data being read is slower. The reason why this type of tag is used is its abilities to read the data near the liquid surfaces. On the contrary, if the system operates using high frequency, the range of the radio waves is longer and also it has a faster rate of data transfer. However, it is not suitable to use high frequency tags for this system because is the tag is sensitive to the metals and liquid surfaces. Therefore, the passive tag is chosen and used in this system as this passive tag is commonly used for most of application like access control, smart label and file tracking.

3.3.3 Construction Phase

The process is focused on the system development while in this construction phase. Besides, the obtained data and all the requirements will turn into the working system.

The figure below shows the rough process of developing and how the security Access Control System. This system works where it can detect intruders or anyone who try attempts to access the owner's room without permission. When the system has detected there is intruder, it will generate the notification to the owner by sending the SMS through the phone. The general flow of the proposed project is showed in the Figure 3.3 below.

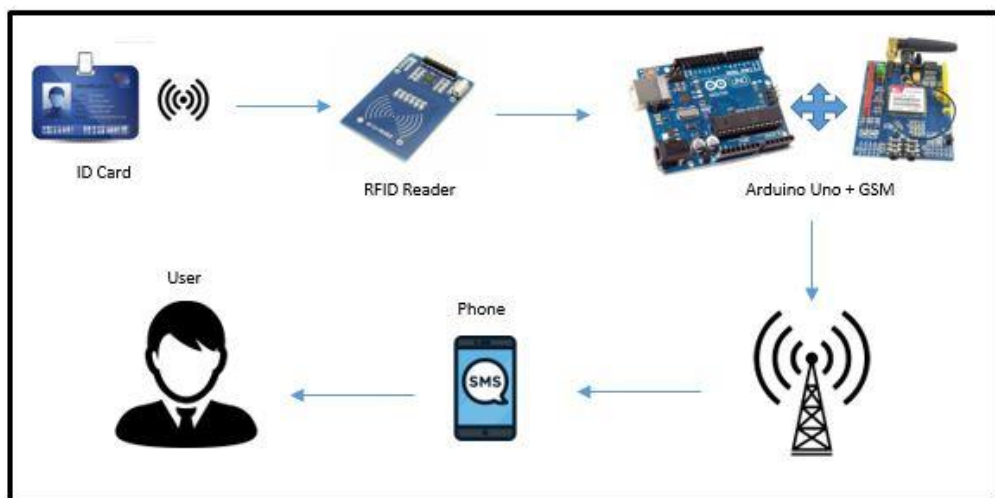


Figure 3.3 Flow Diagram of Security Access Control System

3.3.4 Cutover Phase

After all the phase is going through, in this final phase which is cutover phase, the system will deliver to the end user which is college's students. This phase is basically a combination of the implementation and maintenance phase. Here, testing, training to the user and implementation should be done in this phase. After that, if there are any errors or mistakes, this system needs to be improved and upgraded to meet the user requirement.

3.4 SOFTWARE DESIGN DOCUMENT

3.4.1 Flow chart

A flowchart actually is a kind of diagram which depicts a workflow, algorithm, or process. The flowchart displays the sequences as boxes of multiple kinds, and their order by link up the boxes with arrows. Flow chart is used to visualize the process that flowing throughout this system. The flow chart of the entire system is shown in the Figure 3.4 below.

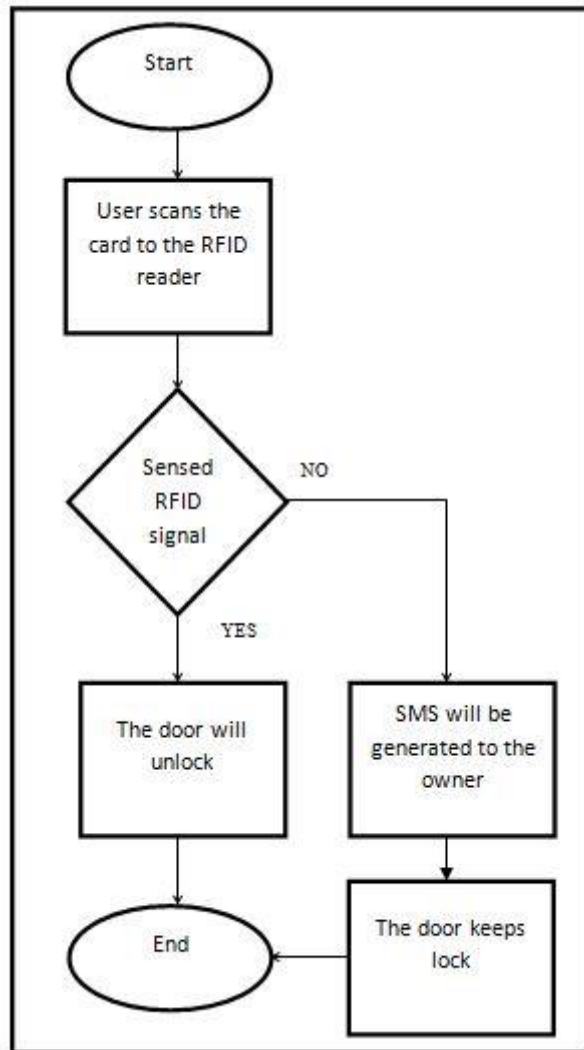


Figure 3.4 Flowchart of the Security Access Control System

3.4.2 Context Diagram

The context diagram of this Security Access Control System is shown in the figure below. It defines the system's boundary and the entities that interact with it also shown.

