ANALYSIS OF SECURITY METHOD IN AUTOMATED GATE SYSTEM

HANI MAISARAH BT ZAINAL SUBARI

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

ANALYSIS OF SECURITY METHOD IN AUTOMATED GATE SYSTEM

HANI MAISARAH BT ZAINAL SUBARI

This report is submitted in partial fulfillment of the requirements for the Bachelor of [Computer Science (Computer Security)] with Honours.

FACULTY OF INFORMATION AND COMMUNICATION TECHNOLOGY UNIVERSITI TEKNIKAL MALAYSIA MELAKA

2021

DECLARATION

I hereby declare that this project report entitled

[ANALYSIS OF SECURITY METHODS IN AUTOMATED GATE SYSTEM]

is written by me and is my own effort and that no part has been plagiarized

without citations.

STUDENT : hanimsrh Date : 9/9/2021

(HANI MAISARAH BT ZAINAL SUBARI)

I hereby declare that I have read this project report and found

this project report is sufficient in term of the scope and quality for the award of

Bachelor of [Computer Science (Computer Security)] with Honours.

SUPERVISOR : Date : 9/9/2021

[ERMAN BIN HAMID]

DEDICATION

In the name of Allah, the Most Gracious, the Most Merciful. This project is dedicated to my beloved parents, siblings and my supervisor who always support and inspire me along the way, completing this project. Without them, I would never be able to finish this project successfully.

ACKNOWLEDGEMENTS

First and foremost, I would like to thank my supervisor, En Erman Bin Hamid for the valuable guidance and advice to lead me till the end of this final year project session 2020/2021. His willingness to motivate me contributed tremendously to my project. I would also like to thank my evaluator for this project, Dr. Nazrulazhar Bahaman for taking his time to evaluate me. This evaluation gave me a deeper understanding of my weakness and what I can improve to make it better.

I would also like to thank the authority of Universiti Teknikal Malaysia Melaka (UTeM) for providing me with a good environment and facilities to complete this project. Finally, an honourable mention goes to my families and friends for their understandings and supports me in completing this project. With the help of everyone that was mentioned above, I was able to overcome many problems and completed my project successfully on time.

ABSTRACT

Analysis of the Security Methods in Automated Gate System is an analysis to figure out which security method is the most secured to be implemented in the automated gate system. There will be three (3) platforms with different security methods that will be tested using specific tools and technique. The problem statements state that the current automated gate system offers many different security methods without knowing how secure it is. Besides that, some of the existing security methods have not identified specific tools that can be used to analyse them. Plus, clients do not know the best security method to be implemented in the Automated Gate System. To solve the current problem statement, security methods that need to be analysed need to be identified. Furthermore, tools to analyse the security methods need to be analysed and the platforms with different security methods need to be developed and analyse by using selected tools. The security methods that will be analysed are QR Code System, RFID System and Voice Recognition System. The security methods will be tested by using four parameters which are accuracy analysis, scan time, scan range and static analysis. The static analysis will be using Sonarqube and VisualCodeGrepper. Each platform will be developed in two phases which are hardware and software development. For QR Code, it will be using Arduino Uno Microcontroller and Visual Basic. For RFID, it will also be using Arduino Uno Microcontroller, RFID scanner and Arduino IDE. Lastly, for Voice Recognition, it will be using Arduino Uno Microcontroller, Python IDE and Arduino IDE. After the platform is developed, a security testing will be done to start doing analysis to identify which security method is the most secured.

ABSTRAK

Analisis Kaedah Keselamatan dalam Sistem Gerbang Automatik adalah analisis untuk mengetahui kaedah keselamatan mana yang paling selamat untuk dilaksanakan dalam sistem gerbang automatik. Akan ada tiga (3) platform dengan kaedah keselamatan yang berbeza yang akan diuji menggunakan alat dan teknik tertentu. Penyataan masalah menyatakan bahawa sistem gerbang automatik semasa menawarkan banyak kaedah keselamatan yang berbeza tanpa mengetahui seberapa selamatnya ia. Selain itu, beberapa kaedah keselamatan yang belum mengenal pasti alat khusus yang dapat digunakan untuk menganalisisnya. Tambahan pula, pelanggan tidak mengetahui kaedah keselamatan terbaik untuk dilaksanakan dalam Sistem Pintu Automatik. Untuk menyelesaikan penyataan masalah semasa, kaedah keselamatan yang perlu dianalisis perlu dikenal pasti. Selanjutnya, alat untuk menganalisis kaedah keselamatan perlu dianalisis dan platform dengan kaedah keselamatan yang berbeza perlu dikembangkan dan dianalisis dengan menggunakan alat yang dipilih. Kaedah keselamatan yang akan dianalisis adalah Sistem Kod QR, Sistem RFID dan Sistem Pengecaman Suara. Kaedah keselamatan yang akan dianalisis adalah Sistem Kod QR, Sistem RFID dan Sistem Pengecaman Suara. Kaedah keselamatan akan diuji dengan menggunakan empat parameter iaitu analisis ketepatan, masa imbasan, julat imbasan dan analisis statik. Analisis statik akan menggunakan Sonarqube dan VisualCodeGrepper. Setiap platform akan dikembangkan dalam dua fasa iaitu pengembangan perkakasan dan perisian. Untuk QR Code, ia akan menggunakan Arduino Uno Microcontroller dan Visual Basic. Untuk RFID, ia juga akan menggunakan Arduino Uno Microcontroller, RFID scanner dan Arduino IDE. Terakhir, untuk Pengecaman Suara, ia akan menggunakan Arduino Uno Microcontroller, Python IDE dan Arduino IDE. Setelah platform dikembangkan, ujian keselamatan akan dilakukan untuk mula melakukan analisis untuk mengenal pasti kaedah keselamatan mana yang paling selamat.

TABLE OF CONTENTS

PAGE

LIST OF FIGURES

PAGE

LIST OF TABLES

PAGE

CHAPTER 1: INTRODUCTION

1.1 Introduction

As the crime rates are now raising, households and companies should take extra caution to prevent any unauthorized entries. Having an appropriate and secured gating system can prevent it from happening. However, there are a lot of approaches of security methods in automated gate. In this project, the security methods will be analyzed to come out which is the most secured to be implemented in the automated gate system.

There are many methods that can be implemented in automated gate system which are using QR (Quick Response) Code, Vehicle License Plate Recognition System, Radio Frequency Identification card reader, Voice Recognition System and Biometric System. Most of the companies will always pay more attention to the cost rather than the security aspect. It is crucial for companies to take security aspect more seriously to protect employees, sensitive data and the property from any unauthorized entries.

The current automated gate system in the market is offering a lot of different security methods to be implemented without knowing how secure it is. This analysis is being made to compare which security methods can offer better security and is actually worth every penny to splurge for it.

1.2 Project Problem Statement

For small companies and households, automated gate needs high installation and maintenance fees. Company will go for price, without taking care of the security aspect whereas security is an important element in gate technology. To make sure it is worth the price and also the security aspects, analysis should be done to compare the methods and knows which methods can provide a secure gating system. It is crucial for companies to use the most secured methods to be implemented in the Automated Gate System to protect employees and important documents from the unauthorized users. Nowadays, there are a lot of security methods that are being used in Automated Gate System. However, before deciding what security method to be used in the Automated Gate System, we need to know how secure it is, in order to protect the properties from unwanted entries. Thus, tools to analyze the security methods have not been identified yet. Automated Gate System is a part of a defense system that need a reliable security method to ensure only the authorized users can enter the property. To achieve that, tools to analyze the security methods need to be identified. Clients deserve to know the best security method before implementing them in the Automated Gate System.

Table 1.1 Summary of Problem Statement

PS	Problem Statement
PS1	The current automated gate system offers many different security methods without knowing how secure it is.
PS2	Some of the existing security methods have not identified specific tools that can be used to analyze them.
PS3	Clients do not know the best security method to be implemented in the Automated Gate System.

1.3 Project Research Question

Project Research Question is used to identify the question of the existing gate system. Based on the research, we can conclude that there are few weaknesses of the current gate system. Table 1.2 shows the summary of the project research question.

Table 1.2 Summary of the Project Research Question

PRQ	Project Research Question
PRQ1	What is the security method that implemented in the Automated Gate System?
PRQ2	What tools can be used to analyse the security methods of the platform developed in Automated Gate System?
PRQ3	What is the best security method for Automated Gate System?

1.4 Project Objectives

Project objective defines the improvement that are achievable at the end of the project. The improvement must be considered based on the problem statement and the project research question of this project. The objectives of this project are shown at table 1.3 below.

Table 1.3 Project Objectives

PO	Project Objectives
PO1	To identify security method, evaluation tools and parameter that implemented in Automated Gate System (AGS).
PO2	To develop the platforms of AGS with three (3) different security methods.
PO3	To analyse the platforms developed using the selected evaluation tools and parameter.

1.5 Project Research Hypothesis

A research hypothesis is the statement created by researchers to improve the outcome of a research. Based on the research, the current gate system has insufficient features and are installed blindly without having a reliable security implementation due to the lack of analysis have been made to compare the security methods, no tools to analyse the security method to be implemented and some of the existing automated gates do not provide any tools to monitor the system. Some of the hypotheses have been suggested to improve the current gate system. Figure 1.1 shows the problem of the current gate system and the hypothesis to make an improvement to the system.

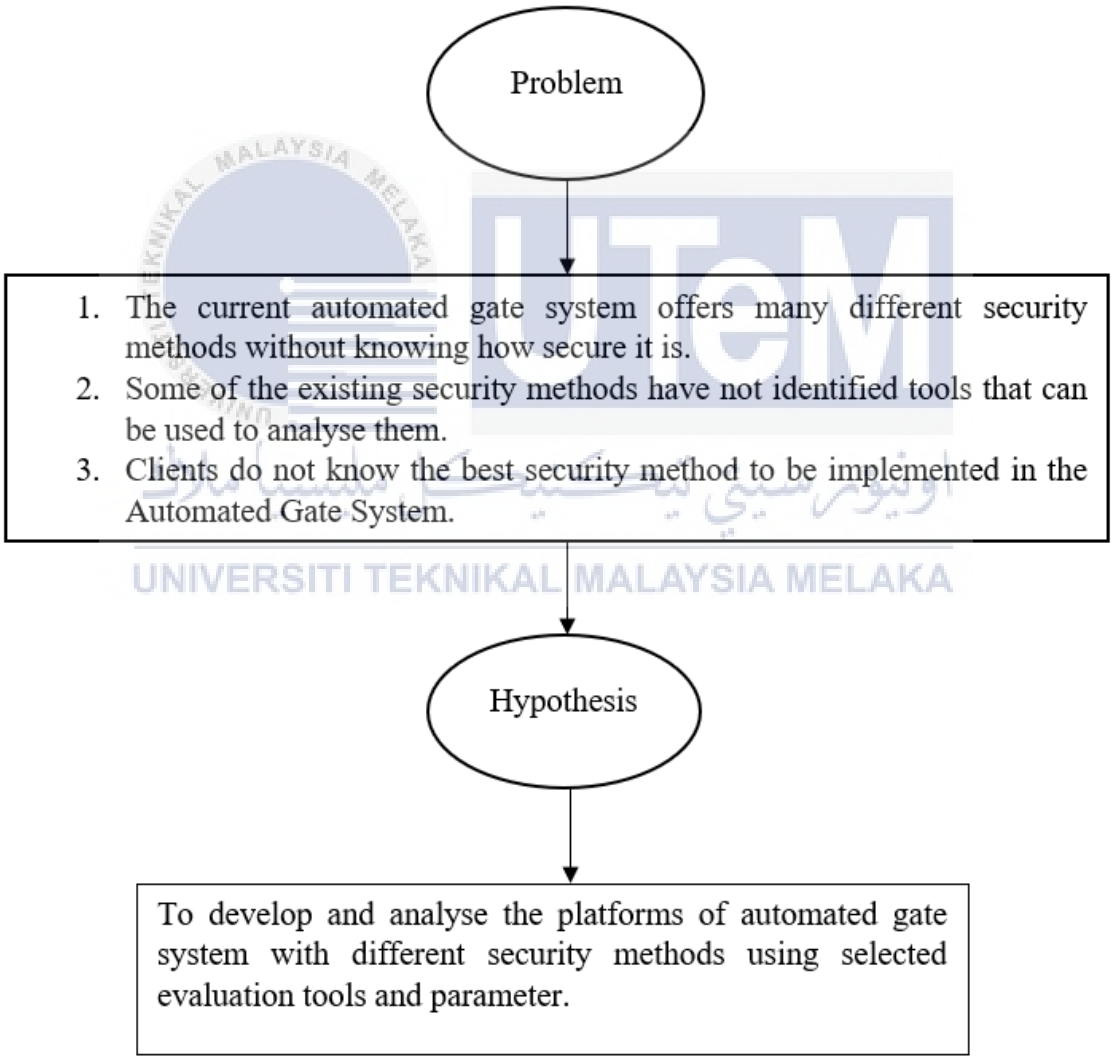


Figure 1.1 Project Research Hypothesis

1.6 Project Scope

The main purpose of this research is to develop a platform of Automated Gate System with different security methods that is worth the money. The security methods will be analysed one by one, using selected tools to find out which security methods can offer the best security to be implemented in the Automated Gate System. After going through many aspects, such as the cost, installation fees, the most common security methods used in the current gate system, three security methods will be analysed using specified tools and techniques.
Techniques will be identified based on the types of security testing and after techniques have been identified, tools can be figured out.

Moreover, the system users will be the valid users and security department in the company. Any activities at the gate will be recorded for security purposes and if any unauthorized users are detected entering the properties, security department will be notified immediately to take any rapid response action.

The platform develop will then be analysed using the tools that will be promoted during project design phase. A literature review will be done to choose the tools that could be used to analyse the security methods listed.

1.7 Project Contribution

Project contribution defines the expected output from this project. This part can be referred to the objectives of this project. The project contribution can be referring to the Table 1.3 below.

Table 1.4 Project Contribution

PC	Project Contribution
PC1	Security methods that are going to be analysed are identified.
PC2	Proposed tools to analyse the security methods.
PC3	Proposed a platform that will be developed and analysed.

1.8 Conclusion

In conclusion, the Analysis of Security Method in Automated Gate System will be able to solve the problem that are facing by companies that know the importance of having a reliable security aspect. This analysis can help companies to choose the security method that will be implemented in the Automated Gate wisely. Companies can also have extra choices to choose and to decide which security methods are suitable to be implemented.

CHAPTER 2: LITERATURE REVIEW

2.1 Introduction

This chapter will be discussing about the background of the security methods, the domain and the keywords, problem and solution of the security methods that will be used for the gate system and to have a better understanding about the concept, technique and tools needed to be implemented in this project. This chapter will also contain the related publish information and material or article, previous project findings and research that are related to the objective of this project. The project title is Analysis of Security Method in Automated Gate System.

The domain of this project is to focus on the finding of the most secure security method to be implemented and tools to analyze the methods. The platform and software development will be using Arduino Uno.

2.2 Related Work

An automated gate system without a secure security method applied is a big loss as it is a part of defense system to protect the property from unauthorized access. Based on Shoewu and Baruwa's work (2006), they used a microprocessor to monitor two gates that has sensors to sense any approaches from a vehicle. The gates will automatically open after sensing a vehicle, wait for a specified time and then close. It can be seen that these gates do not provide any appropriate security methods since any vehicle can enter the property.

According to Asha, Syed, Jayashree and Vijayashree (2018), security is the most fundamental issue wherever on the planet these days. Gate system is a part of

security system that is widely used in companies, personal properties and housing area to protect them against any unwanted intrusion from the outsiders. Knowing what security methods to be implemented will strengthen the security, increase the efficiency and secure the property from burglary.

The idea of implementing automated gate system is not new as there are a lot of types already in the market. However, most of them are quite expensive and have a high installation fee. According to Erman, Lim, Nazrulazhar, Syarulnaziah and Zakiah (2018), installation and maintenance fees for automated gate systems in the market are expensive, which most of the small companies cannot afford to own. Erman et al. (2018) further described that small companies preferably taking risks not installing the gate system as they cannot afford the fee. Most companies will always go for the price first rather than paying attention on the security aspect. It is disappointing but companies are not at fault when they themselves do not know what the most reliable security method is to choose and the importance of implementing a secure security method.

Some of the existing and the most current security methods that are being implemented in the automated gate system are Radio Frequency Identification (RFID) technology (HR Choi, NK Park, DH Yoo, HK Kwon, JJ Shin, 2006), Biometric Identification system (Sanchez del Rio, Moctezuma, Conde, Martin de Diego, & Cabello, 2016), License Plate Recognition system (Al-Mahbashi, L. T. A., Yusof, N. A. T., Shaharum, S., Karim, M. S. A., & Faudzi, A. A. M., 2019) and QR Code (Hamid, Erman, Lim Chong Gee, Nazrulazhar Bahaman, Syarulnaziah Anawar, Zakiah Ayob, and Akhdiat Abdul Malek, 2018).

First, based on the work of HR Choi, NK Park, DH Yoo, HK Kwon, JJ Shin (2006), they were using RFID technology as a security method for the gate system. During the time they were working on the project in 2006, they have mentioned that the current security methods for automated gate system at that time were bar code and video identification technology. But bar code cards easily damaged that causes difficulty for the reading information process. For video identification, it offers better security than the bar code but it needs higher costs for installation and the possibilities to be affected by external

environments are high. Hence, they opted for RFID technology as it has a higher operational efficiency and can offer a tight global security. In this project, they had tested various positions of the tags and antenna to check identification rate along with two aspects which are truck access pattern and truck speed. After testing the tags with different position, access patterns and speed of the truck, the most optimal position were selected.

Another example for automated gate system using RFID is from Asha, Syed Navaz, Jayashree, & Vijayashree (2018) work. According to Asha, Syed Navaz, Jayashree, & Vijayashree (2018), the product that they worked on is made for administration, controlling, exchange activity and keeping up record of the different clients. Firstly, a new user will register with the system and the information of the new user will burn in RFID tag that will be accessible through the system. Then, whoever owns the RFID tag can enter to the property after the tag is put into the reader and the system admit the user as registered one and the information that in the RFID tag match with the information that is stored in the system. If the system recognised it as an imposter, the warning alarm will be triggered. Figure 2.1 will show the flowchart of system based on Asha, Syed Navaz, Jayashree, & Vijayashree (2018) work.

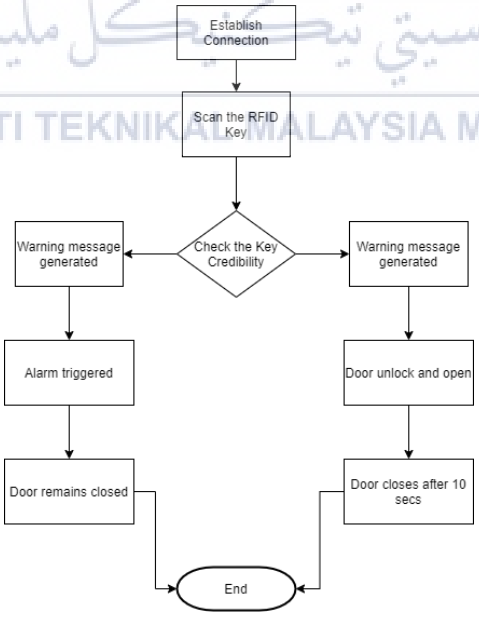


Figure 2.1 Flowchart of the system

(Asha. N, A. S. Syed Navaz, J. Jayashree, & J. Vijayashree, 2018)

Next, another security method that is implemented in automated gate system is License Plate Recognition System. Ismail Saad Eltoum and Zhaojun Xue (2014) proposed an automatic gate control system based on vehicle license plate recognition. According to Ismail Saad Eltoum and Zhaojun Xue (2014), the system is based on PIC microcontroller and regular PC with video camera to catch video frames that also include a vehicle license plate and processes them. To implement the algorithm, they have used MATLAB software, Proteus and Micro C. For the flow of the system, the car will stand in front of the barrier first and then the IR sensor will send signal to the microcontroller to send message to MATLAB. A welcome message will then be displayed on the LCD. The image of the license plate from the camera will be analysed in MATLAB, where most of the data analysis part were done. Then, the analysed image of the license plate will be compared with the information stored in the database. If it matched, MATLAB would send a message to the microcontroller to open the gate and will be close again after some time. But, if the information did not match, the alarm will be triggered and a "you are not allowed to enter, please go back." message will be displayed on the LCD. Figure 2.2 will show you the flowchart of the system.

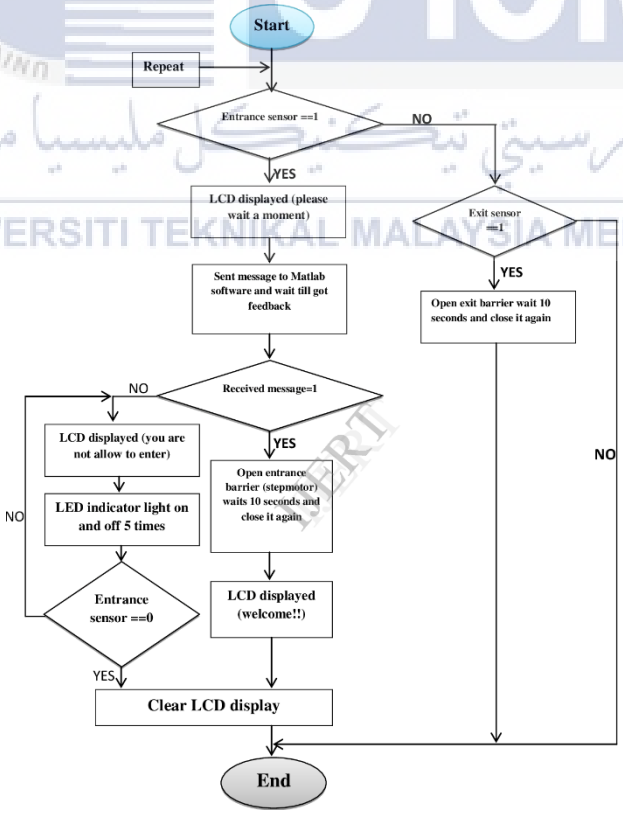


Figure 2.2 Flowchart of the process

(Ismail Saad Eltoum & Zhaojun Xue , 2014)

Next, QR Code is also one of the most recent security methods to be implemented in the automated gate system. Based on Erman, Lim, Nazrulazhar, Syarulnaziah and Zakiah (2018) paper, they have developed a QR code-based automated gate system. The main objective of the research is to develop a medium level security gate system mainly for small companies that cannot afford to install expensive auto gate system. Erman et al. (2018) further described that they implemented salted algorithm and hashing algorithm to increase the security level of the QR code and make it hard to crack. Figure 2.3 will show the example of the salted hashing algorithm.

