

SMARTPHONE-NFC BASED GUARD TOUR MONITORING SYSTEM
FOR REAL TIME DATA RECORDING (eSmartGuard)

KHOR MING EN

This Report Is Submitted In Partial Fulfillment Of Requirements For The Bachelor
Degree of Electronic Engineering (Computer Engineering)

Fakulti Kejuruteraan Elektronik dan Kejuruteraan Komputer
University Teknikal Malaysia Melaka

June 2017

BORANG PENGESAHAN STATUS LAPORAN
PROJEK SARJANA MUDA II

Tajuk Projek : Smartphone-NFC based Guard Tour Monitoring System for Real Time Data Recording

Sesi Pengajian :

1	6	/	1	7
---	---	---	---	---

Saya Khor Ming En mengaku membenarkan Laporan Projek Sarjana Muda ini disimpan di Perpustakaan dengan syarat-syarat kegunaan seperti berikut:

1. Laporan adalah hakmilik Universiti Teknikal Malaysia Melaka.
2. Perpustakaan dibenarkan membuat salinan untuk tujuan pengajian sahaja.
3. Perpustakaan dibenarkan membuat salinan laporan ini sebagai bahan pertukaran antara institusi pengajian tinggi.
4. Sila tandakan () :

SULIT*

*(Mengandungi maklumat yang berdarjah keselamatan atau kepentingan Malaysia seperti yang termaktub di dalam AKTA RAHSIA RASMI 1972)

TERHAD**

** (Mengandungi maklumat terhad yang telah ditentukan oleh organisasi/badan di mana penyelidikan dijalankan)

TIDAK TERHAD

Disahkan oleh:



(TANDATANGAN PENULIS)

Tarikh: 25/5/2017



(COP DAN TANDATANGAN PENYELIA)

Tarikh: 13/6/2017

Vigneshwara Rao A/L Gannapathy
Pensyarah Kenan

Fakulti Kejuruteraan Elektronik dan Kejuruteraan Komputer

Universiti Teknikal Malaysia Melaka (UTeM)

Hang Tuah Jaya

76100 Durian Tunggal, Melaka

“I hereby declare that the work in this project is my own except for summaries and quotations which have been duly acknowledged”




Signature :

Author : KHOR MING EN

Date : 25th MAY 2017

“I acknowledge that I have read this report and in my opinion this report is sufficient in term of scope and quality for the award of Bachelor of Electronic Engineering (Computer Engineering) with Honors.”

Signature : 

Supervisor's Name : VIGNESWARA RAO A/L GANNAPATHY

Date : 25th MAY 2017

A very special dedication for my beloved family especially to my parents,

Khor Chin Thye and Kam Kuan Fong.

Also for my gracious supervisor Engr. Vigneswara Rao A/L Gannapathy

ACKNOWLEDGEMENT

I would like to express my deepest appreciation for those who provided me the possibility to complete this report. A special gratitude I give to our final year project supervisor, Mr. Vigneswara Rao, whose contribution in stimulating suggestions and encouragement, helped me to coordinate my project especially in writing this report.

Furthermore, I would also like to acknowledge with much appreciation the crucial role of the staff of Pejabat Keselamatan, who gave the permission to go around the whole university in testing the system to complete the task “eSmartGuard System”. Last but not least, many thanks go to the previous student of the project, H’ng Jia Jiunn whose have invested his full effort in guiding me in achieving the goal. I have to appreciate the guidance given by other supervisor as well as the panels especially in our project presentation that has improved our presentation skills thanks to their comment and advices.

ABSTRACT

eSmartGuard system is developed to improve the safety level of the people and assets in universities, companies, or any organization by assisting the security personnel to patrol and performs their duty efficiently. The eSmartGuard NFC tags are installed at multiple points along the patrolling routes with unique Identification (ID) which identify different locations/points or routes. The guards will patrol according to their planned routes and records their arrival by scanning the NFC tagged checkpoints with eSmartGuard reader (Smartphone). The system is connected wirelessly to its cloud database on the internet. In line with current trend in technology where information are accessible at the fingertips. eSmartGuard mobile application provides convenient access to system efficiently. Once the NFC tags are scanned, then the information will be transmitted to cloud database. These information (i.e. location/point scanned, time, date, guard ID) are retrievable remotely via mobile device and computer. The reports are available in the form of duty, weekly, monthly and yearly basis for analysis and continual improvement. An important value added (or feature) of this system is real time incidents detection or emergency events with instant notification to authorized personnel. eSmartGuard system is able to help the organization to provide excellent and efficient implementation of standard operating procedure (SOP) and improve the security of the assets and premises.