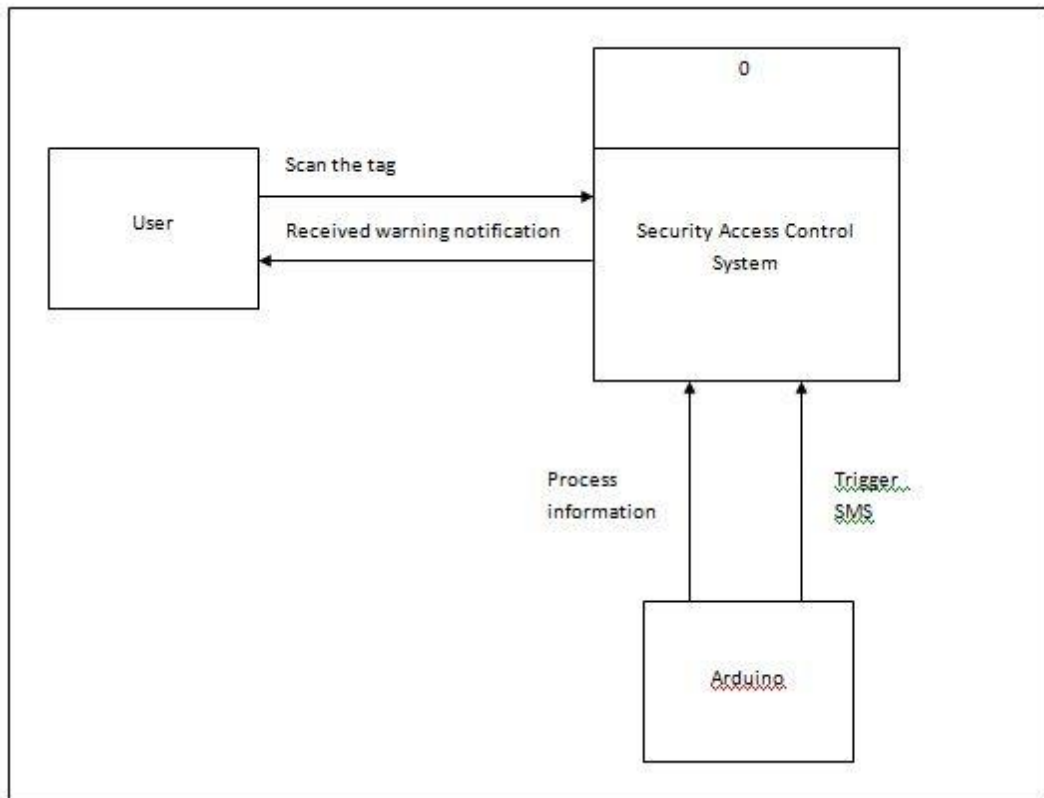


Figure 3.5 Context Diagram

3.4.3 Use Case Diagram

Use case diagram is a representation of the interaction of user with the system that shows the relationship among the user and the different use cases in which the user is involved. The use case diagram for this system is developed in order to show the interaction and relationship between user and the system. This diagram is useful to analyse the effect or influence that could come from this system as shown in Figure 3.10 below. This system will be analysed with list of all functions it could perform. Besides, any actors involve will have to be identified as shown in figure below.

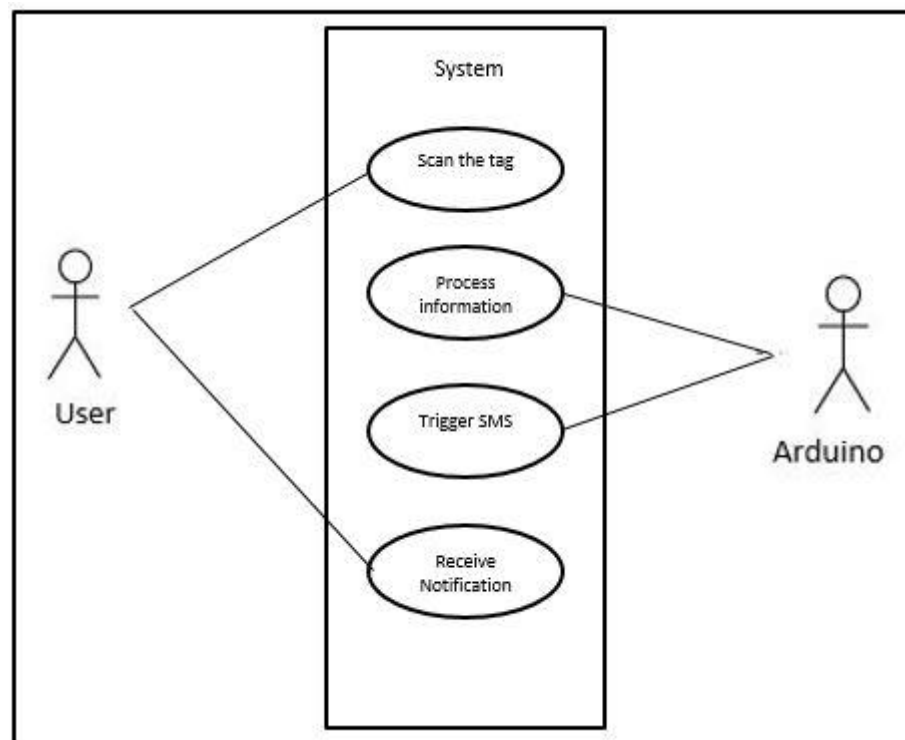


Figure 3.6 Use Case Diagram of Security Access Control System

3.5 HARDWARE AND SOFTWARE

In this section, the type of hardware and software that have been used during the development of the system are described. The hardware that I use are Arduino UNO R3, RFID MIFAIR RC522 IC Card Induction Module, 12VDC Solenoid Electromagnetic, 5V Single Relay Module, SIM900 GSM Modem. The software that I use while developing this system are Arduino IDE and Fritzing.