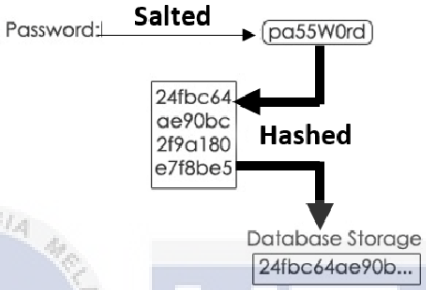


Figure 2.3 Example of the salted hashing algorithm
(Erman Hamid, Lim Chong Gee, Nazrulazhar, Syarulnaziah Anawar, & Zakiah Ayob, 2018)

To produce a high-quality output, they also implemented RAD technology, where according to M. A. Hirschberg (1998), RAD is a four-phase software development cycle that combines the element of Standard System Development Life Cycle. The flowchart of the workflow of the system will be shown in Figure 2.4.

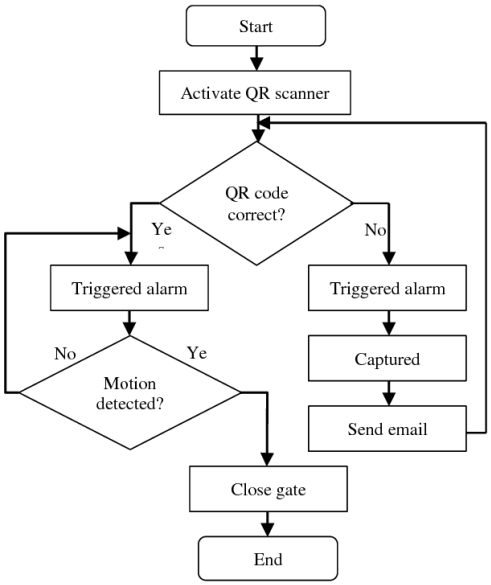


Figure 2.4 Workflow of the system

(Erman Hamid, Lim Chong Gee, Nazrulazhar, Syarulnaziah Anawar, & Zakiah Ayob, 2018)

Lastly, for Voice Recognition System, referring to a paper titled 'Biometric Voice Recognition in Security System wrote by Hairol Nizam Mohd. Shah, Mohd. Zamzuri Ab Rashid, Mohd. Fairus Abdollah, Muhammad Nizam Kamarudin,Chow Kok Lin and Zalina Kamis (2014), it is stated in the paper that voice recognition is safe for the administrator user as this technology use the user features parameter as the password and it is unique for everyone. Based on Hairol Nizam Mohd. Shah, Mohd. Zamzuri Ab Rashid, Mohd. Fairus Abdollah, Muhammad Nizam Kamarudin,Chow Kok Lin and Zalina Kamis (2014), voice biometric technology is more convenient and accurate for authentication use as the user has nothing to be carried or remember any password and scared the ID card might being stolen or being hacked. The voice recognition system has two main modules which are feature extraction and feature matching, while the speech signal and its characteristics can be represented in two different domains which are time and frequency domain. They implemented this system by using MATLAB (SIMULINK). Users have to speak their names and saved it in the .wav file form. Severable variables such as pitch, dynamics and waveform are included and executed to recognize the user voice by using the function block that available in SIMULINK. Figure 2.5 shows the speaker verification process involved in Voice Recognition System.

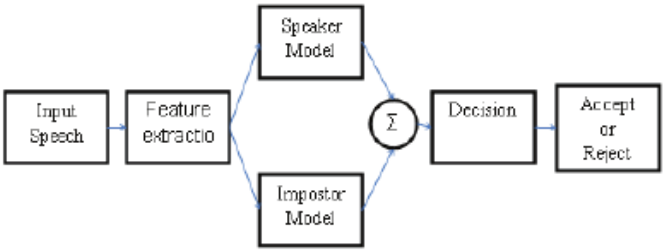


Figure 2.5 Speaker Verification

(Hairol Nizam Mohd. Shah, et al., 2014)

For this project, Hairol Nizam et al. (2014) use MATLAB and Arduino. For MATLAB software, it is used for the voice recognition part while Arduino software is used to focus on the communication system part.

Next, to complete this analysis, the chosen platforms have to be tested before being analyzed to identify which security method is the most secure. Security testing is a type of software testing that helps to uncover vulnerabilities of a system and focuses on finding any possible loopholes and weaknesses of the system (Software Testing | Security Testing, 2019). Security testing can help to identify threats and measure any potential vulnerabilities of the system. It also can help to detect any security risks in the system. For security testing, there are various types that we can choose from such as vulnerability scanning, security scanning, penetration testing, risk assessment and many more. For this analysis, vulnerability scanning and penetration testing are chosen as the security testing type.

Based on Yugansh Khera, Deepansh Kumar, Sujay, Nidhi Garg (2019), vulnerability scanning is the process of discovering and identifying loopholes in the system. Individuals or network administrators can use vulnerability scanning for security purposes, or hackers might use it to obtain unauthorized access to computer systems. Various strategies and approaches will be used to elicit a response from devices within the target scope, depending on the type of scan used by the vulnerability platform. The scanner will attempt to match the findings to a database and assign risk ratings (severity levels) depending on the response of the devices. Vulnerability scanners may be set up to check all network ports for password breaches as well as suspicious apps and services. The scanning service notifies users of security updates or missing service packs, detects malware and code weaknesses, and keeps track of remote access. Unauthenticated scans and authenticated scans are the two types of scans commonly used in vulnerability scan. Unauthenticated scans are those that are performed via the internet or using scanners that are installed locally. This technique does not require a login or an agent.

These scans are vital because they identify vulnerabilities that a hacker can exploit to get access to your system. Because hundreds of new vulnerabilities are discovered every week, such scans should be performed as frequently as needed. Authenticated scans are carried out by enabling the scanner privileged access to the system. This gives the scanner additional information and helps it to identify additional risks from within, such as weak passwords, dangerous malware, installed programs, and configuration problems. The approach may be used to mimic the damage that a system user with specified access may do.

Also referring from Yugansh Khera, Deepansh Kumar, Sujay, Nidhi Garg (2019), the paper is discussing and analysing about life cycle of VAPT process and VAPT tools for finding vulnerabilities in system. VAPT is Vulnerability Assessment, also called as Vulnerability Scanning and Penetration Testing. The process of VAPT is first, connect to IP Address, scan ports (TCP/UDP), map services, report vulnerability and find or exploit the vulnerability. Moreover, there are four vulnerability scanning testing methods that are being discussed in this paper which are Active Testing, Passive Testing and Network Testing. For Penetration Techniques, there are three that are being discussed in this paper which are Funtional Testing, Grey Box Testing and Glass Box Testing. Yugansh et. al (2019) further described that the life cycle of VAPT is a bit lengthy process, that includes Scope, Reconnaissance, Vulnerability Detection, Information Analysis and Planning, Penetration, Privilege Escalation, Result Analysis and Reporting & Clean-up. In this paper, the advantages of VAPT are it can give details about the threats of an application, discovering programming flaw in a system, secure system from malicious attacks and many more. The tools that are used in VAPT and discussed in the paper are WireShark, Nmap, Metasploit, Air crack, Injection and many more. Yugansh et. al (2019) further discussed that by using VAPT technique, a user can discover the vulnerabilities that can result in a variety of harmful attacks such as Denial of Service (DoS) attack, Router Advertisements (RA) flooding and many more.

There are one more paper that discuss about VAPT which is based on Keyur Patel (2019), he discussed about a survey on VAPT for secure communication. This paper discusses about the types of vulnerabilities, as mentioned from the paper that a survey found that minimum 30-40 vulnerabilities found on a daily basis. The survey conducted by CVE details says that 14,600 vulnerabilities were reported in 2017, compared to 6447 in 2016. Keyur Patel

(2019) mentioned that VAPT offers many benefits for the organizations such as a detailed view of potential threats and risks faced by an application can be provided, it can identify the security errors which is left while the creation of the application which leads to cyber-attacks, can provide risk management and also a perfect security model for the organization and many more. The tools discussed are mostly the same as the paper from Yugansh Khera, Deepansh Kumar, Sujay, Nidhi Garg (2019), which are WireSharks, Metasploit, Nessus, NMAP and many more.

Based on Derrick Rountree (2011), the procedure of trying to identify and exploit vulnerabilities in your environment is known as penetration testing, or pen testing. Penetration testing is carried out to provide you an understanding of not just the vulnerabilities that exist, but also the potential damage that these flaws may do if they were exploited. Testing is carried out in an approved and systematic manner in order to report and correct errors. Ethical hackers use pen testing to put themselves in the shoes of harmful hackers. Network owners define a pen testing scope that determines which systems are eligible for testing as well as the duration of the test. Requirement analysis establishes standards, as well as the tone and limits of what the testers may and cannot perform. The ethical hackers set to work scanning for ways into the network after establishing a scope and timeline. A vulnerability scan is generally the first step of a test to find potential open ports into a network. Misconfigured firewalls, for example, might be one of these vulnerabilities. Once a system has been hacked, the tester might attempt to acquire access to privileged accounts in order to investigate the network further and obtain access to other vital systems. Escalation techniques are used by pentesters to study a network and determine what the worst-case scenario may be. Depending on the breadth of the pentest, tests can acquire access to networks in a variety of unorthodox methods.

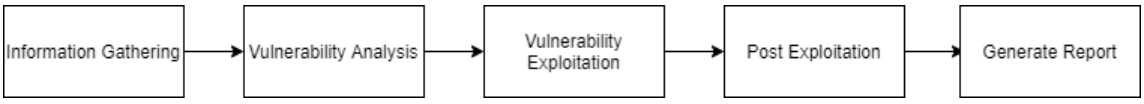


Figure 2.6 The Process of Penetration Testing

Next, for static code analysis, based on McGraw and Chess (2004), Static analysis tools evaluate a program's text statically, rather than attempting to run it. They may theoretically inspect either the source code or the compiled version of a program. Although deciphering the latter might be challenging, both forms of the software can be beneficial. Static analysis tools surpass manual audits because they're faster, allowing for more frequent program evaluations,

and they encapsulate security data in a way that doesn't need the tool operator to have the same depth of security experience as a human auditor. The fact that security vulnerabilities frequently reside in hard-to-reach states or appear under unexpected settings makes testing for them difficult. Static analysis tools can look into more of a program's dark corners with less effort than dynamic analysis, which needs the program to be performed. Static analysis can also be used before a program reaches the point where significant testing can be done. The result of a static analysis tool still has to be evaluated by humans. There's no way for a tool to automatically figure out which issues are more or less significant to you, therefore there's no way to avoid sifting through the data and deciding which issues should be repaired and which pose an acceptable degree of risk. Even non-security professionals should be able to utilize good static analysis tools. This implies that their findings must be intelligible to non-security engineers, and that they must teach their users about proper programming practices. Another important characteristic is the type of knowledge (rule set) enforced by the instrument. The significance of having a good rule set cannot be overstated.

Lastly, a study investigates whether it is possible to produce repair suggestions for common warnings generated by static code analysis tools automatically, and to what degree developers are ready to integrate such proposals into the codebases they manage. FindBugs and SonarQube are two static code analysis tools that are extensively used on open-source and industrial projects to discover a variety of problems that might degrade software quality (Marcilio, Furia, Bonifácio, & Pinto, 2020). Despite the ubiquity of these tools and their high degree of automation, numerous empirical studies show that developers only repair a tiny percentage of identified issues—so-called ‘‘warnings"—typically less than 10% (Marcilio et al., 2019).

For the accuracy analysis, a Voice Recognition system is tested in a paper by Hairol Nizam Mohd. Shah, Mohd. Zamzuri Ab Rashid, Mohd. Fairus Abdollah, Muhammad Nizam Kamarudin,Chow Kok Lin and Zalina Kamis. Based on the paper, they did two experiments to analyse the accuracy of the system, which are accuracy of their own voice an accuracy analysis using other people’s voice. In the accuracy analysis, the experiment is done 20 times to analyse the accuracy of their own voice and the system failed to recognize the voice for 5 times. Hence, they abled to achieve 75% accuracy for the voice recognition system (Hairol Nizam Mohd. Shah, et al., 2014). Next, for QR Code System, an accuracy has been analysed in a paper by Erman Hamid, Lim Chong Gee, Nazrulazhar, Syarulnaziah Anawar and Zakiah Ayob. In the paper, QR Code is implemented in the automated gate system and being analysed for 100 times.

As mentioned in the paper, the system is 99% accurate (Erman Hamid, Lim Chong Gee, Nazrulazhar, Syarulnaziah Anawar, & Zakiah Ayob, 2018).

However, based on Shubhankar Rawat (2019), accuracy is not the only measure that we need to focus on. Also mentioned by Paras Varshney (2020), due of its simplicity in assumptions, accuracy is not really a useful metric for model evaluation. For imbalanced data, he wrote that the class data is usually not equally distributed in real-world issues, with certain classes having a high frequency and others having a low frequency. Consider the medical situation of cancer patients: 90 percent of the data comes from people who do not have cancer, whereas 10% of people have been diagnosed with cancer. In this example, an untrained rule-based model may likewise forecast all points as negative with a 90% accuracy, which can be quite harmful in many situations. Next, for probability estimation, unlike other measures, accuracy does not have the understanding of probability estimations coming from the model instead it will consider only the binary values into consideration. So a model classifying positive and negative values with a probability values of 97% and 3% respectively is given the same accuracy as the other model which will do the same with 62% and 38% probability values, but we know that the first model is much better than the second one, and here accuracy fails to evaluate that. Thus, another metric has to be added to measure and analyse the security methods.

2.3 Critical review of current problem and justification

As we have discussed earlier, automated gate system has been implemented with many security methods. There are most recent and common security methods and a lot of research has been carried out for these security methods which are RFID Technology, QR code, Biometric Recognition and Voice Recognition.

Firstly, in the aspect of expenses and fees, for RFID technology, it can offer a tight security with a high efficiency. However, based on Elechi, Ahiakwo and Shir (2021), RFID technology is not affordable and high cost is needed. Despite the cost, according to Asha, Syed Navaz, Jayashree, & Vijayashree (2018), RFID can be effortlessly accessible and more helpful to utilize. Although RFID technology has been known to be quite costly, there are also a low-cost RFID tag. However, based on Juels A. (2005), they are computationally weak devices that cannot perform basic symmetric- key cryptographic operations. Unlike RFID,

QR code is a low-cost implementation for automated gate system. According to Erman, Lim, Nazrulazhar, Syarulnaziah and Zakiah (2018), a medium-level security can be developed with minimum cost. This is due to the technology and RFID is offering a higher level of security than QR code. Hence, the installation and maintenance fees will be higher. For Vehicle License Plate Recognition system, it is cheaper compared to RFID technology and Biometric Recognition that needs a higher installation and maintenance fees. For cost, QR code offers the lowest cost in total and is affordable for any clients who have a tight budget.

Although these security methods offer a tight security and have many security benefits, it also exposed to many privacy and security threats and risks. Based on Tiago M. Fernández-Caramés, Paula Fraga-Lamas, Manuel Suárez- Albela, Luis Castedo (2017), RFID are exposed to two kinds of risks which is security risks and privacy risks. For security risks, the most common attacks are tag isolation, which is blocking the tag communications to avoid sending data to the reader. Next is tag cloning. Tag cloning is the unique identifier and the content of the RFID tag is extracted and inserted into another tag to access restricted areas. For privacy risks, personal tracking is dangerous as the attacker can know the routes, purchases and habits of the owner of the RFID tag. The information may even be used for marketing purposes.

For QR Code, it is widely known that it is easy to crack and decode. However, the security of QR code can be higher when security features are added. But still, the risks of getting attacks are still there and one of it is phishing. Phishing using QR code is easy as all they need to do is put a sticker with the QR code that leads them to the malicious websites. Most people are not aware of the threats out there and there is only a few awareness about phishing using QR code. This is crucial as people out there just scan the QR code without even knowing the context of the QR code. For biometric and license plate recognition, data breaches can happen. Because of the data are collected and stored to do the recognition process, this can be constant threats from the hackers and a lot of security precautions need to be taken in order to protect clients' sensitive data.

Next, in the aspect of the scanning process, only RFID technology and QR code support 360 degree of reading that makes scanning process faster and easier. It is efficient when there are a lot of scanning process to be done at the same time. Meanwhile, for the range, RFID and Vehicle License Plate Recognition allow a longer range compared to Biometric as the data type for Biometric are either eyes, face or hand palm that needs a shorter range to be identified. Thus, using Biometric, Vehicle License Plate Recognition and QR

code, they can be read and scan one by one at the same time, while RFID can be scan and read many times at a time. Table 2.1 will show the comparison of the security methods.

Table 2.1 The comparison of the security methods

	Biometric Recognition (Voice Recognition System)	RFID technology	Vehicle License Plate Recognition	QR code
Cost	Expensive	Expensive	Cheaper than RFID	Cheapest
Efficiency	Can only scan and read once at a time	Can read and scan many times at once	Can only scan and read once at a time	Can only scan and read once at a time
Scan Range	Short	Longest	Long	Short
Advantage	Offers the best security level and accurate most of the times.	Efficient and tight security.	Real time detection and recognition process.	Low in cost and flexible.
Disadvantage	Too expensive .	Cannot be used if the card or RFID tag is lost and it is expensive to setup and install.	Bad weather or lighting can affect the system and the system will not be completel y effective.	Can be decoded easily

Lastly, to analyse the security methods, some of it have not identified specific tools that can help them to know how secure the security methods can be. It is important as

clients need to know how secure each security methods can be, in order to protect their properties from unauthorized access. Plus, clients need to know what security method to choose to invest for a better security. Based on Keyur Patel (2020), security testing is important as it can discover and evaluate potential vulnerabilities in a system so that attacks can be faced and the system does not stop working or be exploited. It also aids in the detection of any potential security concerns in the system, as well as assisting developers in the resolution of issues through code. Based on a question from Jawad Awan on Research Gate, there are an answer from Narendranath Tangudu that said, before the security method can get evaluated, the vulnerabilities need to be discovered first. Narendranath also mentioned that find the vulnerabilities, determine the risks of exploiting these vulnerabilities, and do a risk analysis for each potential threat. This adds a layer of protection. Its security posture may be assessed based on how threats are resolved (accept, mitigate, transfer). According to Vyacheslav, security is always relative, and any compliance standards might act as a guideline.

2.4 Proposed Solution

Based on the critical reviews, to overcome the problems and weaknesses, an analysis will be done to choose which is the best and the most secure security methods to be implemented. In this analysis, from the current security methods that we have stated earlier, three of them that fulfil the criteria will be chosen to be analyzed and developed to be implemented in the automated gate system. The security methods that have been chosen to be analyzed are RFID technology, QR code and Voice Recognition System as it is accurate in scanning and have a lot of advantages in the security aspect. A proper analysis can help the clients to choose the best security method to be implemented to protect their properties as it is an investment to splurge a lot of money for a gate system.

To identify tools to analyze each different security methods, we have to know what type of security testing that we are going to focus on. The parameters that we are going to use to analyse the platforms are static code analysis, accuracy analysis, scan time and scan range. Analysis will be made based on the parameters mentioned. For the static code analysis, Sonarqube and VisualCodeGrepper will be used to analyse the code to figure if there are any vulnerabilities in the code of the platforms. Accuracy analysis will be done using the platform, scan time will be analysed using the time taken for the platform to finish scanning and scan range is the range for the platform to scan.

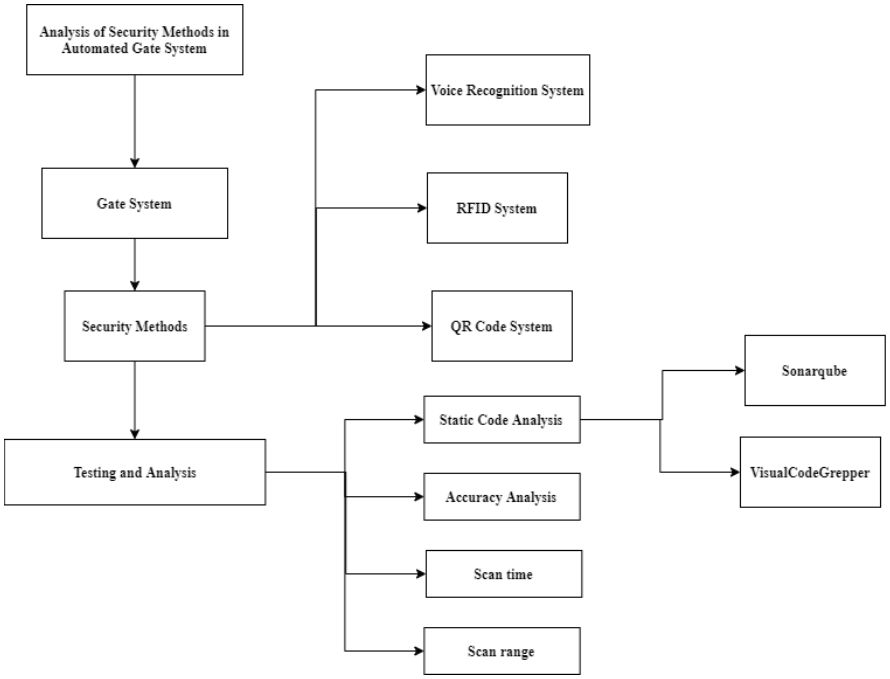


Figure 2.7 Flow of the project

2.5 Conclusion

In conclusion, this analysis will be focused on analyzing the security methods by using three security methods that have been mentioned earlier with selected and specific tools. The finding of the analysis will be recorded. The next chapter will be discussed on how the analysis is done step by step in this project.