ABSTRAK

Sistem eSmartGuard dibangunkan untuk meningkatkan tahap keselamatan rakyat dan aset di universiti, syarikat, atau mana-mana organisasi dengan membantu anggota keselamatan untuk membuat rondaan dan melakukan tugas mereka dengan cekap. Tag NFC dipasang di pelbagai tempat di sepanjang laluan rondaan dengan pengenalan unik (ID) yang mengenal pasti lokasi atau laluan yang berbeza. Pengawal akan membuat rondaan mengikut laluan yang dirancang mereka dan ketibaan mereka akan direkodkan dengan pengimbas NFC (telefon pintar). Sistem ini disambungkan secara wayarles kepada pangkalan data awan di internet. Selaras dengan trend semasa dalam teknologi di mana maklumat boleh diakses di hujung jari. Aplikasi mudah alih eSmartGuard menyediakan akses mudah ke system dengan cekap. Setelah tag NFC diimbas, maklumat itu akan dihantar kepada pangkalan data awan. Maklumat seperti lokasi / tempat diimbas, masa, tarikh, pengawal ID boleh didapati dimana-mana sahaja melalui peranti mudah alih dan komputer. Laporan yang ada dalam bentuk harian, mingguan, bulanan dan tahunan asas adalah untuk analisis dan penambahbaikan yang berterusan. Satu nilai yang penting ditambah (atau ciri) sistem ini adalah pengesanan insiden dalam masa sebenar atau kecemasan dengan pemberitahuan segera kepada kakitangan atasan. Sistem eSmartGuard dapat membantu organisasi untuk menyediakan pelaksanaan yang sangat baik dan cekap melalui standard prosedur operasi (SOP) selain meningkatkan keselamatan aset dan premis mereka.

TABLE OF CONTENTS

CHAPTER	INDEX	PAGE
	PROJECT TITLE	i
	PROJECT STATUS APPROVAL FORM	ii
	DECLARATION	iii
	SUPERVISOR'S DECLARATION	iv
	DEDICATION	v
	ACKNOWLEDGEMENT	vi
	ABSTRACT	vii
	ABSTRAK	viii
	TABLE OF CONTENTS	ix
	LIST OF FIGURES	xii
	LIST OF TABLE	xiv
	LIST OF ABBREVIATIONS	xv
I	INTRODUCTION	
	1.1 Project Overview	1
	1.2 Problem Statement	2
	1.3 Objectives	3
	1.4 Scope of Project	3
	1.4.1 Network	3
	1.4.2 Software	4
	1.4.3 Hardware	4

II LITERATURE REVIEW

2.1	Theoretical Research	5
2.1.1	NFC	5
2.1.2	Attendance System	7
2.2	Types of Guard Tour Systems	8
2.2.1	Mechanical Watchclock	8
2.2.2	RFID-based Data Logger	9
2.3	Review of Relevant Work	11
2.3.1	Bluetooth Based Attendance Management System	12
2.3.2	Wireless Attendance Management System based on Iris Recognition	12
2.3.3	Fingerprint Biometric Authentication	13
2.3.4	Remote Monitoring System based on RFID using GSM Network	14
2.4	Comparison of Relevant Work	15

III PROJECT METHODOLOGY

3.1	Hardware Implementation	16
3.1.1	NFC-enabled Android Phone	16
3.1.2	NFC tags	17
3.1.3	GSM Modem	18
3.2	Software Development	19
3.2.1	Android Studio	19
3.2.2	WampServer	20
3.2.3	Sublime Text 3	21
3.2.4	Visual Studio	22
3.2.5	NFC TagWriter	23
3.3	Network Configuration	24

3.3.1	000webhost	24
3.3.2	FileZilla Client	26
3.3.3	Remote MYSQL database	27
3.3.4	OZEKI NG SMS Gateway	29
3.3.5	ODBC Connector	32
3.4	Flowchart of the Project	33
3.5	System Block Diagram	34
3.6	System Integration	36