3.5.1 Hardware

- a. Arduino UNO R3



Figure 3.7 Arduino UNO

The type of Arduino that will be used is Arduino UNO R3 because in the Arduino family, it is the most commonly used and documented board. Besides, UNO is relatively cheap and easy to setup. It also has own IDE software which is run on developer computer. Using Arduino UNO, it can be directly upload the program into the physical board.

Nowadays, Arduino has become popular as it is an open source platform and also this device unnecessary separated pieces of hardware or programmer to load the source

code onto the board. By referring to Figure 3.2 above, Arduino UNO is hardware used to build electronic projects and could be explained as platform based on easy to use hardware and software. This is due to the Arduino used C++ and C language which is easy for beginner or novice user to learn.

Arduino UNO R3 is a microcontroller board based on the ATmega328. This version is consists of 14 digital input and output pins, 6 analog inputs, a USB connection, an ICSP header, a power jack, a 16 MHz ceramic resonator and a reset button. To get started, simply connect the USB cable from the Arduino UNO R3 USB port to the computer. In other ways, it also can be start by powered it with AC to DC adapter or battery with minimum 12 volts. Refer the Table 3.1 below for further details about the board.

The Arduino board is really advanced as it able read inputs, sending and transmitting the signal by just set the instructions to the microcontroller that attached on the Arduino board. By using Arduino programming language which based on the wiring and Arduino software (IDE) based on the processing, it will tell the board what to do. In addition, this devices source codes are easy to find over the internet. The Arduino will operate as a centre of operation as the other components and wired will be connecting through it. Based on all the fact and reason, this device has been selected as one of main hardware component in order to develop the Security Access Control System.

Table 3.1 The Specification of Arduino UNO 3

Microcontroller	ATmega2560
Input Voltage	12V
Operating Voltage	5V
Digital I/O Pin	14
Input Voltage	6-20 Volts
DC current for 3.3V Pin	40 mA

DC Current per I/O Pin	50 mA
Analog Input Pins	6
Flash Memory	32 KB (ATmega328 if which 0.5 KB used by bootloader)
SRAM	2 KB (ATmega328)
Clock Speed	16 MHz
EEPROM	1 KB (ATmega328)

b. RFID MIFAIR RC522 IC Card Induction Module



Figure 3.8 MIFAIR RC522 RFID Reader

RFID (Radio-Frequency Identification) is popular used nowadays in security systems such as door locks. RFID modules in the market now can be very affordable, such as the Mifare RC522 that will be used in this system. Mifare RC522 is a highly integrated read and write card chip that applied to the 13.56MHz contactless communication. Figure 3.3 above shows the image of MIFAIR RC522 RFID Reader.

This device which launched by the NXP Company is a low cost, low voltage, and small sized non-contact card chip. Hence, it is the best choice for portable handheld device.

The RFID Mifare RC522 communicates with cards up to 1cm using a 13.56MHz electromagnetic field. Then, it sends the data to the Arduino board via SPI communication. This device supports rapid CRTPTO1 encryption algorithm. It is for verifying MIFARE products. It also supports MIFARE series with a two-way data transmission rate of up to 424kbit/s of high-speed non-contact communication.

In this MF522 module, it used original Philips MFRC522 chip. This card reader not only low cost but it also easy to use and applies to the user equipment development. Furthermore, this reader is really good because it can be directly loaded into the variety of the reader mold. To ensure that the module is stable and reliable work, the reader must utilised with voltage 3.3V through the SPI interface simple lines. Then, directly connect with any user CPU motherboard to the communication. The MIFAIR RC522 specification is shown in the Table 3.2 below.

Operating Current	13-26mA / DC 3.3V
Idle Current	10-13mA / DC 3.3V
Sleep Current	<80uA
Peak Current	<30mA
Operating Frequency	13.56MHz
Supported Card type	Mifare 1 S50, mifare 1 S70 IFARE Ultralight, mifare Pro, MIFARE DESFire
Product Physical Characteristize	40mmx60mm
Environmental Operating Temperature	-20 to +80 C

Environmental Storage Temperature	-40 to +85 C
Relative Humidity	5% to 95%

Table 3.2 The Specification of MIFAIR RC522

c. 12VDC Solenoid Electromagnetic



Figure 3.9 Solenoid 12VDC Solenoid Electromagnetic

Solenoid is basically electromagnetic hardware that made from high quality iron, which is strong and durable, secure and safe. The solenoid works when the power is generated to the coil, the slug is pulled inside. The figure 3.4 above shows the 12VDC Solenoid Electromagnetic device.

The typical solenoid basically has a slug with a slanted cut and a mounting bracket. Normally this solenoid is used for a basic cabinet or door. For this project, this solenoid will be attached at the prototype door for lock and unlock process as it has a good mounting bracket. At first, the slug is already outside the body as it means that it is in a lock state. After the 12VDC is connected to the solenoid, the slug will pull inside the body as it means that the door is already unlock. Table 3.3 shows the details of the device.