CHAPTER 3: METHODOLOGY

3.1 Introduction

Methodology is the various procedures or techniques used to classify, pick, process and analyse knowledge about a subject. In this project, the methodology is the procedures that will be used to collect data and result to achieve the objectives of the research. There are many types of methodology that can be applied to different types of situations and developments. Some of them are Waterfall, Agile, Lean and Rapid Application Development (RAD). Each methodology has their own advantages and criteria that you can choose to suit your project needs. For this project, the most suitable methodology that will be applied to help the progression become smoother and can be conducted in the correct way is Waterfall methodology. For this project, Waterfall methodology is perfect as it is plan-driven and the phases need to be completed before moving on to another phase. The SDLC is divided into separate phases, such as requirements gathering, analysis and design, coding and unit testing, system and user acceptability testing, and deployment, using a sequential method.

3.2 Research Process

Research Process is the step-by-step development of this project. Based on Erman, Lim, Nazrulazhar, Syarulnaziah and Zakiah (2018) paper, Data Collection, analysis, Design and Implementation are the stages that are used. For this analysis, there are several stages that must be followed, which are Literature Review, Preliminary Research, Design, Implementation, Testing and Analysis process. Every stage is crucial to successfully carry out this project. The figure below is the flow of the research process.

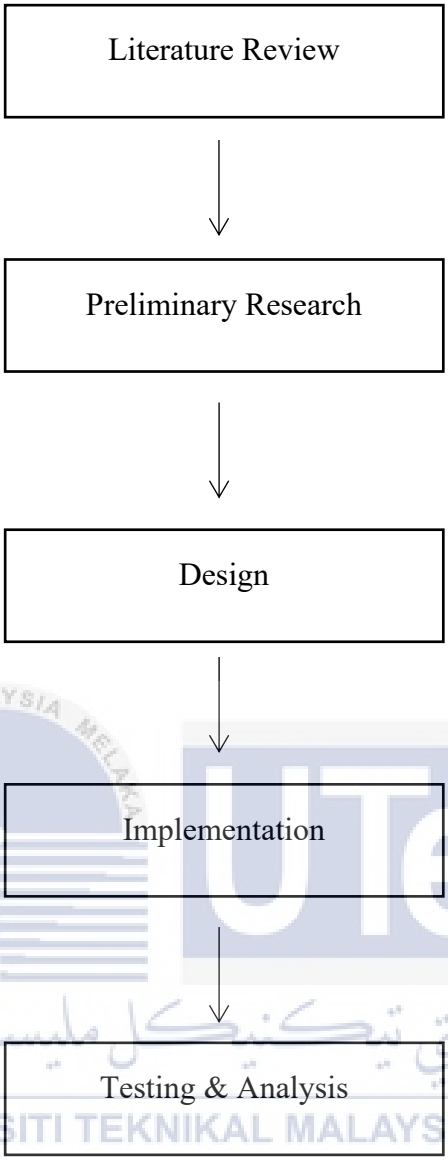


Figure 3.1 Flow of Research Process

3.2.1 Literature Review

Based on the previous research, three security methods have been chosen based on specific criteria. Before the security methods are picked to be analysed, they are being compared based on the cost, efficiency, scan range, advantages and disadvantages. From the comparison, QR Code, RFID technology and Voice Recognition System are the security methods that have been chosen.

Before choosing the right methods to be analysed, a literature review is done so that the pros and cons of the methods are clear and it will be easy to conduct the analysis. For the QR Code, it is based on Erman, Lim, Nazrulazhar, Syarulnaziah and Zakiah (2018) paper. In the paper, the QR Code that is developed is implemented with salted and hashing algorithm to increase the security level of the QR Code and achieve a medium-level security gate system, focused to help small companies with a tight budget to spend on a gate system. Next, for RFID technology, based on Ria Mutiara Sari, Eka Sabna, Refni Wahyuni and Yuda Irawan (2021), they develop a housing gate portal using RFID Card by using Arduino Uno in C++ language. To test the scan range, they blocked the RFID module with an object to see if the module can still read the signal from the RFID card and test out how far the distance to scan the card. They also did an experiment using card that have been registered and card that are not registered to see the result. There is no algorithm to strengthen the security level applied to this method. For Voice Recognition System, a paper from Hairol Nizam Mohd. Shah, Mohd. Zamzuri Ab Rashid, Mohd. Fairus Abdollah, Muhammad Nizam Kamarudin, Chow Kok Lin and Zalina Kamis (2014) is referred as they proposed a biometric voice recognition in security system. According to Hairol Nizam Mohd. Shah, Mohd. Zamzuri Ab Rashid, Mohd. Fairus Abdollah, Muhammad Nizam Kamarudin, Chow Kok Lin and Zalina Kamis (2014), the system is based on MATLAB and Arduino for the software. The system has a speaker recognition system process used to train automatically and computationally feasible to use. The voice recognition is also divided into two phase which are training and testing phase. The voice is collected for up to one second during the training phase. The actual delivered speech will next be detected using silence detection. After that, the signal is windowed. The Fast Fourier Transform is the first transformation, which converts a speech signal from the time domain to the frequency domain. Mel Frequency Cepstrum is converted by the MFCC.

Hairol Nizam et al. (2014) also mentioned in the paper that using voice biometric technology for authentication use is more convenient and accurate. It is also mentioned that it is safe for the administrator user.

For testing phase, the parameters that are going to be used are static code analysis, accuracy analysis, scan time and scan range.

To verify the accuracy of the theory that is discussed in the Literature Review, a questionnaire is done and the result of the questionnaire will be discussed in the 3.3.2 Preliminary Research.

3.2.2 Preliminary Research

For preliminary research, a questionnaire is done with 20 respondents is done as the scope for this project is small. This preliminary research result will be used to compare with the finalized result later. Based on the online research and questionnaire analysis, the result shows that most client do not pay attention on the security aspect. Although there are a lot of security methods that are implemented on the automated gate system, most client do not know the importance of having a secured gate system, protecting their property.

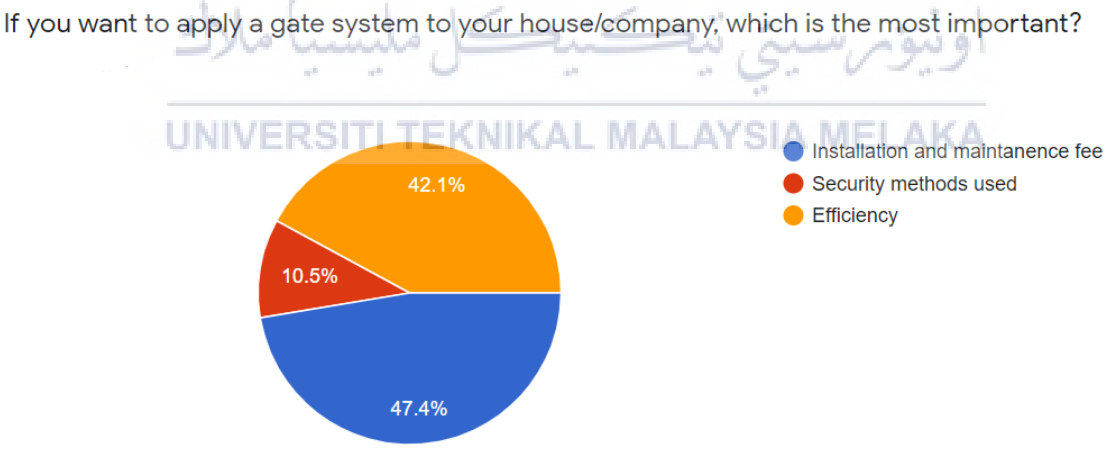


Figure 3.2 Important Factors

As we can see in Figure 3.2, clients always pay more attention to the cost rather than security aspect. This is very risky and dangerous. Only 10.5% think that security method is important when applying a gate system.

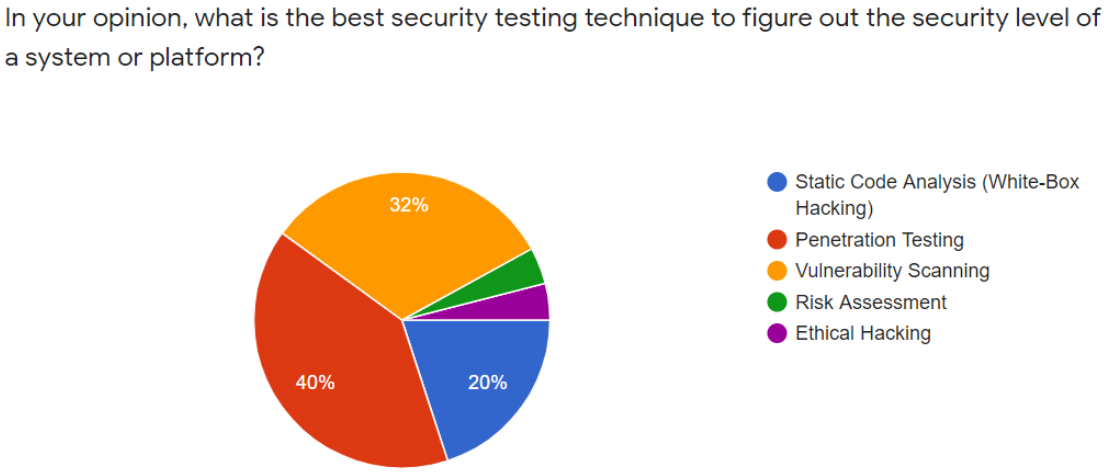


Figure 3.3 The best security testing technique

Besides that, from Figure 3.3, most of the clients agreed that Penetration Testing and Vulnerability Scanning are the best security testing technique to figure out the security level of a system.

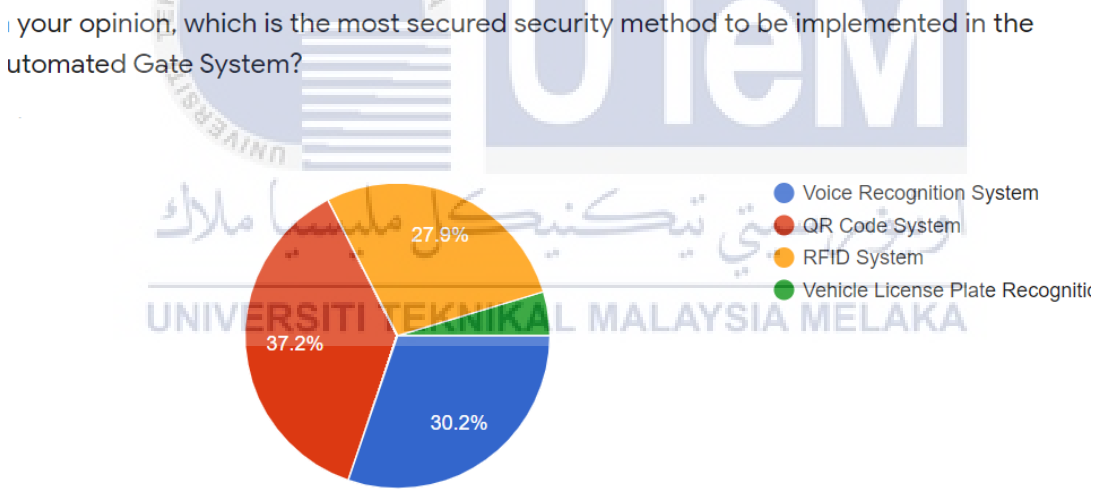


Figure 3.4 The most secured security method

Figure 3.4 shows that 37.2% of the respondents think that QR Code system is the most secured system method. Result of this analysis will be showed in Chapter 6: Testing and Analysis if it is true that QR Code Recognition system is indeed the most secured security method.

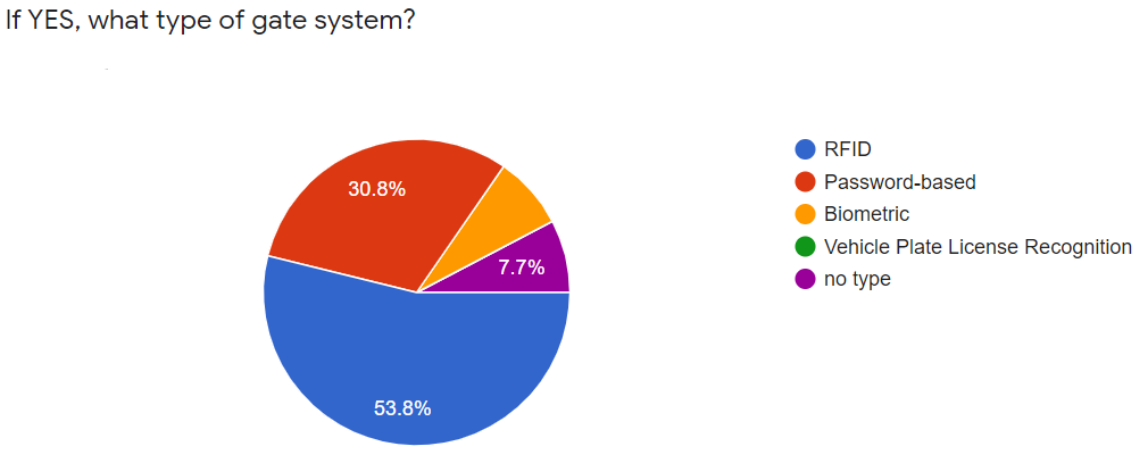


Figure 3.5 Type of Gate System

From there, majority of the client installed a RFID-based gate system and 30.8% installed a password-based gate system. Looking back at Figure 3.2, 42.1% choose 'Efficiency' as the most important when choosing a gate system. RFID is the most popular based on this questionnaire.

3.2.3 Design

a. System Architecture Design

System Architecture Design explained how the flow of the platform. For this project, three platforms will be created by using different security methods. The flow and details of the project design will be discussed further and deeper in Chapter 4: Design.

b. Tools & Technique

Tools and technique will be used in testing phase, before making an analysis to identify the most secured security methods based on the three platforms that have been chosen and created. To figure out and test the platforms, tools and technique have to be identified first. Based on Chapter 2: Literature Review, static code analysis, accuracy analysis, scan time and scan range are the parameters that will be used to identify the security level for each platform. To do the static code analysis, Sonarqube

and VisualCodeGrepper are the tools needed to analyse the platforms. To analyse the accuracy, the platforms need to be tested by running and scanning using security methods implemented in each platform. The accuracy will be calculated using appropriate formula. To figure out the time and range of scanning, each platform nee to be tested and record the result in table to be referred in Chapter 6: Testing and Analysis.

3.2.4 Implementation

For the implementation process, three platform will be done that consists of different security methods applied to each platform. The platforms are referred to existing development and system that have been executed successfully. The scenario is the same for all platforms, however the flow is slightly different.

a. QR Code

- **Hardware Connection**

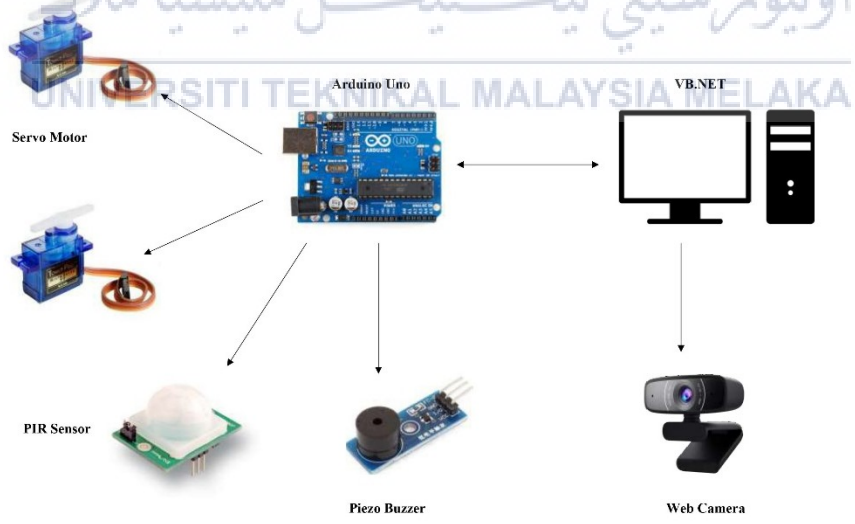


Figure 3.6 Hardware connection for QR Code System

Figure 3.6 above shows the connection of hardware that are implemented in this platform.

Servo motor – By using male to male jumper wire, the servo motor is attached to Arduino Uno microcontroller for gate in and gate out at pins 3 and 5. VB.NET software application is connected to Arduino Uno microcontroller via serial port and the rotation command will be send from VB.NET to Arduino Uno. Then, Arduino Uno microcontroller will interpret the command send from VB.NET and control the rotation of the servo motor.

Piezo buzzer – The piezo buzzer is attached to pin 9 and will be triggered if any unauthorized entries are detected, in order to alert the security department.

PIR sensor – PIR sensor will be attached to pin 12 and it is used to detect the motion of any vehicle, passing by the sensor. Once any vehicle is detected, the rotation of the servo motor will be controlled to make the gate closed by rotating it 90 degrees.

Camera – This will be used as QR Code scanner and security camera. QR Code scanner and security camera will be plugged in to the computer by using USB port. All the data gained from the camera has to be send to VB.NET software application to process and compare the data.

- **Software Development**

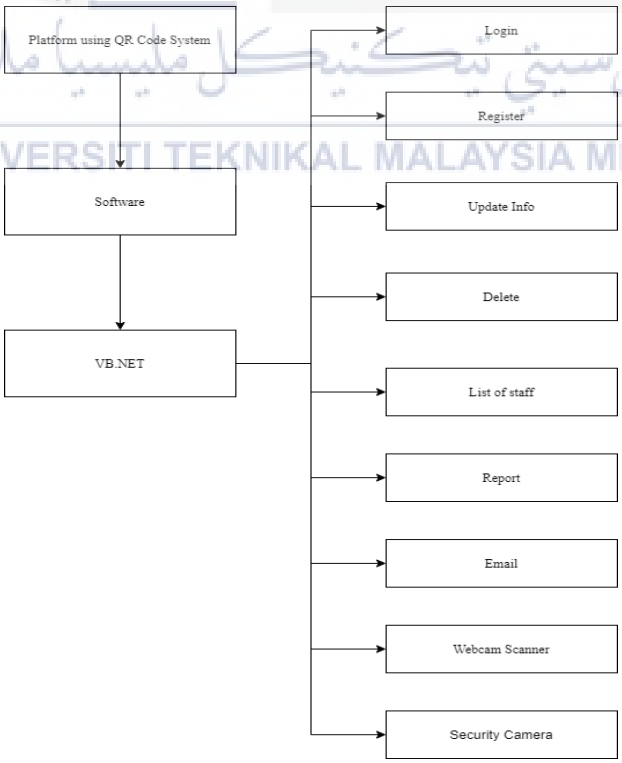


Figure 3.7 Software Connection for QR Code System

For this method, VB.NET Software Application will be used to monitor this platform. Figure 3.7 shows the functionality of the platform using QR Code as security method in details.

Login – This is an authorization process that allows only administrator to login and perform tasks in the software application such as staffs' registration, checking in/out records, activate security camera and more.

Register – This is a process to register and create accounts for any new staff. The information will be saved into the database and at the same time, QR Code will be generated.

Update Info – Staffs' information will be updated from time to time if there is any changes to be made such as phone number, emails or any credentials info to make sure their information is up to date.

Delete – The record that is saved can be deleted to avoid any confusion in the database.

List of staff - All staffs' information will be shown in a table and can be viewed by the administrator.

Report – Any entries will be recorded.

Email – An email will be sent out to the related department if there is any suspicious entries or activities found.

Webcam scanner – A programmed webcam is used as a QR code scanner to detect the QR code scanning for every entry process.

Security camera – The security camera is used to record any activities at the front gate. Any suspicious activities will be captured to be sent as an email to any department involved.

b. RFID

- **Hardware Connection**

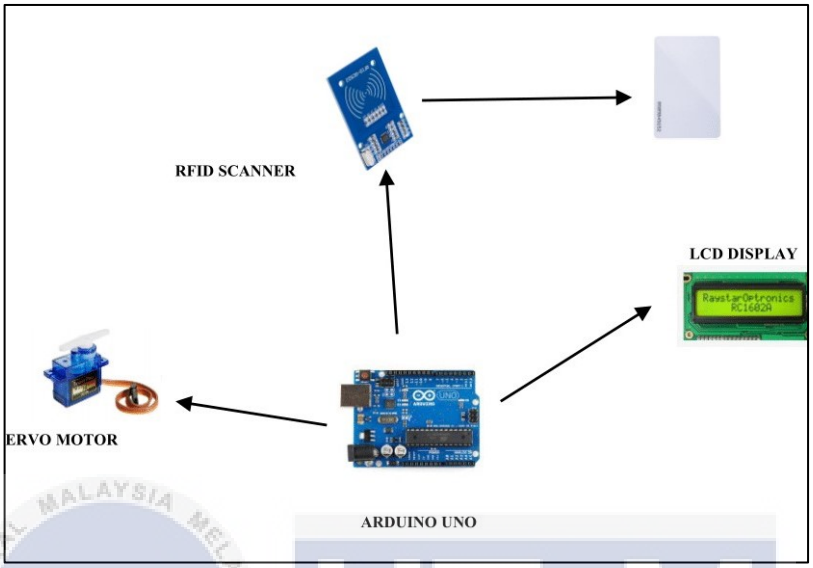


Figure 3.8 Hardware Connection for RFID

For this method, based on Figure 3.8, it shows the hardware connection for RFID system that is going to be implemented in Automated Gate System. The details of the hardware components will be explained below.