Voltage	12VDC
Current	0.6A / 7.2W
Action Form	Pull
Rated Stroke	8mm, 1KG
Body Size (Approx)	60x26x20mm / 2.36x1.024x0.787
Cylinder Size (Approx)	8x8mm / 0.315x0.315
Mounting Hole Part Size	46x36mm / 1.81x1.42
Mounting Hole Distance	33x20mm / 1.30x0.79
Weight	97g

Table 3.3 The Specification of 12VDC Solenoid Electromagnetic

d. 5V Single Relay Module

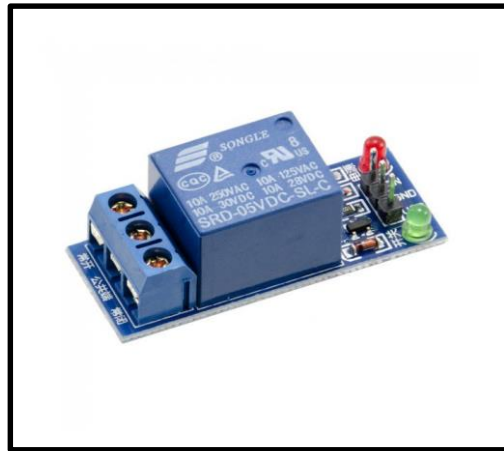


Figure 3.10 Single Relay Module

In developing this system, the 5V relay single module was used to remotely the electrical device switching. Relays normally used electromagnet in order to operate between two circuits. The relay works when the coil of relay is energized, the magnet will change the position of the switch. The function of this relay in this system is to remotely control devices, control the peripherals or other powered devices over a network. Therefore, this relay can be remotely powered to switch whether to turn on or off the system.

This relay was operated when the input (IN) is HIGH (+5V). This relay actually is an optical isolator. It separate connectors for the IN ground (COM) and used 5V supply ground (GND). In this system, the 5V single relay that used is consist of Normally Closed (NC), Normally Open (NO) and Common connection (COM). In order to make this relay worked, the relay must connect to the 5V pins of Arduino device. Figure 3.5 shows the image of Single Relay Module and the specification of the Relay 5V module that will be used in the project is shown in the Table 3.4 below.

Power Supply	5V
Relay Output	COM,NO NC

Table 3.4 The Specification of Ethernet Shield

e. SIM900a GSM Modem



Figure 3.11 SIM900a GSM Modem

Global System for Mobile communication (GSM) is a digital mobile telephony system that is popular in the market as it is widely used around the world. Nowadays in the market, there are different types of GSM modules available. This Security Access Control System is using the most popular module based on SIM900a GSM modem and Arduino Uno. Figure 3.5 shows the image of SIM900a GSM Modem. GSM digitizes and compresses data and then send it down a channel with two other streams of user data which are 900 MHz or 1800 MHz frequency band.

GSM modem is a modem that accepts a SIM card and work over a subscription to a mobile operator likes mobile phone. A GSM modem is capable to work with multiple type of Arduino such as Arduino Mega, Mega ADK, Leonardo and YUN. This device exposes an interface which allows application to send and receive message or SMS and also make voice call through General Packet Radio Service (GPRS) using the GSM library.

The first thing that should be noted is user must subscribe a mobile phone operator either postpaid or prepaid in order to get the connection while using GSM modem. Besides, user also needs a simcard that include information likes mobile phone number and also can store limited amounts of contact and SMS. The SIM900a GSM Modem specification is shown in the Table 3.5 below.

Board	Quad-Band 850/1800/1900 MHz
Protocol	Embedded with TCP/UDP stack
Commands	GSM 07.07 and 07.05 Enhanced commands : SIMCOM AT Commands

Table 3.5 The Specification of SIM900a GSM Modem

CHAPTER 4

RESULTS AND DISCUSSION

4.1 INTRODUCTION

This chapter basically will explain and describe the function of every part of the model after the implementation. To prepare this process, all part is combined together in a circuit in order to make the system works. The sketch that show the process of combining all the part in one circuit by using Fritzing software will help as reference to build the physical prototype. The last step in order to make the system function, all the codes are write in Arduino IDE then compiled and uploaded the code to the Arduino Uno.

4.2 MODEL IMPLEMENTATION

In this project, the main component is Arduino Uno. This device is known as a component that acts like a motherboard for this project. It also has its own Integrated Development Environment (IDE) which is can perform on a computer. This IDE is powerful as it can compile and upload the code into physical Arduino's board. Therefore, all the components must be set up similar to the sketch in Fritzing to make this project run according to what has been set. The steps and guides for the implementation of the components are explained as below.

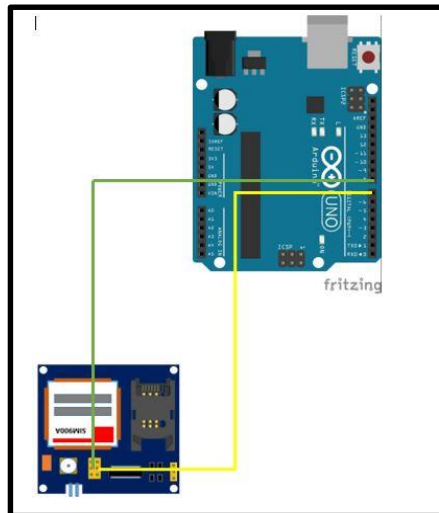


Figure 4.1 Arduino and GSM Modem

In the Figure 4.1 above, the first step that must be taken is connecting GSM modem with Arduino. Since this modem can support the SMS text mode, therefore the GSM can send and receive the SMS using AT commands. This modem also can get the signal and at the same time it can receive message's notification. This is because it has an active simcard that installed in the modem.

The process of embedding the simcard into the GSM modem actually is not too complicated. The step is by inserting the simcard in the slot available on GSM and then carefully lock it. The next step is connecting the adapter to the GSM then turn it on. Then, wait for a while and let the power supply flow to the board. After a few minutes, the LED of GSM modem will blink. Actually the blinking LED means that the modem is already successfully connected with Arduino. In order to connected with the RFID, identify first the connection of the RFID pins to the Arduino. The circuit's connection between the Arduino and the RFID module can be shown as in Figure 4.2 below.