RFID Scanner – used to scan the RFID key card and check the credibility of the card based on information from database and will be attached on Arduino Uno microcontroller.

LCD Display – will be attached on microcontroller and will receive message from Arduino Uno microcontroller to generate message.

- **Software Development**

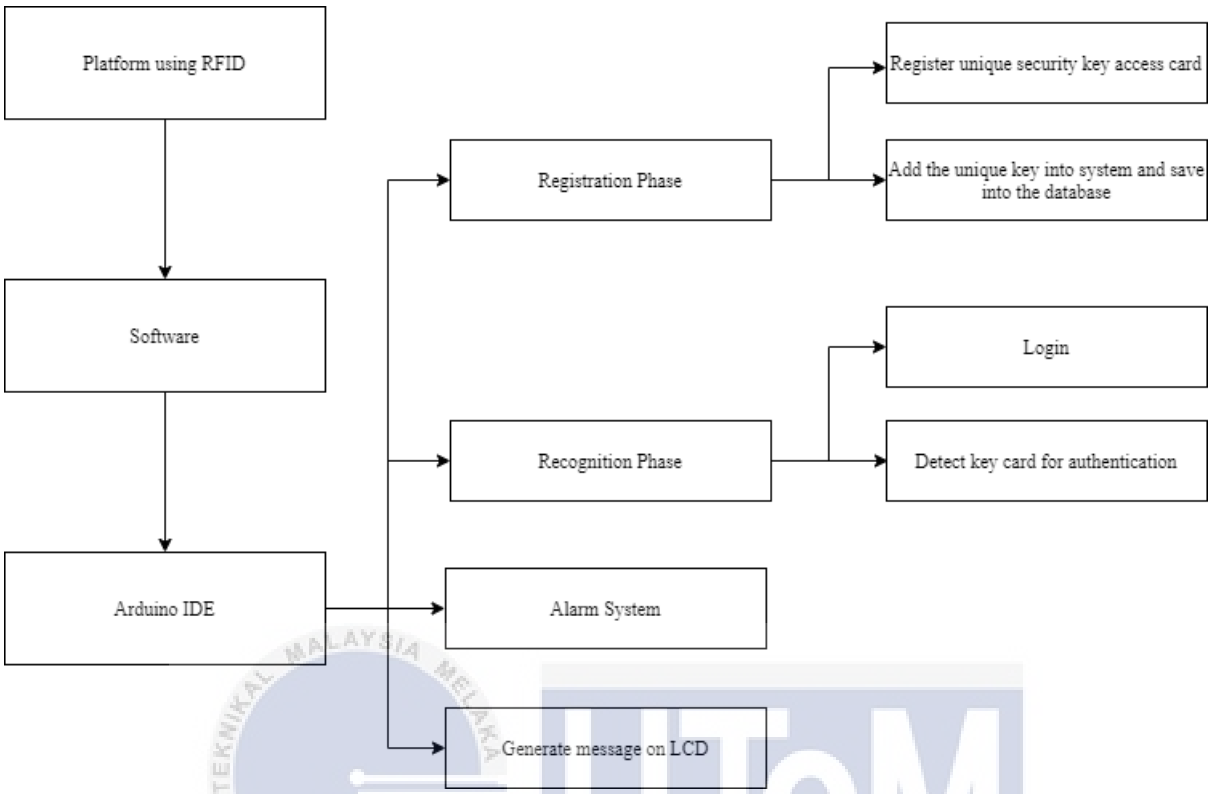


Figure 3.9 Software Development for RFID

Figure 3.9 shows the software development for RFID system. RFID system is using Arduino IDE as the software and have recognition phase, alarm system and message generated on LCD.

Registration Phase – first phase where all the registration of new unique security key access card are made. All the information will be saved into the database. A new user is initially added to the system, and the necessary information is stored on an RFID tag. The system will be able to read this RFID tag. When a registered user approaches the entry point and inserts the tag into the reader, the system verifies whether the person is a legitimate user or an impostor.

Recognition Phase – after all the information are stored, in this phase, whenever user scans the card at the RFID scanner, it would give access to enter the property if the information matched with the database. If not, entry is not possible.

Generate message on LCD – A welcome message will be generated if it is a legitimate user and a warning message will be generated if it is an impostor.

c. Voice Recognition System

- **Hardware Connection**

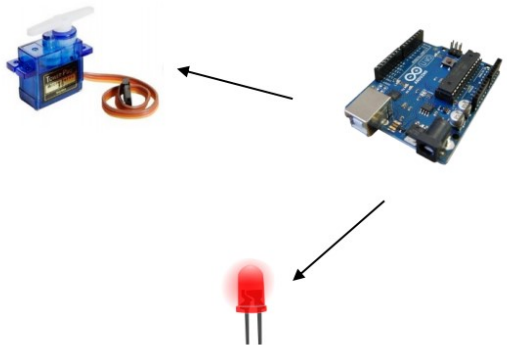


Figure 3.10 Hardware Connection for Voice Recognition System

Figure 3.10 shows the hardware connection for Voice Recognition System that is going to be implemented in Automated Gate System. The hardware components will be explained in detail below.

Servo Motor – The servo motor is attached to Arduino Uno microcontroller for gate in and gate out. Python is connected to Arduino Uno microcontroller and the rotation command will be sent from Arduino IDE to microcontroller. Then, the microcontroller will interpret the command sent and control the rotation of the servo motor.

- **Software Connection**

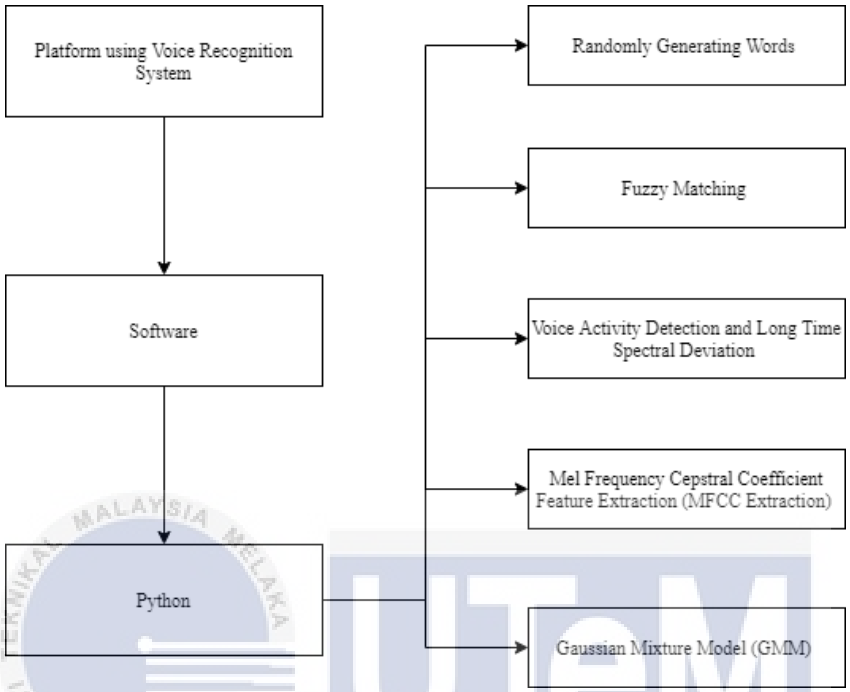


Figure 3.11 Software Development of Voice Recognition System

This platform with Voice Recognition System will be using Python IDE. Figure 3.11 shows the software development for Voice Recognition that has five (5) phases that are needed to go through to implement the security method in the Automated Gate System.

Randomly Generating Words – Users must speak three random words during the registration step, but only one random word is required for the authentication phase, which is produced automatically by the Python script. Only the system's chosen words are valid for users to use to authenticate their voices.

Fuzzy Matching – To detect what the user is saying and match it with the produced text, the system uses IBM voice to text service to determine what the user is saying. This is to avoid comparing the two strings and instead focus on determining how similar they are. Fuzzy logic is used to achieve this. The voice biometric solution recognizes the user's input as acceptable based on the given threshold. The fuzzy matches the words provided by the Google API to the words expected using the Python module FuzzyWuzzy.

Voice Activity Detection and Long Time Spectral Deviation – After the voice input has been received, the system must eliminate as much noise as possible before extracting any characteristics. There are two steps to this. Voice Activity Detection, for example, records background noise first and utilizes it to build a baseline for voice activity in the user's voice input. Then, using Long Time Spectral Deviations, pick those frames with voice activity. The user's voice input is filtered to remove the majority of the noise. To guarantee that the technology eliminates as much background noise as possible from the recordings it captures. Five second recordings of the background noise at the speaker's location were obtained to produce this voice activity detection (VAD).

Mel Frequency Cepstral Coefficient Feature Extraction (MFCC Extraction) – Then there's feature extraction. The MFCC algorithm is used to do this. This procedure begins by dividing the user's voice input into smaller windows for processing, then applying the discrete Fourier transform to one of the windows to get a short temporal Fourier transform. The filter bank coefficients are then obtained by running this through a Mel scale. The voice print is defined by a collection of characteristics. The models are then trained by using a discrete cosine transform to decrease the amount of features and produce the final set of features.

Gaussian Mixture Model (GMM) – Finally, a Gaussian mixture model is used to train the model. This is a clustering method that groups the many characteristics of a user's speech into a voice print. The voice print is then saved in a database of voice prints. The system will construct a Gaussian Mixture Model (GMM) for each user in order to authenticate them. A GMM may combine several Gaussians to create a distribution that reflects the chance of a feature vector landing in a given region, with the probability never being zero.

3.2.5 Testing & Analysis

Testing is a process of executing any system applications to make sure it is running well. There will be two types of testing involved in this phase, which are hardware and software application testing and security testing. Detailed explanation will be discussed more in Chapter 6: Testing and Analysis.

Hardware Testing: Hardware that are included in the hardware testing are webcam, Arduino Uno Microcontroller, PIR motion sensor, Piezo Buzzer, PIC16f877, LCD Display, IR Sensor, Indicator

Software Application Testing: Every created function of the system will be tested to make sure it will run smoothly. The database will also be tested to verify all information is successfully stored and can be used in the database.

Security Testing: Security testing will be done to start the analysis. Security testing is done based on the parameters that have been discussed earlier which are static code analysis, accuracy testing, scan time and scan range.

An analysis will be made after all platform is done and has been tested using the appropriate parameters and evaluation tools. In this phase, all of the platforms will be tested and analysed to study which security method is the most secure to be implemented in the automated gate system. Detailed explanation and analysis will be discussed more in Chapter 6: Testing and Analysis. This analysis will be a Testbed Analysis as all platforms are done referring to the existing developed system to be analysed using the result of the security testing.

3.3 Methodology

In this analysis, Waterfall model will be implemented as this methodology method is the most suitable because based on S.Balaji and DR.M.Sundararajan Murugaiyan (2012), this model is plan-driven and the phases need to be completed before moving on to another phase. Thus, Waterfall model do the testing phase until last half of a project and it suits the flow of this analysis. One of the characteristics of Waterfall model is it determines the end goal early. For this analysis, it was clear from the beginning what is the goal that I have to achieve at the end of this analysis.

The SDLC is divided into separate phases, such as requirements gathering, analysis and design, coding and unit testing, system and user acceptability testing, and deployment, using a sequential method.

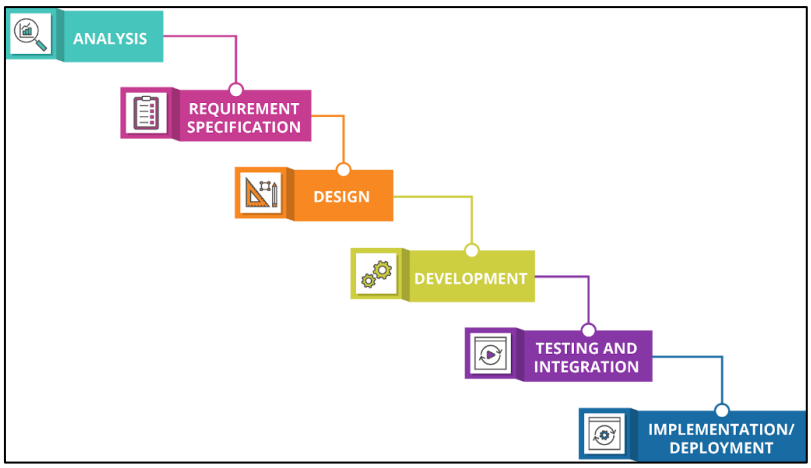


Figure 3.12 Process of Waterfall Model

3.4 Project Milestone

Project Milestone as a reference point that will be used to monitor the project's progress and marks the major activity in a project.

In order to make sure the flow of this project runs smoothly; a project milestone will be created to have a well-planned project and to ensure all of the activities in the project are able to complete in time.

Gantt chart will be able to track the progress of every chapter. Figure 3.13 shows the summary of the Gantt Chart table.

PSM GANTT CHART	START DATE	DUE DATE	DURATION
Proposal PSM	15/3/21	28/3/21	1 WEEK
Chapter 1: Introduction	29/3/21	11/4/21	1 WEEK
Chapter 2: Literature Review	12/4/21	25/4/21	2 WEEK
Chapter 3: Methodology	26/4/21	9/5/21	2 WEEK
Chapter 4: Design	17/5/21	23/5/21	3 WEEK
Project Demo	24/5/21	20/6/21	2 WEEK
PSM 1: Final Presentation	21/6/21	27/6/21	1 WEEK
Chapter 5: Implementation	1/7/21	1/8/21	4 WEEK
Chapter 6: Testing	2/8/21	16/8/21	2 WEEK
Chapter 7: Conclusion	17/8/21	24/8/21	1 WEEK
PSM 2: Final Demonstration (Product & Report)	25/8/21	18/8/21	3 WEEK

Figure 3.13 Gantt Chart

3.5 Conclusion

As a conclusion, this chapter explains the methodology that will be used in this project. The Waterfall methodology consists of different phases that will help the flow of this project to be smooth and efficient. The milestones set the time to finish the project so that the progression will always be in track. This is crucial to make sure this project can be done in time.

CHAPTER 4: DESIGN

4.1 Introduction

This chapter will define the results of the analysis of the preliminary design and the result of the detailed design.

The requirement analysis, including the hardware and software needed in this project are explained in this chapter. The block diagram architecture, proper analysis and flowcharts in detail for this project will also be stated to ensure this project can be completed and well designed.

4.2 Network System Architecture

To carry out this analysis, three platforms of gate system with different security methods need to be done and undergo several testing to figure out how secure the security methods are. From there, an analysis will be done based on the result of the testing. By the end of this analysis, the most secured method that can be implemented to the gate system will be identified based on the analysis of the testing result. Figure 4.1 shows the flow of the analysis in a big picture.

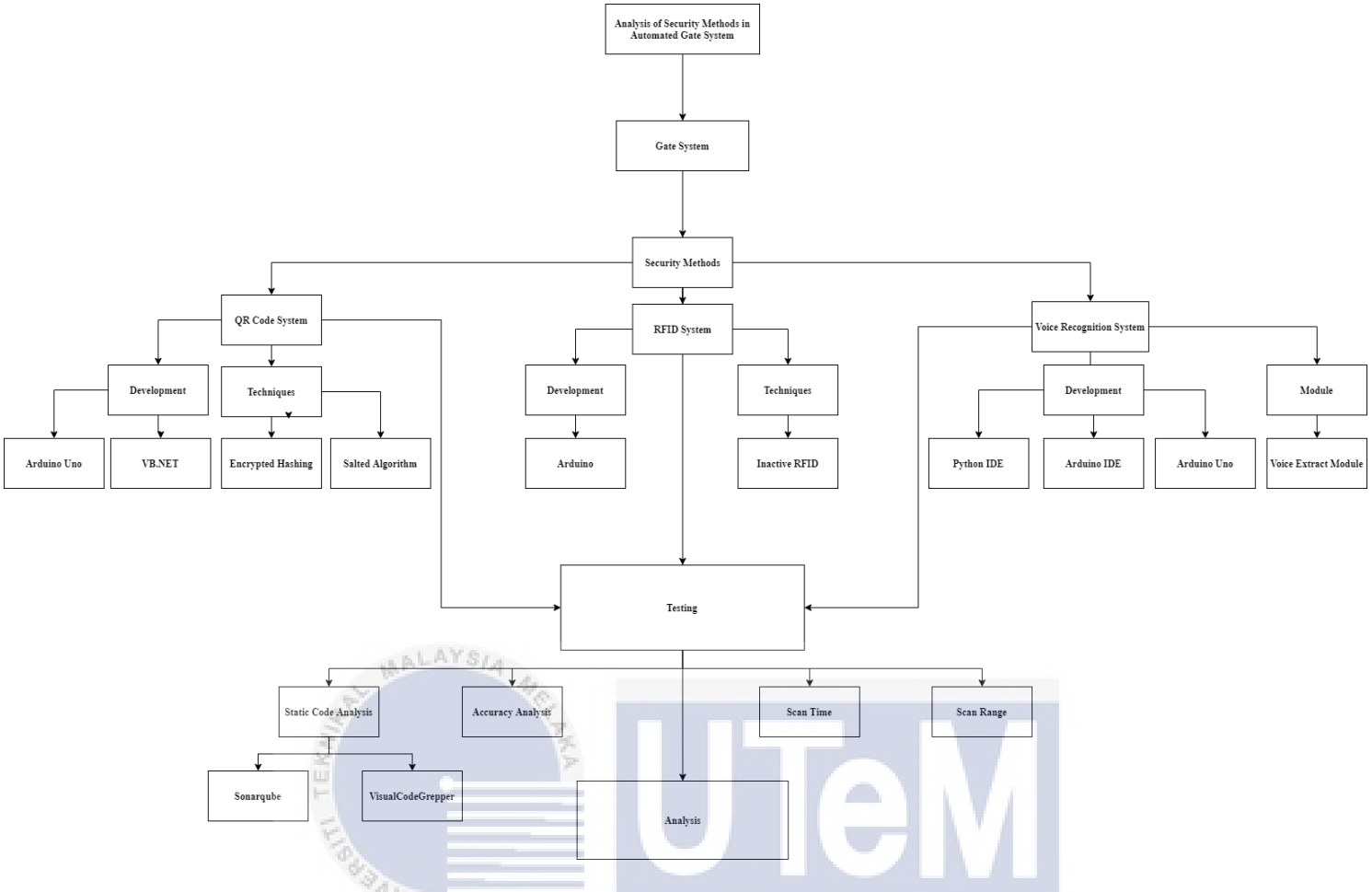


Figure 4.1 Flow of the analysis in a big picture

5.1. System Architecture

All platforms will be designed separately, using different security methods with a same scenario. These platforms are designed by referring to study and paper that have developed this system successfully using the security methods that have been chosen.

i. QR Code System

Referring to Erman, Lim, Nazrulazhar, Syarulnaziah and Zakiah (2018), by using VB.NET, an interface will be created in order to control the Arduino Uno Microcontroller. Before performing the rotation of the servo motor, Arduino Uno Microcontroller will receive the command via serial port. The servo motor will rotate 90 degree is the authorized scanning is detected as the gate open. Or else, it will not rotate and the regarding department will be receiving an email regarding the unauthorized scanning detected. Other than that, to detect the QR code, cameras will be used to act as a scanner. All data and information of the staffs or any person related will be save in the SQL database along with the in/out record and the created QR code. Figure 4.2 shows the system architecture for QR Code.

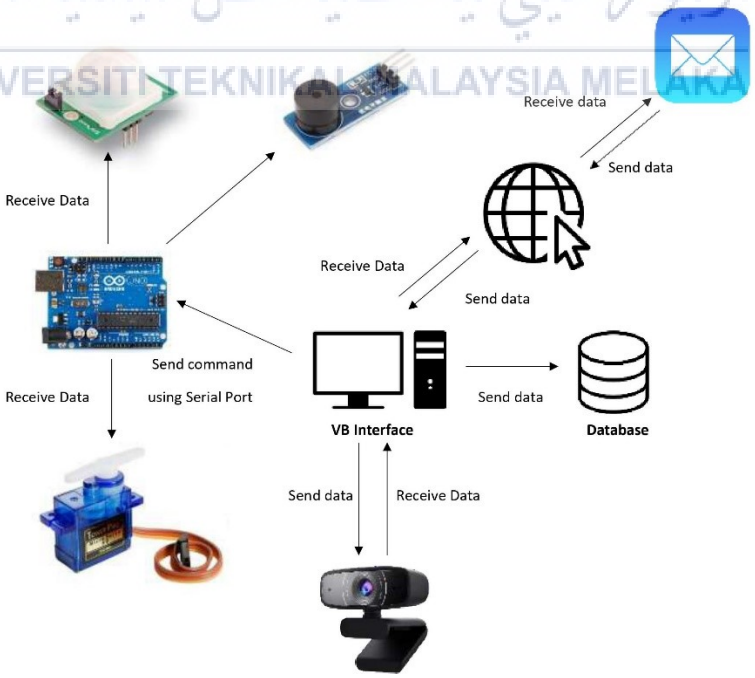


Figure 4.2 System Architecture for QR Code

ii. RFID System

Figure 4.3 shows the system architecture for the platform using RFID system. This RFID based platform is based on Asha. N, A. S. Syed Navaz, J. Jayashree and J. Vijayashree. Firstly, based on the figure above, this system consists of a unique security key access card that is saved in the database and only allow anyone enter the property is the unique key card is detected. If it did not match the unique key card that is stored in the database, there will be an alarm triggered. In the system software, there are two modules which are registration phase and recognition phase. The unique key card is registered in the system in the registration phase and the recognition phase is used when the key card is used at the gate.