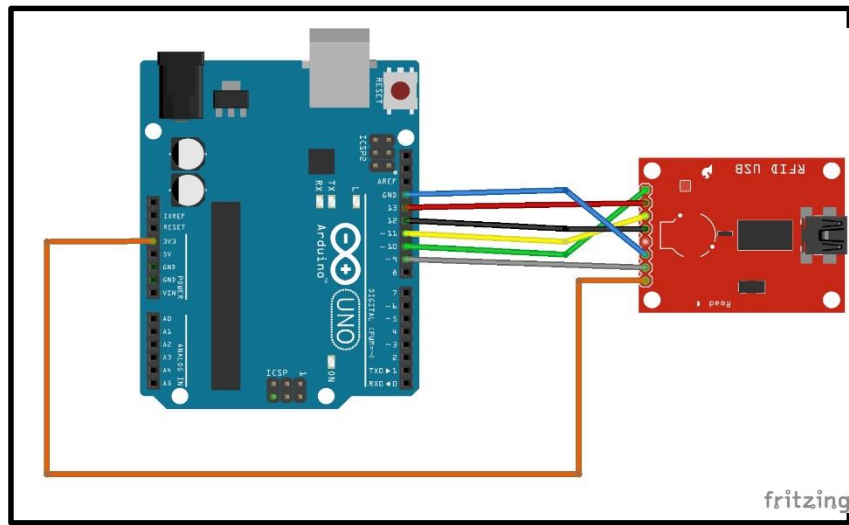


Figure 4.2 RFID and Arduino Circuit

The connection of RFID module with Arduino:

SDA	10
SCK	13
MOSI	11
MISO	12
GND	GND
RST	9
3.3V	3V3

In this system, relay is used so the system will more efficiently function. This relay must attach together into the modem which RFID connected. This is to show the action of the lock and unlock of the door. Figure 4.3 below shows the process of the signal from RFID in order to unlock the door. The detail description about the relay and what pins that must be connected to the board are shown below.

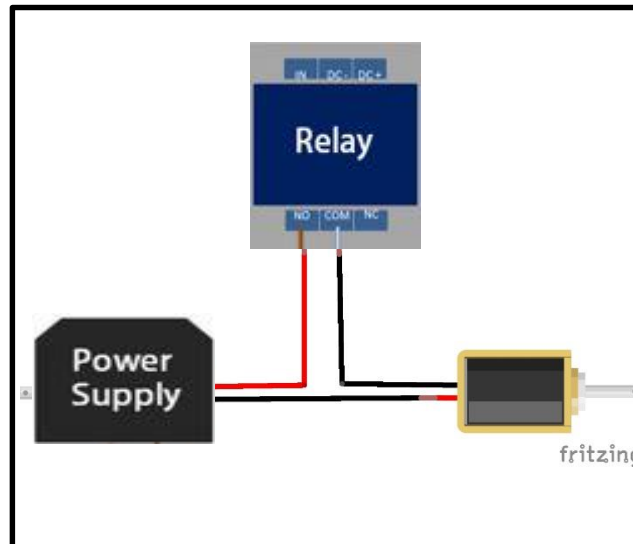


Figure 4.3 Connection of Relay, Solenoid, and Power Supply

Basically, the implementation of this program is the door will always in closed state. In order to unlock the door, we must trigger the relay module. Hence, it will unlock the solenoid for a few seconds based on the program coded. Basically, the COM part of the relay module is actually function as a switch. The lock and unlock process can be done by plugging the relay with the solenoid. Besides, to make the system running properly, the relay and solenoid should be connected to the power supply.

The connected pins:

Relay		Power Supply		Solenoid	
IN	8	1 wired	Solenoid	1 wired	Power Supply
DC-	GND	1 wired	NO Relay	1 wired	COM Relay
DC+	5V				
NO	Power supply				
COM	Solenoid				

Table 4.1 Connected pins

Then, the next process is done by combining all the circuit. Before combining all the part together in a 1 complete design, all the connection of pins must be checked that it connects with right connection. After all the parts are combined, then the codes of the program can be uploaded into the board. Figure 4.4 shows the complete design for Security Access Control System based on Radio Frequency Identification (RFID) and Arduino Technologies.

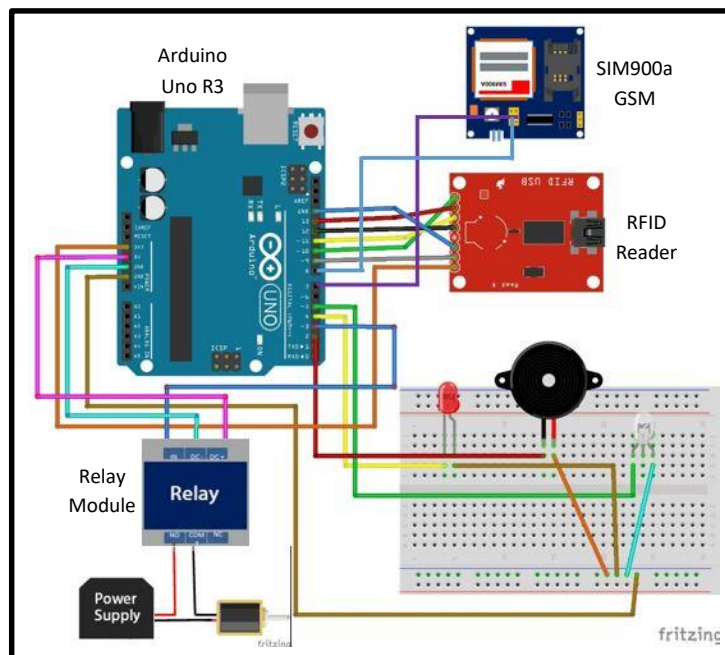


Figure 4.4 Complete Circuit and Design

In the Figure 4.4 above, the actual design of the system is shown to test the contact of solenoid with the relay through Arduino board, GSM and RFID module. Before connect all the components to the power supply, all the pins must be properly connected based on the complete circuit designed. Then, the program code can be uploaded to the board. For this system, the solenoid is basically in a lock state. This can be seen where the plunger of solenoid is currently outside of the component's body. When the RFID module reads the tag, the door will unlock as the connected pin to relay sent the signal to the solenoid.