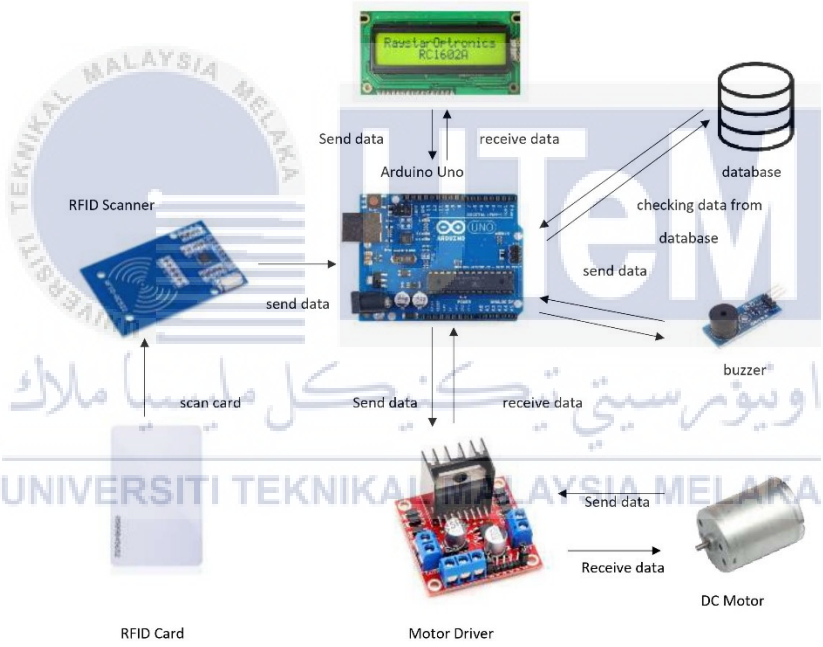


Figure 4.3 System Architecture for RFID system

iii. Voice Recognition System

For Voice Recognition System, there are two phases which are enrollment phase and authentication phase. In enrollment phase, admin will register the authorized users voice. The users will record their voices and after successfully recording their voices, the voices will be stored into the database. In authentication phase, the authorized users need to log in using their devices and need to speak random words that is being generated

automatically from the system. Then, their voices will be compared with the database. Figure 4.4 shows the system architecture for Voice Recognition System.

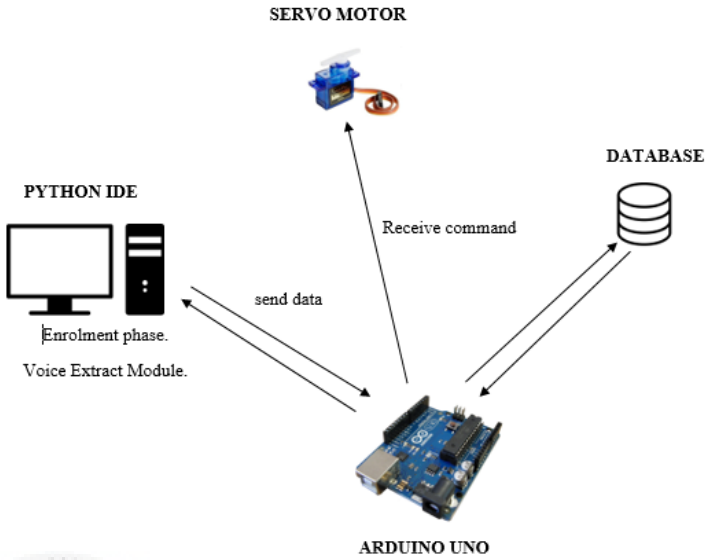


Figure 4.4 System Architecture for Voice Recognition

4.5 Requirement Analysis

4.5.1 Functional Requirement

Each platform will be divided into several blocks named microcontroller block, input/output block and development block. Figure 4.2 shows the details of the platform's block diagram for this project.

- **QR CODE**

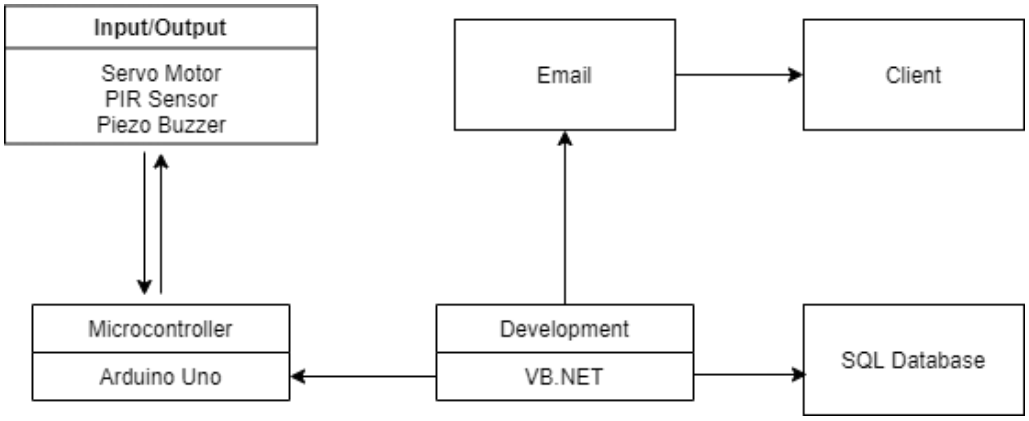


Figure 4.5 Block Diagram for QR Code

For QR Code, based on Figure 4.5, it shows the details of the block diagram as there are several blocks such as microcontroller block, input/output block and development block.

1. Input/Output

   The servo motor will serve as the gate, controlling whether the rotation is open or closed. The rotation of the servo motor will be controlled by an Arduino instruction. It will be wired directly to the Arduino microcontroller.

   If any unwanted scanning is discovered, the Piezo Buzzer functions as an alarm, alerting the security department. The alarm will be activated for around 5 seconds, after which an email will be sent from the VB.NET program.

   The motion of vehicles that have successfully activated the gate system is detected by a PIR motion sensor. The gate will automatically close whenever the vehicle is spotted by the PIR sensor.

2. Microcontroller

   The VB.NET instruction will be received by the Arduino Uno microcontroller, which will then transmit the order to the servo motor. By using IDE, all of the code for controlling the servo motor will be written in this microcontroller.

3. Development

The development block will house the principal function. The function includes monitoring the QR code scanner, recording entry/exit times, and creating staff QR codes, among other things. A USB cable will be used to connect the Arduino Uno microcontroller. The Arduino Uno microcontroller will be able to transmit and receive commands using VB.NET.

- **RFID**

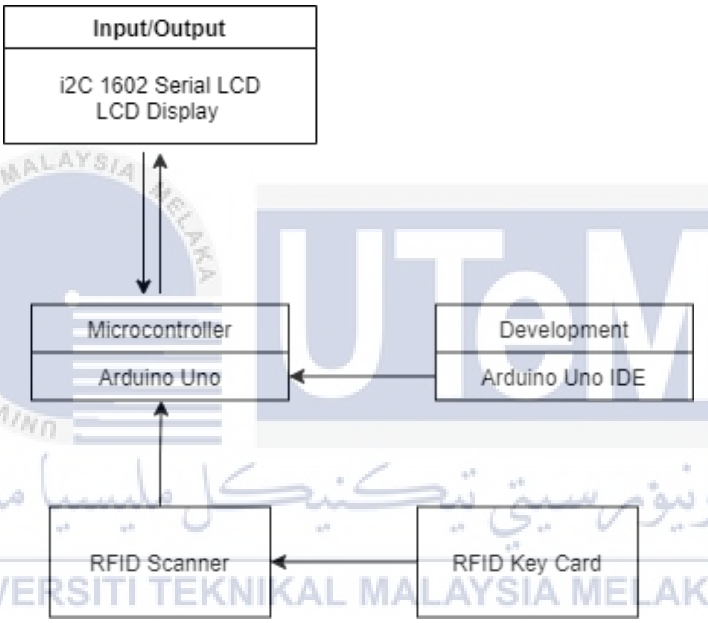


Figure 4.6 Block Diagram for RFID

For RFID, based on Figure 4.6, it shows the details of the block diagram as there are several blocks such as microcontroller block, input/output block and development block along with related hardware components such as RFID key card and RFID scanner.

1. Input/Output

Motor Driver will get message from Arduino Uno to control the movement of the motor. LCD display will generate a welcome or a warning message after key credibility has been checked.

2. Microcontroller

   Any message from RFID scanner will be received by the Arduino Uno microcontroller, which will then transmit the order to the servo motor. By using IDE, all of the code for controlling the servo motor will be written in this microcontroller.

3. Development

   All the programming will be made in Arduino IDE, linked with the Arduino Uno Microcontroller.

- **Voice Recognition System**

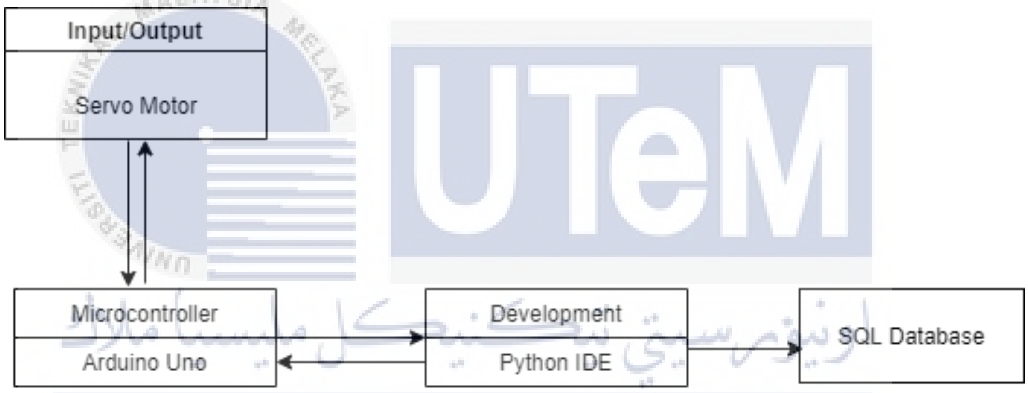


Figure 4.7 Block Diagram for Voice Recognition

For Voice Recognition System, based on Figure 4.7, it shows the details of the block diagram as there are several blocks such as microcontroller block, input/output block and development block along with related hardware component.

1. Input/Output

   The system will check the input of the user and if it is valid the gate will unlock. If not, valid the user needs to enter the username, password and record their voice again. Arduino IDE will send instruction to control servo motor.

2. Microcontroller

The Python instruction will be received by the Arduino Uno microcontroller, which will then transmit the order to the servo motor. Any instruction from Arduino IDE will be sent out to servo motor whether to open the gate or not.

3. Development

This platform will be using Python IDE and Arduino IDE and most of the data analysis are done in Python. There are a lot of phases done in Python, which are Mel Frequency Cepstral Coefficient Feature Extraction (MFCC Extraction), Gaussian Mixture Model (GMM), Voice Activity Detection and Long Time Spectral Deviation, Fuzzy Matching and Randomly Generating Words.

4.3.2 Hardware Requirement

1. Arduino Uno Microcontroller.

Arduino Uno is a microcontroller board based on the ATmega328P It has 14 digital input and output pins, with 6 of them serving as PWM output pins. This microcontroller's operating voltage is 5V. This board has 32KB of flash memory. To supply the current, it is generally linked to a PC by USB or a battery. This microcontroller will be used for QR Code, RFID system and Voice Recognition System.

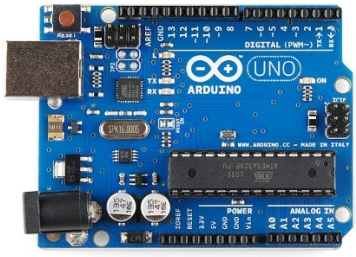


Figure 4.8 Arduino Uno Microcontroller

2. Tower Pro Micro Servo Motor SG90

Tower Pro Micro Servo Motor SG90 is a small and light motor with a high output power. Servo motors may spin 180 degrees (90 degrees in each direction) and function in the same way as standard motors, although they are considerably smaller. The Arduino Uno Microcontroller can control the servo motor. This servo motor will be used by QR Code and Voice Recognition System.

Figure 4.9 Tower Pro Micro Servo Motor SG90

3. Jumper Wire

Jumper wires are a simple way to link other devices such as servo motors, Arduinos, and Raspberry Pis. Jumper wires come in a variety of colors, lengths, and types. Male to male, male to female, and female to female are the three types of jumper wires. Every sort of jumper wire serves the same purpose, although they are designed for different devices. Jumper wire will be used by QR Code, RFID and Voice Recognition System.

Figure 4.10 Male to female jumper wire

4. PIR Motion Sensor

PIR Motion Sensor is a type of motion sensor. GND, Output, and DC voltage are the three pins connected to the sensor. The Female-to-Male jumper cable connects the PIR Motion Sensor to the Arduino Uno Microcontroller. This will be used by QR Code System.

Figure 4.11 PIR Motion Sensor

5. Piezo Buzzer 5V

The alarm system in this project is a Piezo Buzzer, which is an audio signaling device. GND, INPUT/OUTPUT, and VCC are the three pins on the board. The Piezo Buzzer is connected to the Arduino Uno Microcontroller using a Female-to-Male jumper wire. Piezo Buzzer will be used in QR Code.

Figure 4.12 Piezo Buzzer

6. RFID Scanner

A radio frequency identification (RFID) reader is a device that collects data from RFID tags, which are used to monitor particular things. Data is sent from the tag to the reader

through radio waves. RFID technology allows many products to be scanned rapidly and provides for instant identification of a certain product even when it is surrounded by other products. This will be used in RFID system.

Figure 4.13 RFID Scanner

7. LCD Display

A liquid crystal display (LCD) may be readily interfaced with an Arduino to create a user interface. LCDs are frequently used to show data in devices such as calculators, microwave ovens, and a variety of other electronic gadgets. There are 16 pins on the 16x2 LCD utilized in this experiment. This will be used in RFID System.

Figure 4.14 LCD Display

4.3.3 Software Requirement

1. Arduino IDE

Arduino IDE is an open source that make it easily to update the source code to the board. It supports on Windows, Linux and Mac OS. The model and the port number have to be selected in order to make it work correctly during uploading the source code. The figure 4.23 shows the interface of IDE.

RFID System, QR Code and Voice Recognition will be using Arduino IDE to be implemented in the platform.

Figure 4.15 interface of IDE

2. VB.NET

Visual Basic. NET (VB.NET) is an object-oriented programming language that implemented on the .NET Framework. It is easier and faster way to create an application and support drag and drop for the interface.

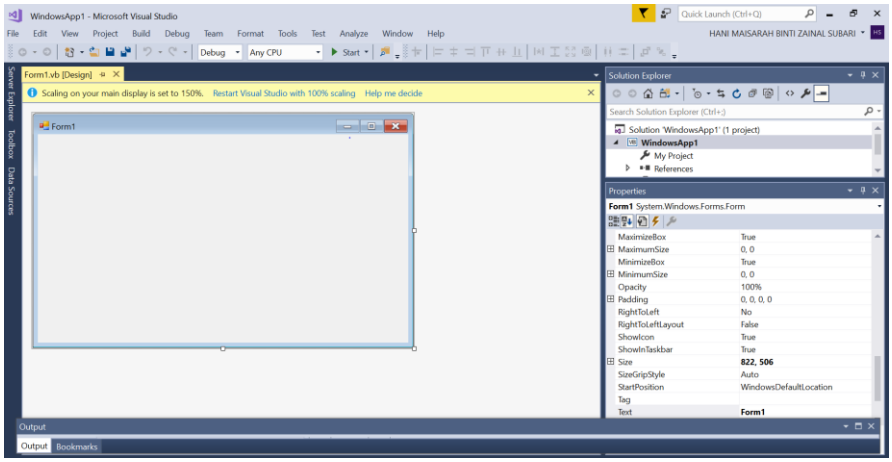


Figure 4.16 interface of VB.NET

3. Python

Python IDE is an open-source programming software. Additionally, an IDE stands for built in development environments for python. In this project, Python 3 version 3.6.8 will be used to run the system. Voice Recognition will be using Python to be implemented in the platform.

Figure 4.17 Python logo

4. SonarQube

SonarQube (previously Sonar) is an open-source platform built by SonarSource for continuous code quality inspection using static analysis to discover defects, code smells, and security vulnerabilities in code written in more than 20 programming languages. Duplicated code, coding standards, unit tests, code coverage, code

complexity, comments, bugs, and security vulnerabilities are all covered by SonarQube reports.

Figure 4.18 Sonarqube

5. VisualCodeGrepper

VCG is an automatic code security review tool for C++, C#, VB, PHP, Java, and PL/SQL that identifies bad/insecure code to dramatically speed up the code review process. It comes with a couple of features that should make it helpful. It also contains a config file for each language that allows you to add any problematic functions (or other text) that you wish to look for, in addition to doing some more complicated tests. It looks for terms in comments that could signal faulty code, and it displays statistics and a pie chart (for the whole codebase and specific files) that show the proportions of code, whitespace, comments, style comments, and poor code.

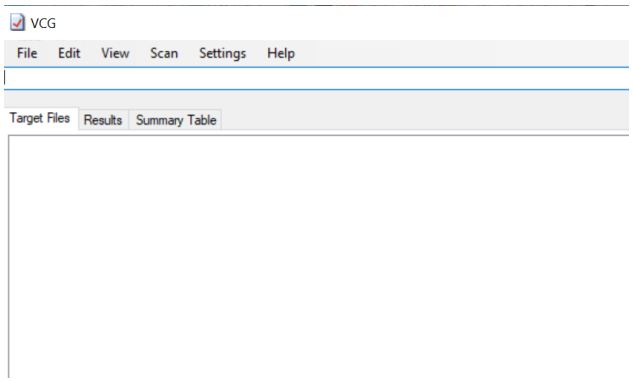


Figure 4.19 interface of VCG

4.4 Logical and Physical Design

- **QR Code**

For QR Code, when the QR scanner is activated, it will analyze whether the QR Code is in the database or not. If it matches, the gate will be opened or closed. If it does not match, alarm will be triggered and the unauthorized access will be captured using camera to send email to the authorized department. Figure 4.20 shows the flowchart of the platform using QR Code system.

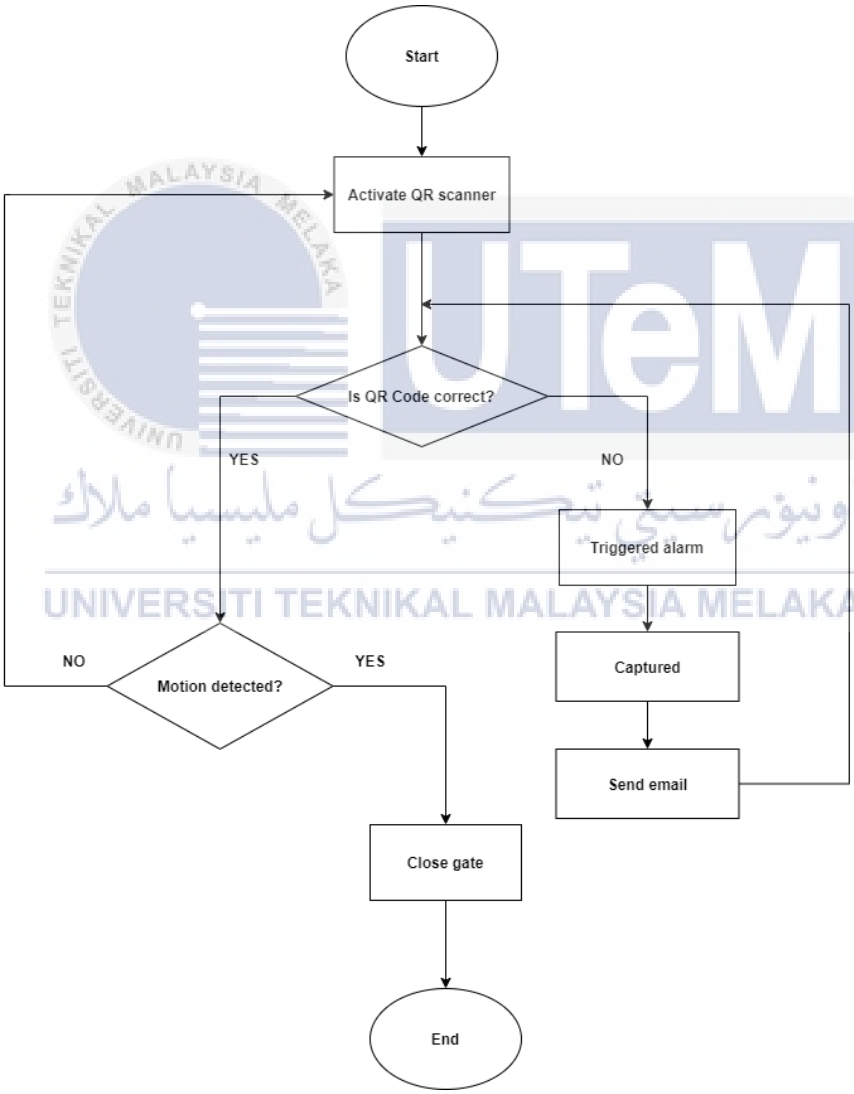


Figure 4.20 Flowchart of platform using QR Code.

- **RFID**

For RFID, after RFID scanner is activated and the key card is scanned, the credibility will be checked and if it matches with the information in the database, a welcome message will be displayed and the gate will be unlocked and open. It will close after 10 seconds. If the card does not match with the information in the database, a warning message will be displayed, alarm will be triggered and the gate will remain closed. Figure 4.21 shows the flowchart of the platform using RFID system.