4.3 THE IMPLEMENTATION OF CODING AND TESTING

In this system, the Arduino IDE is used in order to build the code and run the program. The Figure 4.5 below shows the Arduino IDE Software. As mention before, the coding must be write in this IDE then compiled and upload it to the Arduino board. Before begin the coding implementation, firstly the main board must be connected to the PC or laptop. This can be done by plugging the board to the USB cable then connect the cable to PC. The power from this PC will flow to the board to make this system working.

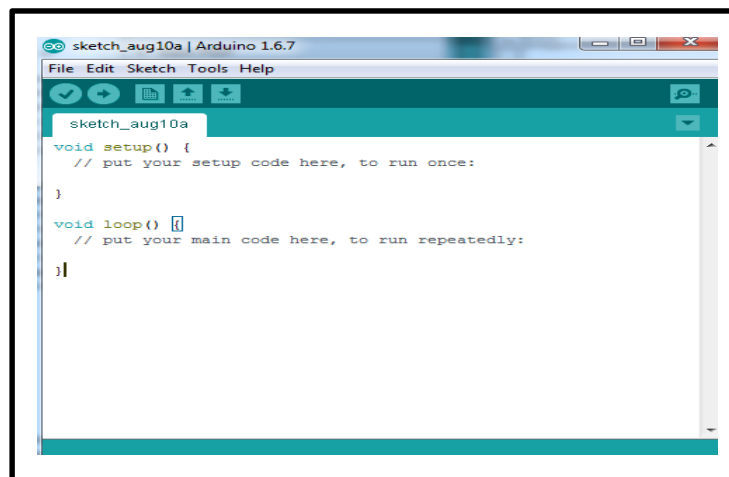


Figure 4.5 Arduino Software IDE

Before testing the code for GSM to trigger the SMS, the Arduino board should be set up properly first and must function well. The Arduino IDE needs to be ready with GSM library that can be get at the example provided by Arduino program. If the codes are successfully work, then combine it with the RFID codes in order to get complete code of the system. Figure 4.6 below shows the codes to generate the warning notification to the owner.

```
void sendSMS(String message)
{
  SIM900.print("AT+CMGF=1\r"); // AT command to send SMS message
  delay(1000);
  SIM900.println("AT + CMGS = \"+60134484332\"); // recipient's mobile number,
in international format
  delay(1000);
  SIM900.println(message); // message to send
  delay(1000);
  SIM900.println((char)26); // End AT command with a ^Z, ASCII code 26
  delay(1000);
  SIM900.println();
  delay(100); // give module time to send SMS
  //SIM900power(); // turn off module
}
```

Figure 4.6 Codes to Generates Notification

The connection pin for relay then can be done after the function for generating message is works. The codes to implement the pins that connected to the relay to unlock the door is tested. Figure 4.7 below shows the codes.

```
#define RELAY    3    // relay pin
#define ACCESS_DELAY 2000
#define DENIED_DELAY 1000

void setup() {

digitalWrite(RELAY, HIGH);

void loop() {

    digitalWrite(RELAY, LOW);

    delay(ACCESS_DELAY);

    digitalWrite(RELAY, HIGH);

}
```

Figure 4.7 Codes for Relay

In this system, the crucial part is the process of scanning the RFID card. Therefore, the code that have been implemented in the system is to detect the card's ID and also to trigger the pin 3. If there is unauthorized user try to scan their card to the RFID reader, the message will be automatically generated and send to the owner of the room. The Figure 4.8 below shows the RFID code and main code for generate the warning message.

```

#include <SPI.h>
#include <MFRC522.h>
#include <SoftwareSerial.h>
String textForSMS;
SoftwareSerial SIM900(7,8);

#define RST_PIN      9      // Configurable, see typical pin layout above
#define SS_PIN       10     // Configurable, see typical pin layout above
#define LED_G        5      // define green LED pin
#define LED_R        4      // define red LED pin
#define BUZZER       2      // buzzer pin
#define RELAY        3      // relay pin
#define ACCESS_DELAY 2000
#define DENIED_DELAY 1000

MFRC522 mfrc522(SS_PIN, RST_PIN); // Create MFRC522 instance

void setup() {

  Serial.begin(9600); // Initialize serial communications with the PC
  SIM900.begin(9600);
  while (!Serial); // Do nothing if no serial port is opened (added for Arduinos
based on ATMEGA32U4)
  SPI.begin(); // Initialize SPI bus
  mfrc522.PCD_Init(); // Initialize MFRC522
  mfrc522.PCD_DumpVersionToSerial(); // Show details of PCD - MFRC522 Card
Reader details

  pinMode(LED_G, OUTPUT);
  pinMode(LED_R, OUTPUT);
  pinMode(RELAY, OUTPUT);
  pinMode(BUZZER, OUTPUT);
  noTone(BUZZER);
  digitalWrite(RELAY, HIGH);

  Serial.println(F(""));
  Serial.println(F(""));
  Serial.println(F("WELCOME TO SECURITY ACCESS CONTROL SYSTEM"));
  Serial.println(F("      by @ammarfaez11"));
  Serial.println(F(""));
  Serial.println(F(""));
  Serial.println(F("Put your card to the reader..."));
  Serial.println(F(""));
}