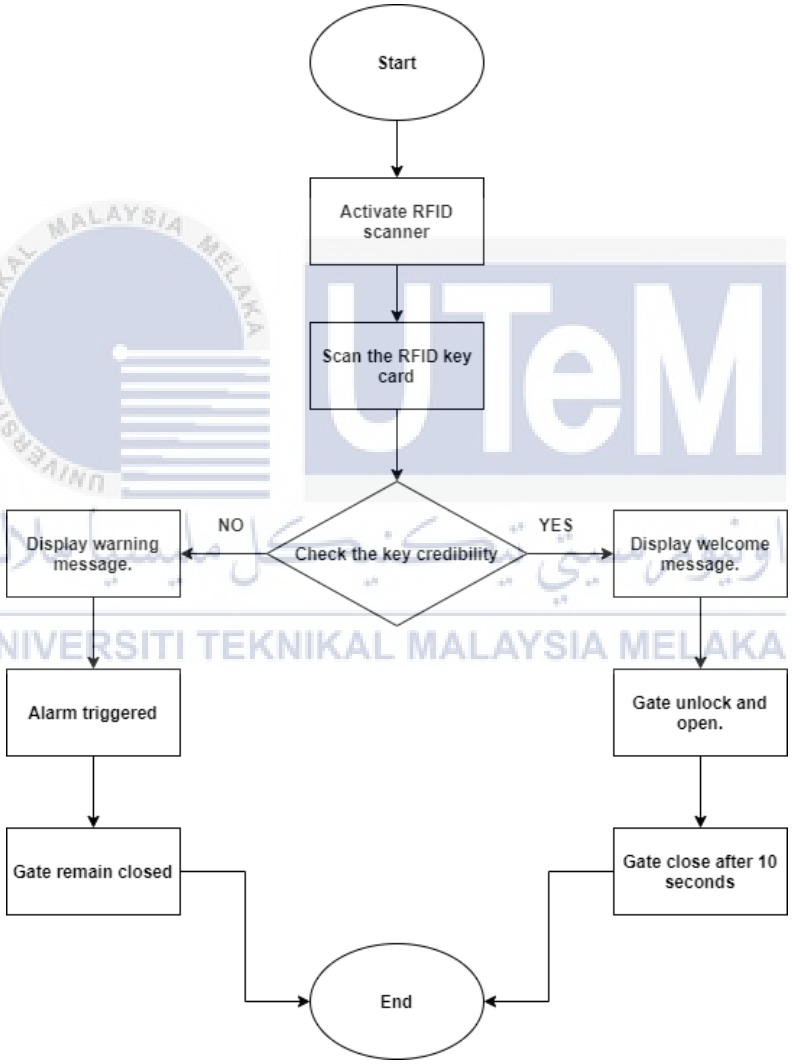


Figure 4.21 Flowchart of platform using RFID

- **Voice Recognition System**

For Voice Recognition, before using the system, user need to register and record their voices by speaking random words that is being generated automatically. The audio file then will be saved in the database. For login, user will need to speak random words that are being generated and if it matches the audio file in the database, gate will unlock. If it does not, it will not recognize the user. Figure 4.22 shows the flowchart of the platform using Voice Recognition system.

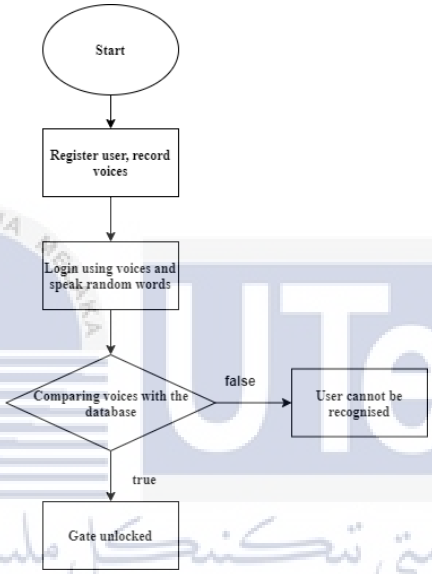


Figure 4.22 Flowchart of platform using Voice Recognition

4.5 Conclusion

Design is one of the important parts to implement a project. All software and hardware requirements need to be identified and studied before carrying out a project. This chapter is pre-preparation stage for the implementation and it also include the flow of the overall system so that to have a better understanding before implementing it. Chapter 5: Implementation will discuss how the project to be implement and the output and goal expected for this project.

CHAPTER 5: IMPLEMENTATION

5.1 Introduction

This chapter will focus on how to implement the platforms using QR Code, RFID system and Voice Recognition System in both software and hardware development. The testing process will also be carried out to figure out which platform is the most secure. The system will be tested using the right technique and parameter by following the proper procedure to identify the system's performance. After the implementation of all platforms are done, the methods will be analysed and compared to figure out which platform is the most secure.

5.2 Environment Setup

The development environment setup for the three platforms will involve hardware and software requirements. All setups for the platforms will be stated step by step and will be clearly shown. The hardware and software requirements are stated in the Chapter 4 and will be explain further for the connection in the below section.

5.2.1. Hardware Development Setup

In this project, the hardware used are stated in Chapter 4. There are three platforms in this project and all platforms are using Arduino Uno as a microcontroller. Figure 5.1 shows the Arduino pins.

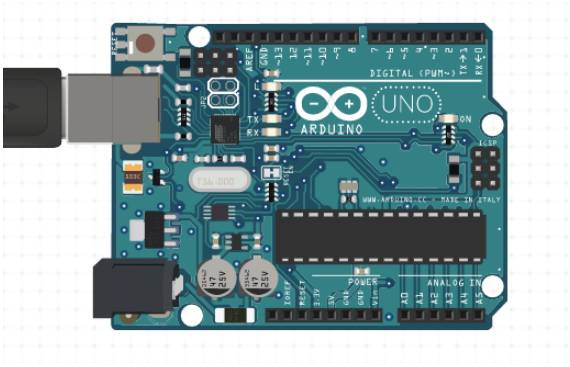


Figure 5.1 Arduino Pins

- QR Code System

For QR Code System, there are two servo motor, piezo buzzer, and PIR motion sensor that will be attached to the Arduino Uno microcontroller. Arduino Uno microcontroller will receive command from the VB.NET to control the hardware. Table 5.1 shows the details of each pins number.

Table 5.1 Details of each pins number for QR Code

Hardware	Wire	Pins
Led Light (Red)	Power	5V
	Signal	6
Led Light (Green)	Power	5V
	Signal	5
PIR Motion Sensor	VCC	5V
	OUT	3
	GND	GND
Piezo Buzzer 5V	VCC	5V
	I/O	2
	GND	GND
Servo Motor 1	GND	GND
	Power	5V

	Signal	4
Servo Motor 2	GND	GND
	Power	5V
	Signal	7

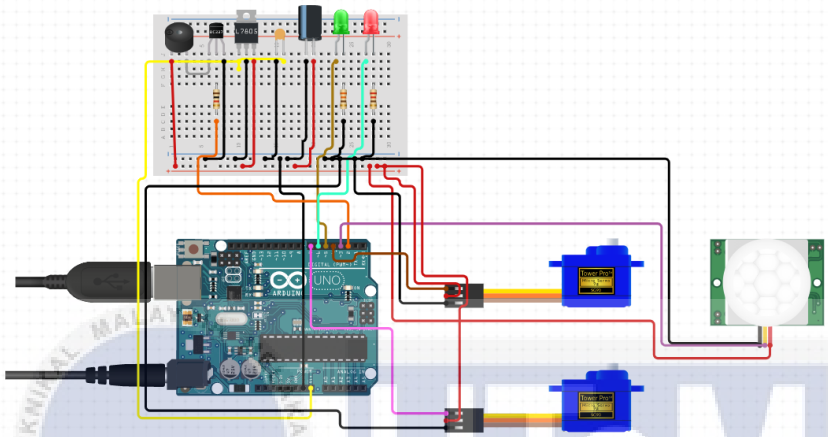


Figure 5.2 Details of each pins number for QR Code

Figure 5.2 shows the hardware prototype and details of the hardware that are connected to the Arduino. Arduino is connected to the PC via USB port. All connection is followed based on Table 5.1.

Figure 5.3 Platform developed using QR Code

Figures 5.3 shows the platform that is developed from the details above. For this platform, ideas are referred from a paper titled Implementation of Intelligent Automated Gate (Erman Hamid, Lim Chong Gee, Nazrulazhar, Syarulnaziah Anawar, & Zakiah Ayob, 2018).

- RFID System

For RFID System, there are servo motor, I2C Module and RFID Scanner that will be attached to the Arduino Uno microcontroller. Arduino Uno microcontroller will receive command from the Arduino IDE to control the hardware. Table 5.2 shows the details of each pin numbers.

Table 5.2 Details of each pins number for RFID System

Hardware	Wire	Pins
I2C Module	GND	GND
	VCC	5V
	SDA	A4
	SCL	A4
RFID Scanner	3.3V	3.3V
	RST	9
	GND	GND
	MISO	12
	MOSI	11
	SCK	13
	SDA	10
Servo Motor	GND	GND
	Power	5V
	Signal	3

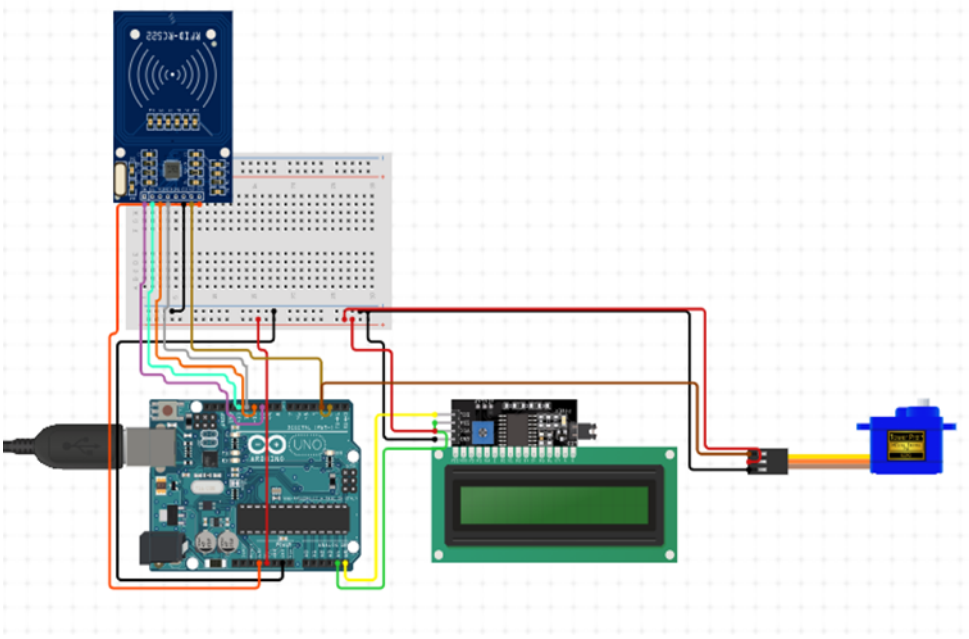


Figure 5.4 Hardware Details for RFID System

Figure 5.4 shows the hardware prototype and details of the hardware that are connected to the Arduino. Arduino is connected to the PC via USB port. All connection is followed based on Table 5.2.

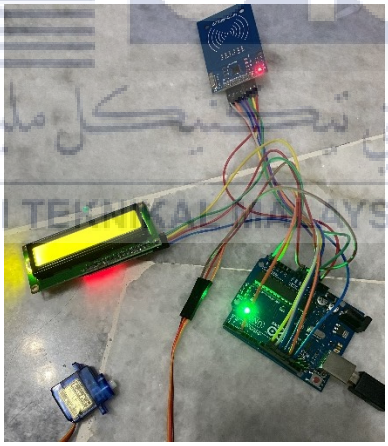


Figure 5.5 Platform developed using RFID system

Figures 5.5 shows the platform that is developed from the details above.

- Voice Recognition System

For Voice Recognition System, there are servo motor and LED that will be attached to the Arduino Uno microcontroller. Arduino Uno microcontroller will receive command from the

Arduino IDE and Python to control the hardware. Table 5.3 shows the details of each pins number.

Table 5.3 Details of each pins number for RFID System

Hardware	Wire	Pins
Led Light (Green)	Power	5V
	Signal	5
Led Light (Red)	Power	5V
	Signal	6
Servo Motor	GND	GND
	Power	5V
	Signal	2

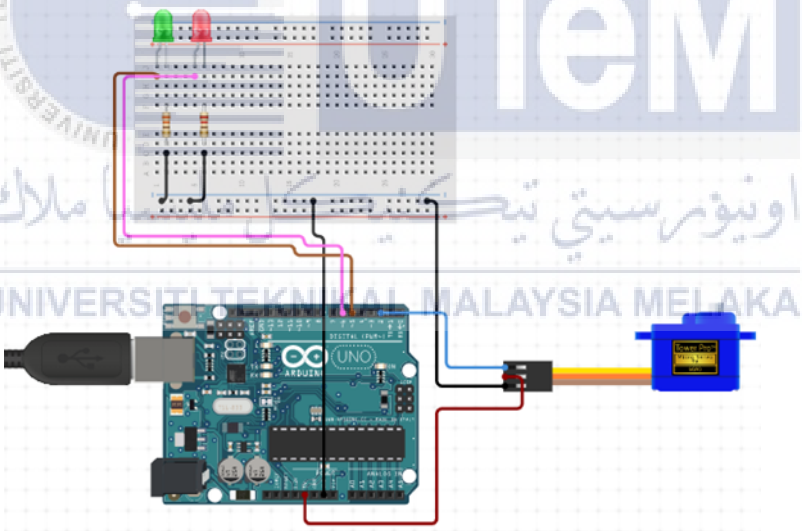


Figure 5.6 Hardware Details for Voice Recognition System

Figure 5.6 shows the hardware prototype and details of the hardware that are connected to the Arduino. Arduino is connected to the PC via USB port. All connection is followed based on Table 5.3.

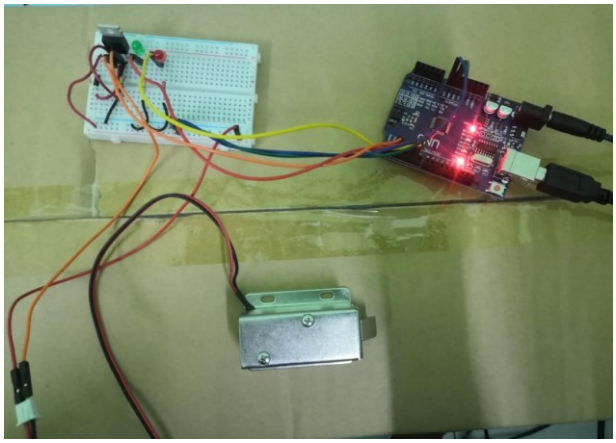


Figure 5.7 The platform developed for Voice Recognition System

Figures 5.7 shows the platform that is developed from the details above.

5.2.2. Software Development Setup

In this part, the deployment of each platform will be explained one by one.

- QR Code

For QR Code, this system will be using Arduino IDE, Microsoft VB.net and Microsoft SQL. Figure 5.8 shows the system deployment for the platform using QR Code system.

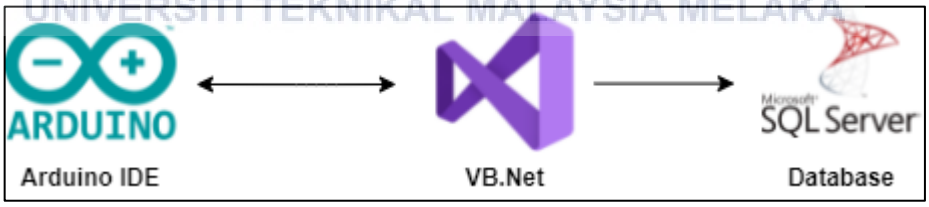


Figure 5.8 System Deployment for QR Code

The Arduino Uno microcontroller must first be programmed using Arduino IDE before it can interpret any command from VB.net. To control the rotation of the servo motor, PIR motion sensor and more, VB.net will send commands to Arduino Uno via serial port. Several functions like registration, generate QR Code, update or delete information will be created using C# as the language on VB.net. For the system to work perfectly, all functions should make sure to be developed and coded correctly. Information retrieved from the system will be saved into a local

database, which is Microsoft SQL as backup to make sure the information needed will be easily retrieved and making the process more smoothly.

Figures below will explain about the coding snippet of the platform using QR Code system.

Coding Snippet using Arduino IDE:

```
#include <Servo.h>
#define ALARM 9
Servo myservo;  //creates servo object
Servo myservo2;     //a max of 8 servo obj can be created

//time for sensor to calibrate
int calibrationTime = 30;

//time when sensor outputs a low impulse
long unsigned int lowIn;

//amount of ms sensor has to be low
//before we assume all motion has stopped
long unsigned int pause = 5000;
boolean lockLow = true;
boolean takeLowTime;
int pirPin = 12;     //digital pin connected to the PIR's output
const int buzzer = 9;
float sinVal;
int toneVal;
int led=6;
int ledState;
```

Figure 5.9 Arduino coding in QR Code system

Figure 5.9 shows the coding in Arduino IDE that are coded for Arduino Uno to control the servo motor and perform a rotation.

Coding Snippet:

```
Public Shared Sub AddStaff(ByVal name As String, ByVal ic As String, ByVal position As String, ByVal phone As String, ByVal mail As String, ByVal qr As String)
    Using sqlCon = New SqlConnection(CONNECTION_STRING)

        sqlCon.Open()

        Dim sqlText = "INSERT INTO Staff(staffName,staffIC,staffPosition,staffPhone,staffMail,staffQR) VALUES(@name,@ic,@position,@staffPhone,@staffMail,@qr)"
        Dim sqlCmd = New SqlCommand(sqlText, sqlCon)
        sqlCmd.Parameters.AddWithValue("@name", name)
        sqlCmd.Parameters.AddWithValue("@ic", ic)
        sqlCmd.Parameters.AddWithValue("@position", position)
        sqlCmd.Parameters.AddWithValue("@staffPhone", phone)
        sqlCmd.Parameters.AddWithValue("@staffMail", mail)
        sqlCmd.Parameters.AddWithValue("@qr", qr)

        sqlCmd.ExecuteNonQuery()
        sqlCon.Close()


    End Using
End Sub
```

Figure 5.10 Coding VB.NET for staff registration system

Figure 5.10 shows the coding for staff registration where staff information will be saved into SQL database. For this section, a pre-checking action will be taken where the format of the phone number can only be numeric, alphabet is allowed for names and new email can be registered. If all format is correct, only then the information will be saved into the database.

Coding Snippet:

```
Private Sub ButtonVIDEO2_Click_1(sender As Object, e As EventArgs) Handles ButtonVIDEO2.Click
    If ButtonVIDEO2.BackColor = Color.Gainsboro Then
        SaveFileDialog2.DefaultExt = ".avi"
        If SaveFileDialog2.ShowDialog() = System.Windows.Forms.DialogResult.OK Then
            Dim ANCHO2 As Integer = Camare2.VideoResolution.FrameSize.Width
            Dim ALTO2 As Integer = Camare2.VideoResolution.FrameSize.Height

            memoryWritter2.Open(SaveFileDialog2.FileName, ANCHO2, ALTO2, NumericUpDownFPS2.Value, VideoCodec.Default, NumericUpDownBRT2.Value * 1000)
            memoryWritter2.WriteVideoFrame(BMP2)
            ButtonVIDEO2.BackColor = Color.Red
            ButtonVIDEO2.Text = "Recording"
        End If
    Else
        ButtonVIDEO2.BackColor = Color.Gainsboro
        ButtonVIDEO2.Text = "Video"
        memoryWritter2.Close()
    End If
End Sub
```

Figure 5.11 Coding VB.NET for video recording

Figure 5.11 shows the coding for video recording. This function is important and needed in a security system as it can be evidence if any unauthorized entries happened. The video recorded will be saved in AVI format and the height and width of the video must be stated.

- RFID System

For RFID, this system will be using Arduino IDE that will be uploaded in the Arduino Uno microcontroller. Figure 5.12 shows the system deployment for the platform using RFID system.

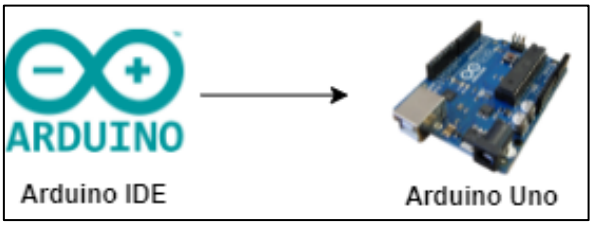


Figure 5.12 System Deployment for RFID system

The Arduino Uno microcontroller must first be programmed using Arduino IDE and uploaded into Arduino Uno microcontroller. To control the rotation of the servo motor, LCD display and RFID scanner, it must be coded in Arduino IDE. For the system to work perfectly, all functions should make sure to be developed and coded correctly.

Figures below will explain about the coding snippet of the platform using RFID system. The coding shows how Arduino Uno can scan the RFID card using the scanner in the loop function. The unique ID is printed on the serial monitor and LCD.

Coding Snippet:

```
void setup() {
  Serial.begin(9600);
  servo.write(70);
  lcd.init();
  lcd.backlight();
  servo.attach(3);
  SPI.begin();
  rfid.PCD_Init();
}
```

Figure 5.13 Coding for setup function

Figure 5.13 shows the coding for a setup function. In the setup function, the modules for the serial monitor, LCD display, SPI bus have started.

Coding Snippet:

```
void loop() {
  if ( ! mfrc522.PICC_IsNewCardPresent()) {
    return 0;
  }
  if ( ! mfrc522.PICC_ReadCardSerial()) {
    return 0;
  }

  lcd.clear();
  lcd.setCursor(0, 0);
  lcd.print("Scanned UID");
  a = 0;
  Serial.println(F("Scanned PICC's UID:"));
  for ( uint8_t i = 0; i < 4; i++) {  //
    readCard[i] = mfrc522.uid.uidByte[i];
    Serial.print(readCard[i], HEX);
    Serial.print(" ");
    lcd.setCursor(a, 1);
    lcd.print(readCard[i], HEX);
    lcd.print(" ");
    delay(500);
    a += 3;
  }
```

Figure 5.14 Coding for tag scanning

Figure 5.14 shows the coding in a loop function, which is the RFID tag is scanned and the unique identity of each card is printed on the LCD screen and serial monitor.