```

```

void loop() {
    // Look for new cards
    if ( ! mfr522.PICC_IsNewCardPresent() ) {
        return;
    }

    // Select one of the cards
    if ( ! mfr522.PICC_ReadCardSerial() ) {
        return;
    }

//Read data from Card
//Show UID on serial monitor
Serial.println();
Serial.print("Your ID Card No. :");
String content= "";
byte letter;
for (byte i = 0; i < mfr522.uid.size; i++)
{
    Serial.print(mfr522.uid.uidByte[i] < 0x10 ? " 0" : " ");
    Serial.print(mfr522.uid.uidByte[i], HEX);
    content.concat(String(mfr522.uid.uidByte[i] < 0x10 ? " 0" : " "));
    content.concat(String(mfr522.uid.uidByte[i], HEX));
}
Serial.println();
Serial.print("Message : ");
content.toUpperCase();
if (content.substring(1) == "8A 65 39 8F" || content.substring(1) == "FA 7F 4C 79" ||
content.substring(1) == "8A 65 39 8F" || content.substring(1) == "A4 6A F8 D0")
{
    Serial.println("Authorized access!You May Enter The Room.");
    Serial.println();
    delay(500);

    digitalWrite(RELAY, LOW);
    digitalWrite(LED_G, HIGH); //green led turn on
    tone(BUZZER, 2000 , 500); //buzzer sound on
    //delay(500);
    delay(Access_Delay);
    digitalWrite(RELAY, HIGH);
    digitalWrite(LED_G, LOW); //green led off
    noTone(BUZZER); //buzzer off
}
}

```

```

else{

  Serial.println(" Access denied! Please Go Away!");

  digitalWrite(LED_R, HIGH); //led red turn on
  tone(BUZZER, 2000, 300); //buzzer sound on
  delay(DENIED_DELAY);
  digitalWrite(LED_R, LOW); //led red turn off
  noTone(BUZZER); //buzzer sound off

  textForSMS = "\nWARNING!!! SOMEONE IS TRYING TO BREAK INTO YOUR ROOM
!";
  sendSMS(textForSMS);
  Serial.println(textForSMS);
  Serial.println("message sent.");
  delay(5000);
}
}

void sendSMS(String message)
{
  SIM900.print("AT+CMGF=1\r"); // AT command to send SMS message
  delay(1000);
  SIM900.println("AT + CMGS = \"+60134484332\""); // recipient's mobile number, in
international format
  delay(1000);
  SIM900.println(message); // message to send
  delay(1000);
  SIM900.println((char)26); // End AT command with a ^Z, ASCII code 26
  delay(1000);
  SIM900.println();
  delay(100); // give module time to send SMS
  //SIM900power(); // turn off module
}

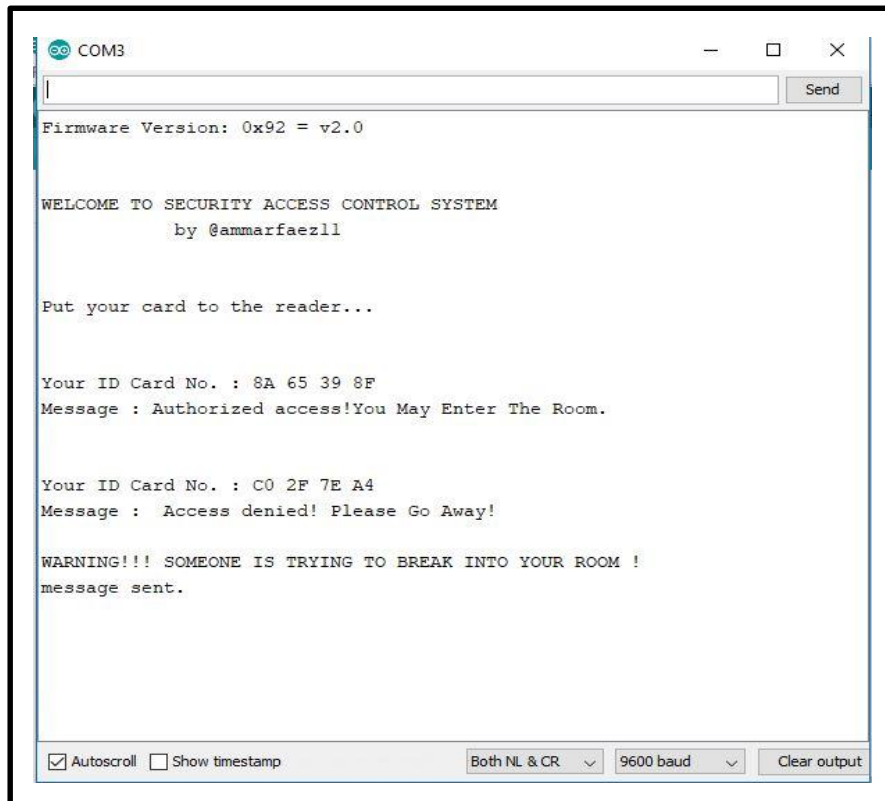
//Dump debug info about the card; PICC_HaltA() is automatically called
//uncomment to read data from card
// mfr522.PICC_DumpToSerial(&(mfr522.uid));
//}

```

Figure 4.8 Main Code

4.4 RESULTS AND DISCUSSION

For this section, all the results of this Security Access Control System Based on RFID and Arduino Technology are covered and discussed. After all the system's code are implemented and tested, then uploaded to the Arduino Board, the program can be run according to the requirement needed and meet the objectives of the project.



```
COM3
Firmware Version: 0x92 = v2.0

WELCOME TO SECURITY ACCESS CONTROL SYSTEM
  by @ammarfaez11

Put your card to the reader...

Your ID Card No. : 8A 65 39 8F
Message : Authorized access!You May Enter The Room.

Your ID Card No. : C0 2F 7E A4
Message : Access denied! Please Go Away!

WARNING!!! SOMEONE IS TRYING TO BREAK INTO YOUR ROOM !
message sent.
```

Figure 4.9 Result in Logical Side

Based on Figure 4.9 above, it shows the result in logical side. When user scan their card to the reader, then in this serial monitor, it shows the user's ID card number. Besides, the message also will be print there which show whether user can access the room or not. Here, the error message is displayed if unauthorized user scanned their card. Then, the system will trigger a warning notification that automatically sent to owner's mobile phone.