Coding Snippet:

```
if (ID.substring(1) == UID && lock == 0 ) {
  servo.write(70);
  lcd.clear();
  lcd.setCursor(0, 0);
  lcd.print("Gate is locked and secured.");
  delay(1500);
  lcd.clear();
  lock = 1;
} else if (ID.substring(1) == UID && lock == 1 ) {
  servo.write(160);
  lcd.clear();
  lcd.setCursor(0, 0);
  lcd.print("Gate is opening..");
  delay(1500);
  lcd.clear();
  lock = 0;
} else {
  lcd.clear();
  lcd.setCursor(0, 0);
  lcd.print("Wrong card!");
  delay(1500);
  lcd.clear();
}
```

Figure 5.15 Coding for servo motor

Coding in figure 5.15 shows that it is using IF function where it is testing the unique identification for the RFID card. It is written in the code that the servo motor rotates 70 degrees and 160 degrees. If the unique identification in the scanned RFID card is correct, the gate will be opening and a "Gate is opening.." will be displayed. But if the unique identification in the scanned RFID card is incorrect, a "Wrong card!" message will be displayed and the gate will remain unlocked.

- Voice Recognition System

For the platform using Voice Recognition System, this system will be using Python, Microsoft SQL Server and Arduino IDE that will be uploaded in the Arduino Uno microcontroller. Figure 5.16 shows the system deployment for the platform using QR Code system.

Figure 5.16 System Deployment for Voice Recognition System

To make the system work, codes are written in the python and information will be sent to Arduino Uno to control the rotation of the servo motor.

Figures below will explain about the coding snippet of the platform using Voice Recognition System.

Coding Snippet:

```
@app.route('/vad', methods=['GET', 'POST'])
def vad():
    if request.method == 'POST':
        global random_words

        f = open('./static/audio/background_noise.wav', 'wb')
        f.write(request.data)
        f.close()

        background_noise = speech_recognition.AudioFile(
            './static/audio/background_noise.wav')
        with background_noise as source:
            speech_recognition.Recognizer().adjust_for_ambient_noise(source, duration=1)

        print("Voice activity detection complete ...")

        random_words = RandomWords().random_words(count=1)
        print(random_words)

        return "  ".join(random_words)

    else:
        background_noise = speech_recognition.AudioFile(
            './static/audio/background_noise.wav')
        with background_noise as source:
            speech_recognition.Recognizer().adjust_for_ambient_noise(source, duration=1)

        print("Voice activity detection complete ...")

        random_words = RandomWords().random_words(count=1)
        print(random_words)

        return "  ".join(random_words)
```

Figure 5.17 Coding for voice detecting

Figure 5.17 shows the coding about voice detection process. Users need to speak random words for the recognition process. The voice then will be saved in an audio file using .wav format. Random Words is a python package to generate English words.

Coding Snippet:

```
@app.route('/voice', methods=['GET', 'POST'])
def voice():
    global user_directory
    global filename_wav

    print("[ DEBUG ] : User directory at voice : ", user_directory)

    if request.method == 'POST':
        #    global random_string
        global random_words
        global username

        filename_wav = user_directory + "~".join(random_words) + '.wav'
        f = open(filename_wav, 'wb')
        f.write(request.data)
        f.close()

        with open(filename_wav, 'rb') as audio_file:
            recognised_words = speech_to_text.recognize(audio_file, content_type='audio/wav').get_result()

        recognised_words = str(recognised_words['results'][0]['alternatives'][0]['transcript'])


        print("IBM Speech to Text thinks you said : " + recognised_words)
        print("IBM Fuzzy partial score : " + str(fuzz.partial_ratio(random_words, recognised_words)))
        print("IBM Fuzzy score : " + str(fuzz.ratio(random_words, recognised_words)))
```

Figure 5.18 Coding for word recognising

Then, Figure 5.18 shows the coding after voice has been recorded and save. This coding is to recognise any words the user is saying. Fuzzy Wuzzy is to calculate the differences between sequences in a package using Levenshtein Distance.

Coding Snippet:

```
# Load the Gaussian user Models
models = [pickle.load(open(user, 'rb')) for user in gmm_models]

user_list = [user.split("/")[-1].split(".gmm")[0]
             for user in gmm_models]

log_likelihood = numpy.zeros(len(models))

for i in range(len(models)):
    gmm = models[i]  # checking with each model one by one
    scores = numpy.array(gmm.score(extracted_features))
    log_likelihood[i] = scores.sum()

print("Log liklihood : " + str(log_likelihood))

identified_user = numpy.argmax(log_likelihood)

print("[ * ] Identified User : " + str(identified_user) +
      " - " + user_list[identified_user])

auth_message = ""

if user_list[identified_user] == username:
    print("[ * ] You have been authenticated!")
    auth_message = "success"
if user_list[identified_user]!= username:
    print("[ * ] Sorry you have not been authenticated")
    auth_message = "fail"
```

Figure 5.19 Coding for user identification

Then, in Figure 5.19, after the words have been recognised, the coding above is using Gaussian Mixture Models (gmm). It is a clustering algorithm that clusters the different features of the voice to create the user's voice print. Then the voice print is then stored in a voice print database. Coding above shows that the user has been identified using the audio file stored earlier.

5.3 Conclusion

In conclusion, the implementation chapter is about implementing platforms that are going to be used in Chapter 6: Testing & Analysis. This chapter need to be done beforehand to complete the whole analysis and it includes the process of hardware installation and software setup and development. The implementations of the platforms provide a clear picture and idea to do the analysis and achieve the objective of this project.

CHAPTER 6: TESTING & ANALYSIS

6.1 Test Results and Analysis

For the test results and analysis, there are four parameters that are going to be used which are:

i. Accuracy Analysis
ii. Scan Time
iii. Scan Range
iv. Static Code Analysis.

Each platform will be going through test and analysis based on the parameters.

- QR Code

1. Accuracy Analysis

For this system, the QR Code detection was tested 100 times to calculate accuracy of the system. A QR Code sample is used to do the accuracy analysis. Table 6.1 shows the result of this analysis:

Table 6.1 Accuracy Analysis QR Code

No. of detection	Correct detection	Error detection	Success %
100	99	1	99%

QR Code system achieves 99% accuracy, where there is only one error detected out of 100 detections.

2. Scan Time

For this section, the time taken for the camera to finish scanning the QR Code is collected. To get a more precise result, it took 20 sample tests to get an accurate average time taken for the camera to finish scanning.

Table 6.2 Scan Time for QR Code

Test	Time taken (sec)
1	6.10
2	5.31
3	4.30
4	6.00
5	4.09
6	5.23
7	3.89
8	6.05
9	6.07
10	4.43
11	5.70
12	3.99
13	6.34
14	4.38
15	4.46
16	6.40
17	4.21
18	5.28
19	4.29
20	6.26
Average: (102.78) / 20 = 5.14 second	

Table 6.2 shows the result for the time taken for the scanner to finish scanning and open/close the gate. The formula used to get the average time taken is:

(total of all time taken) / (number of tests)

The average time taken for RFID scanner to scan the tag is **(102.78) / 20 = 5.14 second.**

3. Scan Range

The scan range for is short as the camera need to capture every symbol to decode them faster. To scan QR Code, the distance cannot be too far as it is harder for the camera to detect the QR Code. But it is actually depending on the size of the QR code printed. If the size is bigger, then the distance can be far. For this system, the scan range cannot be far than 10 cm as the QR code printed is quite small.

Table 6.3 Scan Range for QR Code

Scan distance (cm)	Result
2.0	Too close.
3.0	Too close.
4.0	Scanned, but took too long.
5.0	Successfully scanned.
6.0	Successfully scanned.
7.0	Successfully scanned.
8.0	Successfully scanned.
9.0	Successfully scanned.
10.0	Successfully scanned.
11.0	Too far.
Range: 4.0 – 10.0 cm	

4. Static Code Analysis

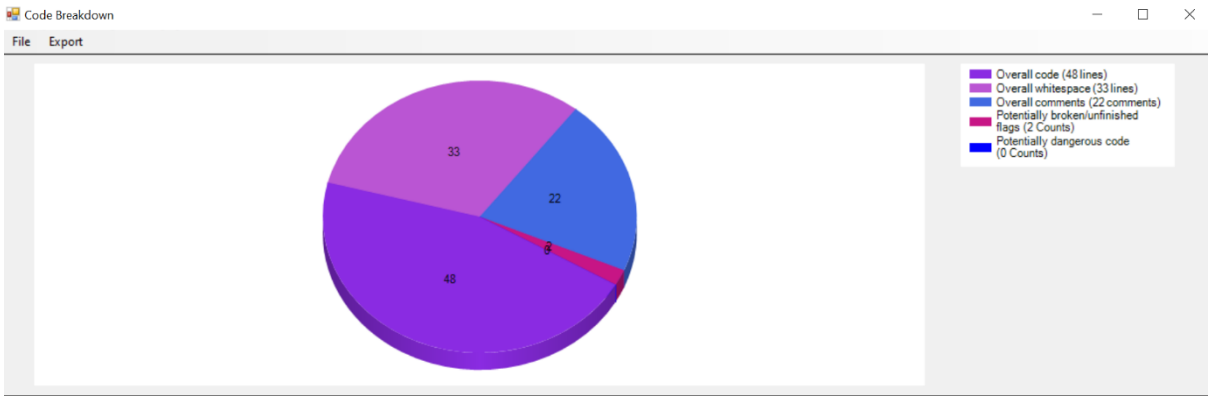


Figure 6.1 Scanning code for Arduino

Figure 6.1 is showing the pie chart for the code analysis that is done using VisualCodeGreeper (VCG) for Arduino IDE that is read as c++ language. After being analysed, there is no potentially dangerous code recorded.

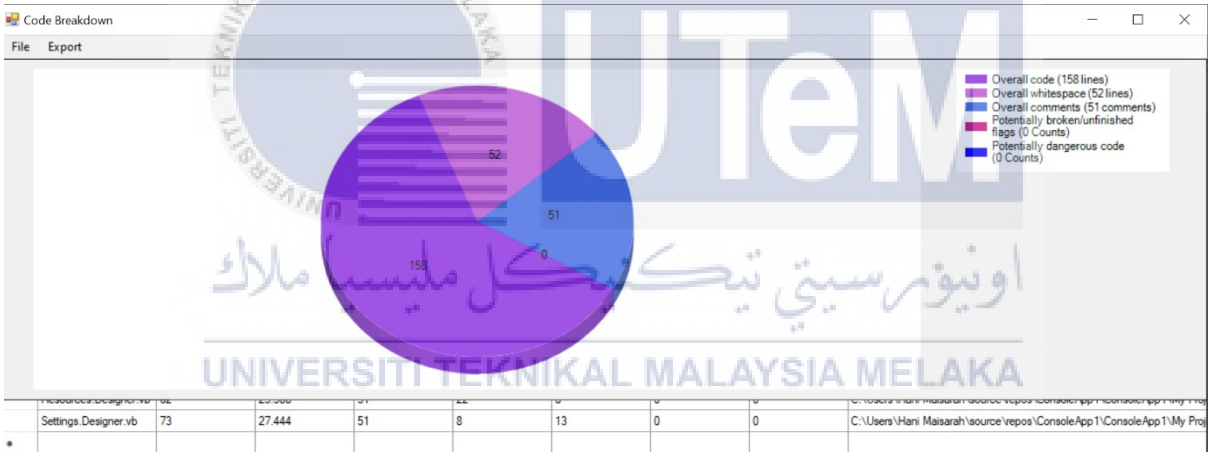


Figure 6.2 Scanning code for VB.NET

Next, Figure 6.2 is showing the pie chart for the code analysis that is also done using VGC for VB.NET coding. There is also no potentially dangerous code recorded.

- RFID System

1. **Accuracy Analysis**

For this system, there are two RFID tag used to analyse the accuracy. One RFID tag is registered, while the other one is not registered. The table below shows the result of this analysis:

Table 6.4 Accuracy Analysis RFID

True Positive	True Negative
✓	✓
✓	✓
✓	✓
✓	✓
✓	✓
✓	✓
✓	✓
✓	✗
✓	✓
✓	✓
✓	✓
✓	✓
✓	✓
✓	✓
✓	✓
✓	✓
✓	✓
✓	✓
✓	✓
✓	✓
✓	✓
✓	✓
✗	✓
✓	✓
✓	✗
✓	✓
✓	✓

✓	✓
✓	✓
✓	✓
✓	✓
✓	✓
✗	✓
✓	✓
✓	✓
✓	✓
✓	✓
✓	✓
✓	✓
✓	✓

Table 6.4 shows the result of the analysis. For the true positive is the outcome when the RFID scanner successfully identify the registered RFID tag while the true negative is the outcome for not registered RFID tag unsuccessful to identify the tag using other the scanner. Then, the accuracy of the RFID system will be calculate using this formula:

((TP + TN) / Total) X 100

For this result, the accuracy of the voice RFID System is **((38 + 38) / 80) X 100 = 95%.** The result is affected by surrounding and frequency of the RFID tags.

2. **Scan Time**

   For this section, the time taken for the RFID scanner to finish scanning the tag is collected. To get a more precise result, it took 20 sample tests to get an accurate average time taken for the scanner to finish scanning.

Table 6.5 Scan Time for RFID

Test	Time taken (sec)
1	1.56
2	1.38
3	1.40

4	1.55
5	1.46
6	1.71
7	1.86
8	1.29
9	1.79
10	1.74
11	1.35
12	1.44
13	1.46
14	1.30
15	1.65
16	1.23
17	1.32
18	1.30
19	1.23
20	1.43
Average: (29.45)s / 20 = 1.47 second	

Table 6.5 shows the result for the time taken for the scanner to finish scanning and open/close the gate. The formula used to get the average time taken is:

(total of all time taken) / (number of tests)

The average time taken for RFID scanner to scan the tag is **(29.45) / 20 = 1.47 second.**

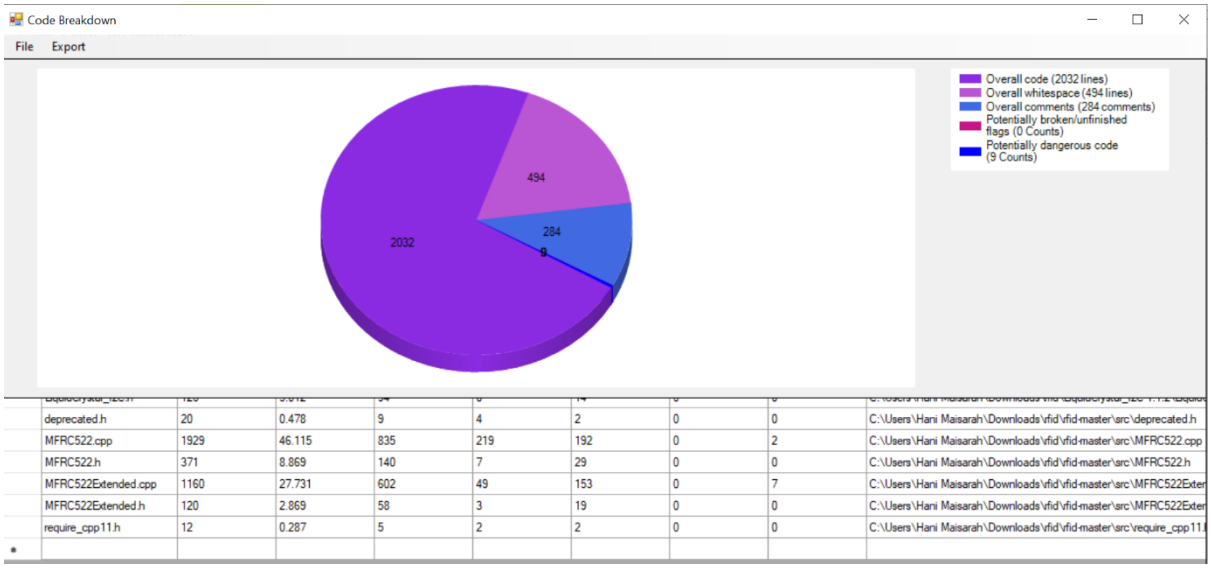
3. Scan Range

For the scan range in RFID System, the range is big as the read range for RFID is long. However, it depends on the RFID module as the frequency is different. For this platform, the module used is a cheap RC522 module so the frequency is not very high. Hence, the range is limited too. The frequency for this module is 13.56 MHz. The scan range for RFID is between 5 cm to 30 cm.

Table 6.6 Scan Range for RFID

Scan distance (cm)	Result
2.0	Too close.
4.0	Scanned, but not clear.
5.0	Successfully scanned.
10.0	Successfully scanned.
15.0	Successfully scanned.
20.0	Successfully scanned.
25.0	Successfully scanned.
30.0	Successfully scanned.
35.0	Too far, RFID tag are not scanned properly.
40.0	Too far, RFID tag are not scanned properly.
Range: 5.0 – 30.0 cm	

4. Static Analysis



deprecated.h	20	0.478	9	4	2	0	0	C:\Users\Hani Maisarah\Downloads\rfid\rfid-master\src\deprecated.h
MFRC522.cpp	1929	46.115	835	219	192	0	2	C:\Users\Hani Maisarah\Downloads\rfid\rfid-master\src\MFRC522.cpp
MFRC522.h	371	8.869	140	7	29	0	0	C:\Users\Hani Maisarah\Downloads\rfid\rfid-master\src\MFRC522.h
MFRC522Extended.cpp	1160	27.731	602	49	153	0	7	C:\Users\Hani Maisarah\Downloads\rfid\rfid-master\src\MFRC522Exter
MFRC522Extended.h	120	2.869	58	3	19	0	0	C:\Users\Hani Maisarah\Downloads\rfid\rfid-master\src\MFRC522Exter
require_cpp11.h	12	0.287	5	2	2	0	0	C:\Users\Hani Maisarah\Downloads\rfid\rfid-master\src\require_cpp11.h

Figure 6.3 Scanning code for Arduino in RFID system

Figure 6.3 is showing the pie chart for the code analysis that is done using VGC for Arduino coding that is read as c++ language. Based on the pie chart, there are 9 potentially dangerous code counted in the RFID system program.

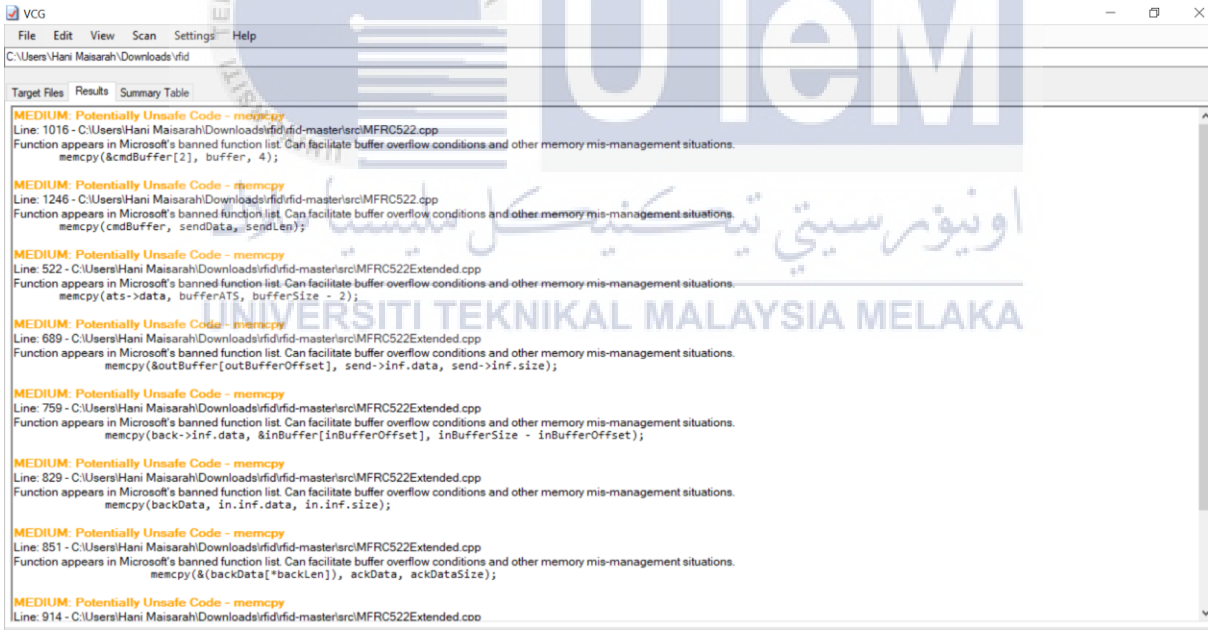


Figure 6.4 Details for the dangerous code

Based on Figure 6.4, these are the potentially dangerous code that are counted in the pie chart previously. Referred from a website, the use of "unsafe" functions, such as memcpy, strcpy, strncpy, and other C++ mainstays, is one of the fundamental causes. These routines are deemed dangerous since they deal with unbounded buffers directly, and without thorough bounds checking, they will generally overflow any target buffers (Ouglen, 2011).