Figure 4.10 Result in Physical Side

From the Figure 4.10 above, it shows the results of the physical side of this system. It shows that the message has been triggered by the Arduino through the signal that the RFID rejected. This happen whenever the RFID could not read the cards which leads to the Arduino board triggered a warning notification as a SMS to owner's mobile phone.

CHAPTER 5

CONCLUSION

5.1 INTRODUCTION

In the previous chapter, there is multiple of phase that has been going through in order to complete this project. For this chapter, it will conclude that this Security Access Control System based on Radio Frequency Identification (RFID) and Arduino Technologies was a success as it achieves the objectives of this project. The final result of this project is the warning notification will send to the room's owner as an alert based on certain condition that has been programmed. In this project, a Short Message Service (SMS) will be sent to the owner as a notification.

For a conclusion, the Security Access Control System based on Radio Frequency Identification (RFID) and Arduino Technologies capable to inform owner if the outsiders are attempting to breaking into the owner's room without authorize. The essential thought of this system is the entryway at the room's college will continuously in locked state. In order to make the door unlocked, the first thing to do is the user's card must be scanned around the RFID reader. Next, the RFID reader will read the ID whether it is available in system or not, then the signal will send to the Arduino board. The Arduino then process the instruction to make the door unlock. This can be done when Arduino send the signal to the relay that connected to solenoid lock. On contrary, the GSM will execute the notification whenever the RFID reader cannot find ID match with the unauthorized user's card.

5.2 PROJECT CONSTRAINT AND CHALLENGES

Honestly there are a few constraints that had been face during completion of this project. One of the problem that had been identified is the problem with the RFID reader. This is because during the scanning process, the RFID reader cannot function well. The RFID reader sometimes hard to detect the scanned card. As we know, the cards must be

scanned using wave that RFID provided. The problem comes when user needs to scan the card for a few times before it successfully read because the reader cannot detect the card. Hence, this situation gives a worried feeling to the user because they afraid if the message will generate and send to the room's owner.

Besides, the other constraint that comes was problem in handling the communication between Arduino and GSM modem. Sometimes the notification message was error because the signal that GSM provided to trigger the notification is failed. In addition, the GSM modem that had been used for the project is currently lack of some function for example for this version of GSM modem, it only allows the notification to be sent to one person or one number only at a time. The solution for an alternative way to solve this problem will explain later on which another device that can be used instead of Arduino Uno.

5.3 FUTURE WORK

Once the project has been completed, there are some aspects that can still be improved in the future. These suggestions to ensure that this project can be enhanced even the project's goals and objectives of the project have been achieved. For example, the warning notification message. As we know, the warning message notification implemented in this system is still lacking because it is only able to send a message to only one recipient at a time. Therefore, other ways should be considered to improve this shortcoming. One of the best way to solve this lack is by using Arduino Mega or advance GSM modem as this device is able to send messages to multiple recipients at a time.

REFERENCES

- Administrator. (2016). *10 Simple Arduino Projects For Beginners with Code*. Retrieved from Electronics Hub.
- Agarwal, T. (2012). *Know about Access Control Systems and Their Types with Features*. Retrieved from elprocus.
- Arduino. (2003). *Introduction*. Retrieved from Arduino.
- Astc. (2016). *Advantages and disadvantages of RFID Door Locks*. Retrieved from Astclocks.
- Chudasma, S. (2014). *RFID Based Attendance System using 8051 Microcontroller*. Retrieved from EngineerGarage.
- Fabio. (2006). *What is Arduino, Why we choose it, what can we do with it?* Retrieved from varesano.net.
- IDtech. (2016). *UNIPASS The simple, efficient access control system*.
- Ishabakaki, P. (2015). *Radio Frequency Identification based Drug Management and Monitoring System: A Case of Public Hospitals in Tanzania*.
- Långström, H. (2013). *Grocery industry operations are facing a real paradigm shift*. Retrieved from RFID ARENA.
- Mukherjee, A. (2016). *Security Access Using RFID Reader © GPL3+*. Retrieved from Project Hub.
- Pandey, D. P. (2016). *Application of RFID Technology in Libraries and Role of Librarian*.
- Rouse, M. (2006). *RFID (radio frequency identification)*. Retrieved from IoT Agenda.

Smiley, S. (2016). *Active RFID vs. Passive RFID: What's the Difference?* Retrieved from RFID Insider Tracking The RFID Industry.

Soyal. (2016). *DM1 Door access package.*

Soyal. (2016). *DR2 Door access package.*

Thrasher, J. (2013). *How is RFID Used in Real World Applications?* Retrieved from RFID INSIDER TRACKING THE RFID INDUSTRY.

UK, M. F. (2014). *Personal Alarm Mini Foaming Defence Spray UK.* Retrieved from Crime Prevention Products.

University, Y. (2006). *Security Systems.* Retrieved from It's Your Yale.

Viper. (2009). *Viper LCD 2-Way Security System.* Retrieved from Viper.

Vivint. (2012). *Vivint.SmartHome.* Retrieved from Vivint.

Waxton. (2016). *STANDALONE CARD AND PIN.* Retrieved from Waxtonit.

APPENDICES

APPENDIX A

Gantt Chart