- Voice Recognition System

1. Accuracy Analysis

For this system, I create five users. Then each user is tested using confusion matrix method to the calculate accuracy of the system. First step, each users need to log in their own accounts and identify their voices. The second step, they need to log in into the others account to identify if the system still can recognize their voices or not. The table below shows the result of this analysis:

Table 6.7 Accuracy Analysis Voice Recognition

User	True Positive	True Negative
Hani Maisarah	✓	✓
	✓	✓
	✓	✓
	✓	✓
	✓	✓
	✓	✓
	✓	✓
	✓	✓
	✓	✓
	✓	✓
	✗	✓
	✓	✓
	✓	✓
	✓	✓
	✓	✓
	✗	✓
	✓	✓
	✓	✓
	✓	✓
	✓	✓
	✗	✓

Haziq Iskandar	✓	✓
	✓	✓
	✓	×
	✓	✓
	×	✓
	✓	✓
	✓	✓
	✓	✓
	✓	✓
	✓	✓
	✓	✓
	✓	✓
	✓	✓
	×	✓
	✓	✓
	✓	×
	✓	✓
	✓	✓
	✓	✓
	✓	✓
Hedi Izham	✓	✓
	✓	✓
	✓	✓
	✓	✓
	✓	✓
	✓	✓
	✓	✓
	✓	×
	✓	✓
	✓	✓
	✓	✓
	✓	✓

	✓	✓
	✓	✓
	✓	✓
	✓	✓
	×	✓
	×	✓
	✓	✓
	×	✓
Ruzaini	✓	✓
	✓	✓
	×	✓
	✓	✓
	✓	×
	✓	✓
	✓	✓
	✓	✓
	×	✓
	×	✓
	✓	✓
	✓	✓
	×	✓
	✓	✓
	✓	×
	✓	✓
	✓	✓
	×	✓
	✓	✓
	✓	✓
Zainal Subari	×	✓
	✓	✓
	✓	✓
	✓	✓

	✓	✓
	✓	✓
	✓	✓
	✓	×
	×	✓
	×	✓
	×	✓
	×	✓
	✓	✓
	✓	×
	✓	✓
	✓	✓
	✓	✓
	✓	✓
	✓	✓

Table above shows the result of the analysis. For the true positive is the outcome when the true users successfully identify their voices while the true negative is the outcome for false users unsuccessful to identify their voices using other accounts. Then, the accuracy of the voice recognition system will be calculate using this formula:

((TP + TN) / Total) X 100

For this result, the accuracy of the voice recognition is **((82 + 94) / 200) X 100 = 88%.** The result is affected by surrounding and health condition of the users which can change the users' voices. Other cases, the system recognize female user with others female users which have similar tone.

1. **Scan Time**

Table 6.8 Scan Time Voice Recognition

Test	Time taken (sec)
1	6.45
2	5.94
3	6.90
4	6.25
5	7.05
6	5.94
7	5.36
8	6.25
9	5.93
10	6.15
11	5.52
12	7.01
13	6.35
14	5.78
15	5.95
16	4.73
17	5.26
18	6.21
19	6.26
20	5.73
Average: (121.02) / 20 = 6.05 second	

Table above shows the result for the time taken for the scanner to finish scanning and open/close the gate. The formula used to get the average time taken is:

(total of all time taken) / (number of tests)

The average time taken for RFID scanner to scan the tag is **(121.02) / 20 = 6.05 second.**

2. **Scan Range**

For Voice Recognition system, the scan range is not too far as the background noise will interrupt if the voice is too far. For this system, to scan, the user needs to speak a random word that is generated automatically. If the system cannot hear the word clearly, it will not recognise the authenticated user.

Table 6.9 Scan Range for Voice Recognition

Scan distance (cm)	Result
2.0	Too close.
4.0	Too close.
6.0	Scanned, but not clear.
8.0	Successfully scanned.
10.0	Successfully scanned.
12.0	Successfully scanned.
14.0	Scanned, but not clear.
16.0	Too far, too many backgrounds noise.
18.0	Too far, too many backgrounds noise.
20.0	Too far, too many backgrounds noise.
Range: 6.0 – 14.0 cm	

3. Static Analysis

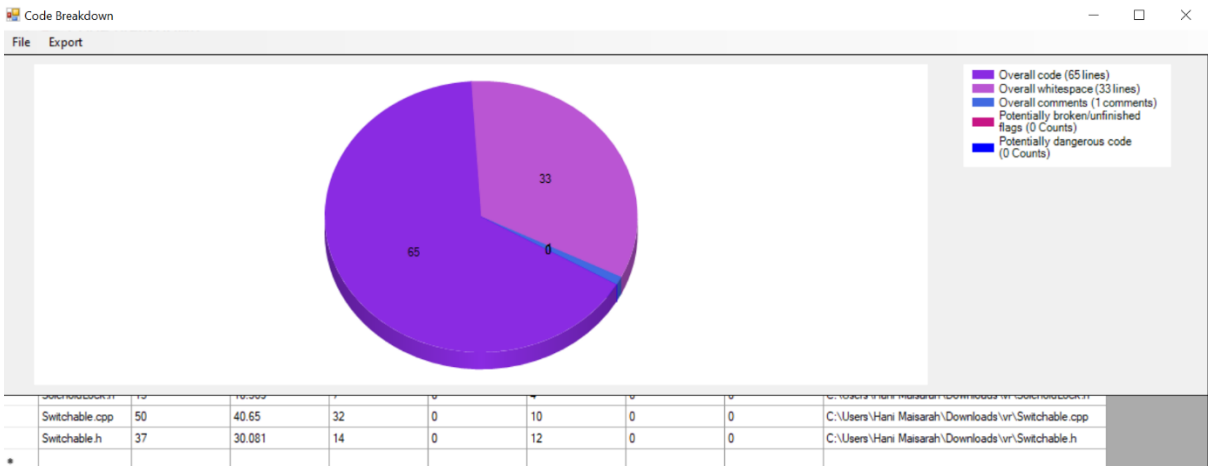


Figure 6.5 scanning code for Arduino in Voice Recognition

Based on Figure 6.5, the pie chart is showing the coding analysis that is done in VCG for Arduino coding that is read as c++ language. From the pie chart, there is no potentially dangerous code in the Arduino Code.

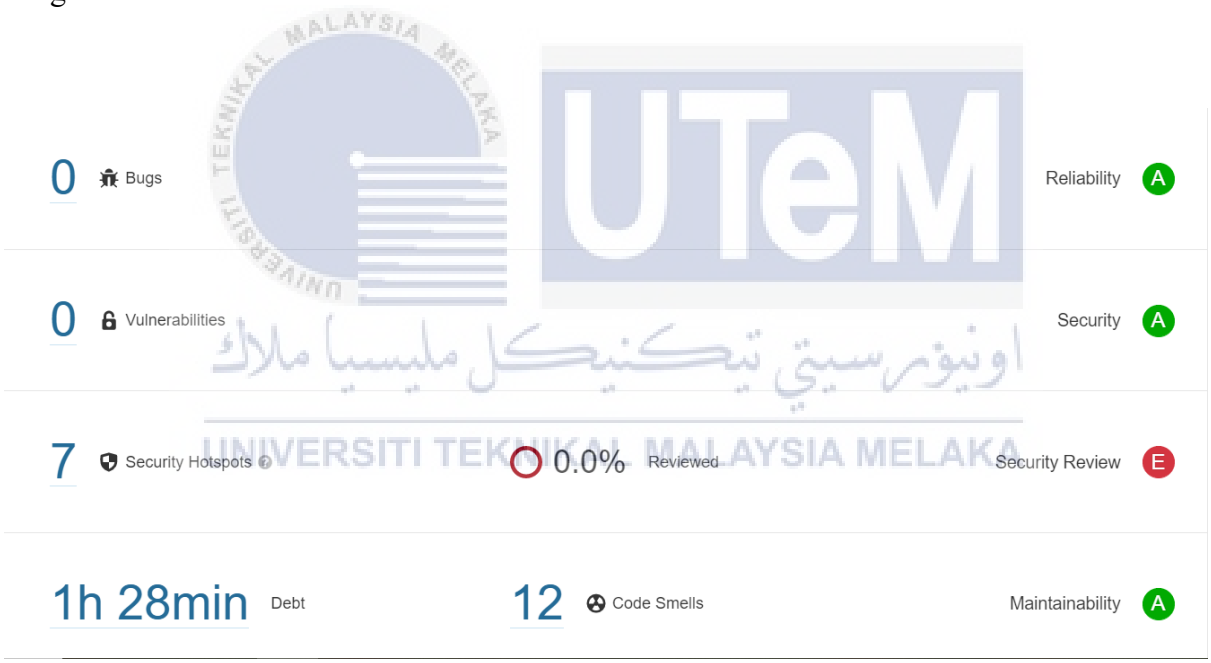


Figure 6.6 Scanning code for Python in Voice Recognition

Based on figure 6.6, the figure is showing the output after analysing Python code in Sonarqube. The reason why Sonarqube is used is because VCG cannot analyse Python. From the analysis, there are 7 security hotspots in the Python code but there is no vulnerability.

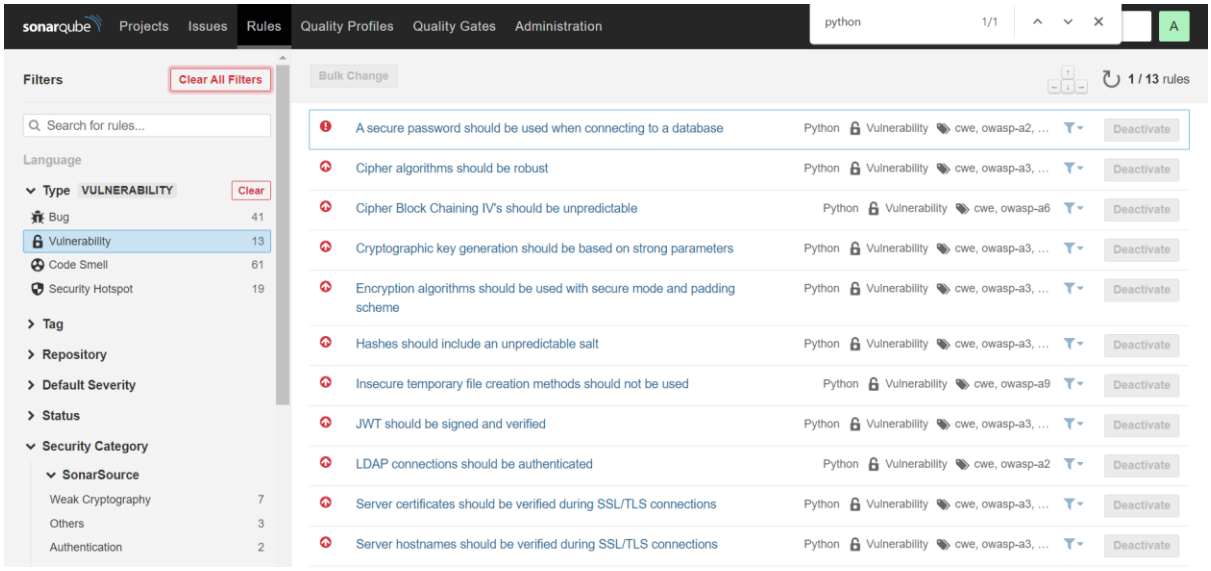


Figure 6.7 Rules used to analyse Python code.

Figure 6.7 shows the rules used to run Python code. If there are no vulnerabilities, that means the code does not breaking any rules implemented in the scanner.

Figure 6.8 Security Hotspots

Based on figure 6.8, there are 7 security hotspots in the code. Based on Sonarqube website, Security Hotspot indicates a part of code that needs to be reviewed for security reasons. However, the overall security of the application may not be affected.

6.2 Conclusion of Analysis

To finalize the analysis, the parameters used to analyse the platforms will be compared between each security methods. There are four parameters used which are Accuracy Analysis, Scan Time, Scan Range and Static Code Analysis.

For Accuracy Analysis, the highest accuracy percentage is the platform using QR Code System. QR Code System achieve 99% accuracy, which is close to a perfect system. It proves the findings on Literature Review for Chapter 2 that said QR Code is reliable and accurate. RFID System achieve 95% accuracy and Voice Recognition achieve 88% accuracy. The accuracy analysis is affected by so many conditions and environments. For example, for the Voice Recognition System, voice can sound different day and night. Thus, it can affect the accuracy percentage result. However, for this analysis, QR Code achieve the highest accuracy percentage. From the preliminary research in Chapter 3, 42.1% of the respondents choose "Efficiency" as the most important aspect in Automated Gate System.

Next, for scan range, RFID System can scan and read the tag further than the other two. The range for RFID System is up to 30 cm far. While QR Code can only scan 4 to 10 cm in range. Cameras need a little space for them to be able to read the QR Code symbols. For Voice Recognition, the system can scan and read the voice from 6 to 14 cm. If the voice is scanned too near, it will become not clear enough for the system to be able to recognize the voice. If it is too far, there will be a lot of backgrounds noises that could affect the reading. Once again, it approves the finding found in Literature Review as RFID System can read long range of distance while QR Code and Voice Recognition can only read a short range of distance.

Then, for scan time, RFID System can scan and read in 1.47 seconds in average. It is really quick compared to the other two security methods. Voice Recognition system took the longest to scan and read which is 6.05 seconds in average. For QR Code system, it took 5.14 seconds in average to read and scan the system. Once again, from this analysis, it proves the finding in Literature Review where it said that RFID System can read a lot of tags at once.

Lastly, for Static Code Analysis, based on the analysis result, both RFID System and Voice Recognition System has security issues with their own code. For RFID System, there are 9 potentially dangerous code recorded by VCG and there are 7 security hotspots recorded for

Voice Recognition System, that is analysed by Sonarqube for Python code. For QR Code System, there are no dangerous code recorded during static code analysis session.

Thus, we can conclude that QR Code System is the most secured security method, compared to the other two security methods as both Accuracy and Static Code Analysis are security related analysis. QR Code System is the most secured security method based on the two-security related analysis. This once again proves that QR Code is accurate and the most secured security method based on the preliminary research question. 37.2% of the respondents answered QR Code is the most secured security method out of three other choices. Then, RFID System can achieve for the most efficient security method compared to the other two as RFID System achieve great results in Scan Range and Scan Time Analysis that are made to check efficiency rate. This proves the finding in Literature Review that RFID System can work efficiently.

6.3 Conclusion

In conclusion, this chapter is the most important part of this project. All platforms are being analysed to figure out which security method is the most secure among all platforms. For the next chapter, it will conclusion for the overall of this system. The conclusion will include in few aspects such as limitation and future works for this project.

CHAPTER 7: PROJECT CONCLUSION

7.1 Introduction

In this chapter, I will conclude and summarize the overall project from beginning until the completion of the system. The contribution, limitation and future work of the project will also be stated for any further improvement in the future. This will effectively improve the efficiency of the analysis and make it more beneficial and comprehensive.

7.2 Project Summarization

Analysis of the Security Methods in Automated Gate System is an analysis to figure out which security method is the most secured to be implemented in the automated gate system. There will be three (3) platforms with different security methods that will be tested using specific tools and technique. The security methods that will be analysed are QR Code System, RFID System and Voice Recognition System. The security methods will be tested by using four parameters which are accuracy analysis, scan time, scan range and static analysis. Each platform will be developed in two phases which are hardware and software development.

The first objective of this project is to identify security method, evaluation tools and parameter that implemented in Automated Gate System. To complete the analysis, three platforms need to be implemented using different security methods. After the security methods have been identified and implemented, evaluation tools and parameter will be used to analyse the security methods.

The second objective of the project is to develop the platforms of AGS with three different security methods. Three platforms have been developed using QR Code system, RFID system and Voice Recognition system. For QR Code, it will be using Arduino Uno Microcontroller and Visual Basic. For RFID, it will also be using Arduino Uno Microcontroller, RFID scanner and Arduino IDE. Lastly, for Voice Recognition, it will be using Arduino Uno Microcontroller, Python IDE and Arduino IDE.

The third objective is to analyse the platforms developed using the selected evaluation tools and parameter. The platforms will be analysed using four different parameters which are accuracy analysis, scan time, scan range and static analysis. The tools that are used are Sonarqube and VisualCodeGrepper. This is very important as this project is based on this analysis.

Analysis of the Security Methods in Automated Gate System has been fully developed and analysed and meet all the objectives in this project. The hardware and software are well integrated with each other and provide a comprehensive system to smooth out the analysis part. This analysis has figure out the most secured security methods to be implemented based on the methods analysed.

a. Project Weakness

- Beneficence

  When the analysis is done, it will not be as beneficial to the real industry as they are using a high-end product that will cost more money. The result of the analysis is differed, according to the products used. For example, MC522 RFID module is a cheap product, so the frequency is not high. It affects the scan and read range for RFID.

- Open-Source Tools

  For the analysis, Sonarqube and VisualCodeGrepper are used and these tools are open-source tools. Hence, there are limited features that can be used to analyse the code. Details of the vulnerabilities or security issues are not explained and showed well as it is free and needed to be paid to use extra features. This weakness affects the analysis done as it cannot be shown in detail.

b. Project Strength

- Provide code scanning for each platform

  Each platform is developed and scanned to achieve the objectives of this project. For coding in Arduino, the coding is read as c++ language and it is analysed using VisualCodeGrepper along with the coding in VB.NET. For Python code, it is analysed using Sonarqube. Every coding in every platform is analysed using appropriate tools and parameters.

- Done a thorough testing for each platform

  Each platform is tested very thoroughly by using four parameters. Not only security testing, scan range and time are also included to provide a better and clear analysis.

- Figured out the most secured security system based on the analysis

  In this analysis, the most secured security analysis has been figured out by comparing three security methods implemented in three different platforms.

7.3 Project Contribution

Analysis of the Security Methods in Automated Gate System aims to provide an analysis to help those companies solving the problem of choosing reliable security method to be implemented in the automated gate wisely. It is crucial to ensure each company knows what security aspects need to be implemented to prevent any unauthorized enters.

In this analysis, the security methods that are going to be analysed has been identified. The security methods used for this analysis are QR Code System, RFID System and Voice Recognition System. All platforms are set up correctly and the software application are

well integrated with hardware setup. The platforms are set up perfectly so that it will give a clear idea on how it will look like in real environment.

To complete the analysis, tools needed to analyse the security methods have also been proposed. Tools and parameters have been proposed and used for the analysis in Chapter 6: Testing & Analysis. The parameters used are Accuracy Analysis, Scan Time, Scan Range and Static Code Analysis. Tools that are used are VisualCodeGrepper and Sonarqube. The analysis has been done completely.

Analysis of the Security Methods in Automated Gate System has also developed and analysed the proposed platform using different security methods. All platforms are developed completely, well integrated for both hardware and software requirements.

7.4 Project Limitation

This project consists of some limitation which stated as below.

- Platforms

  Each platform is made with affordable hardware; however, it does affect the analysis a bit as the result is not as expected when using a cheap product. When the analysis is done, it will not be as beneficial to the real industry as they are using a high-end product that will cost more money. The result of the analysis is differed, according to the products used.

- Tools used

  Tools to analyse the security methods has a limited features that affects the analysis progress. It is important to analyse the code deeper as the main reason code analysis is done is to find the vulnerabilities in codes. Plus, the

tools used might give false positive feedback that might affect the result of the analysis.

7.5 Future Works

There are many future works can be done in the analysis to make it more beneficial and functional. Below shows few examples to improve the analysis.

- Analysis Tools

  This analysis can be improved by using a tool that is systemized to analyse code to find vulnerabilities with many features. With that, the result of the analysis will be more accurate and the codes are properly being analysed one by one.

- Parameters

  More defined parameters added to analyse the security methods. This can be used to analyse more security features in a platform.

- Platforms

  The platforms are developed more closely to how it is in the real industry. So, this analysis is beneficial and can be useful to more people. By using what they use in the real industry, the analysis will come out more precise.

7.6 Conclusion

This project is to analyse the security methods in automated gate system and figure out which security method is the most secure. The security methods are QR Code System, RFID System and Voice Recognition System. This project provides three platforms with different security

methods implemented in the automated gate system. All platforms are analysed using four parameters which are Accuracy Analysis, Scan Time, Scan Range and Static Code Analysis and use appropriate tools which are Sonarqube and VisualCodeGrepper. This project met all the objectives stated in Chapter 1 and the testing and analysis part are clearly shows in previous chapter. Lastly, this project is a success as it can figure out which security method is the most secure at the end of the analysis.

REFERENCES

Asha. N, A. S. Syed Navaz, J. Jayashree, & J. Vijayashree. (2018). RFID BASED AUTOMATED GATE SECURITY SYSTEM . *ARPN Journal of Engineering and Applied Sciences*, 8904.

Erman Hamid, Lim Chong Gee, Nazrulazhar, Syarulnaziah Anawar, & Zakiah Ayob. (2018). Implementation of Intelligent Automated Gate. *(IJACSA) International Journal of Advanced Computer Science and Applications*, 359.

Hairol Nizam Mohd. Shah, Mohd. Zamzuri Ab Rashid, Mohd. Fairus Abdollah, Muhammad Nizam Kamarudin, Chow Kok Lin, & Zalina Kamis. (2014). Biometric Voice Recognition in Security System. *Indian Journal of Science and Technology*, 110 - 111.

Ismail Saad Eltoum , & Zhaojun Xue . (2014). Automatic Gate Control System Based. *International Journal of Engineering Research & Technology (IJERT)*, 81.

Larrabee, R. D. (n.d.). *WILLRICH PRECISION INSTRUMENT*. Retrieved from PRECISION, ACCURACY, UNCERTAINTY, AND TRACEABILITY: https://willrich.com/metrology-education-old/precision-accuracy-uncertainty-and-traceability/

Marcilio, D., Furia, C. A., Bonifácio, R., & Pinto, G. (2020). SpongeBugs: Automatically generating fix suggestions in response to. *The Journal of Systems & Software*, 1-18. Retrieved from Core.

McGraw, G., & Chess, B. (2004). Static Analysis for Security. *Building Security In*, 76-78.

Ouglen, A. (2011, April 20). *Stack Exchange*. Retrieved from Secure memcpy for pure C: https://security.stackexchange.com/questions/3210/secure-memcpy-for-pure-c

RFID4u. (2021). Retrieved from How to Select a Correct Tag - Frequency: https://rfid4u.com/rfid-frequency/

Software Testing | Security Testing. (2019, May 10). Retrieved from GeeksforGeeks: https://www.geeksforgeeks.org/software-testing-security-testing/

Yugansh Khera, D. K. (2019). Analysis and Impact of Vulnerability Assessment. *2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (Com-IT-Con)*, 527.