IV RESULTS AND DISCUSSION

4.1	Android Application	37
4.2	Login and Register Page	38
4.3	Main Page	39
4.4	Webpage	42
4.4.1	Patrols Page	43
4.4.2	Emergency Page	45
4.5	eSmartGuard.exe	46
4.6	Emergency Alert	48
4.7	Overall System	50

V CONCLUSION AND RECOMMENDATION

5.1	Conclusion	53
5.2	Recommendation	54

REFERENCES	55
-------------------	-----------

LIST OF FIGURES

NO	TITLE	PAGE
2.1	Amano PR600 Watchclock	8
2.2	RFID-based Data Logger Components	9
2.3	RFID-based Data Logger operation	10
2.4	Bluetooth Based Attendance System	12
2.5	Iris Recognition Verifying Process	13
2.6	Fingerprint Identification Process	14
2.7	System Architecture of Remote Monitoring System	15
3.1	NFC-enabled Android Phone	17
3.2	NFC tags	18
3.3	GSM Modem	18
3.4	Android Studio	19
3.5	WampServer	20
3.6	Sublime Text 3	21
3.7	Visual Studio 2015	22
3.8	NFC TagWriter	23
3.9	Statistics of 000webhost	24
3.10	000webhost FTP	25
3.11	Website details	25
3.12	FileZilla Client	26
3.13	Login page of phpMyAdmin	27
3.14	phpMyAdmin main screen	28
3.15	Database and tables	28
3.16	OZEKI NG admin login page	29

3.17	GSM Configuration	30
3.18	Database Connection	30
3.19	Inbox	31
3.20	ODBC configuration	32
3.21	Flowchart of the Project	33
3.22	Block diagram of the System	34
3.23	Android Connect to PHP and Database	35
3.24	Flow Diagram of Integrated System	36
4.1	Icon of the Android Application and Android Phone Features	37
4.2	Login and Register Page	38
4.3	Main Interface Layout	39
4.4	Scanning the Checkpoints	40
4.5	Checkpoints Completed	41
4.6	Homepage (via Computer)	42
4.7	Homepage (via mobile phone)	42
4.8	Patrol page (via Computer)	43
4.9	Searching Function is applied (via Computer)	44
4.10	Patrol Arrivals in table form (via mobile phone)	44
4.11	Report in Excel Form	45
4.12	Emergency Page	46
4.13	Exact Emergency Location	46
4.14	Admin Portal and Main Menu	47
4.15	Patrol Arrival	47
4.16	Emergency occurs	48
4.17	Received Email	49
4.18	Received SMS	49
4.20	Flow Chart of the Overall System	50

LIST OF TABLE

NO	TITLE	PAGE
2.1	Comparison of Project	15

LIST OF ABBREVIATIONS

NFC	-	Near Field Communication
GPS	-	Global Positioning System
SMS	-	Short Message Service
GUI	-	Graphical User Interface
RFID	-	Radio Frequency Identification
RF	-	Radio Frequency
ID	-	Identity
PC	-	Personal Computer
GSM	-	Global System for Mobile Communication
NDEF	-	NFC Data Exchange Format
URL	-	Uniform Resource Locator
SIM	-	Subscriber Identification Module
IDE	-	Integrated Development Environment
SQL	-	Structured Query Language
API	-	Application Program Interface
STL	-	Standard Template Library
JSON	-	JavaScript Object Notation
XML	-	EXtensible Markup Language
IP	-	Internet Protocol
NAT	-	Network Address Translation
HTTP	-	Hypertext Transfer Protocol
ODBC	-	Open Database Connectivity
PHP	-	Hypertext Preprocessor

CHAPTER I

INTRODCUTION

1.1 Project Overview

eSmartGuard system is a system used to help companies or organizations to organize, preform and execute guard tours or patrol in their asset, besides to ensure that employees will perform their duties within a predetermined time interval. One of the way to ensure these safety level is to manage the security operations efficiently by knowing their currently patrolled locations and their patrol status. Security guards must patrol the building as scheduled, in order to relieve the worrying and anxiety of peoples. Android phone and NFC tags can help in creating a better security touring system. In this project, NFC tags act as checkpoints for the touring system while Android phone used as a scanner. An Android application with login and register functions, as well as tagging function has been developed. The Android phone will start recording real-time attendance once the user has reached the checkpoint. The recorded information is stored in the cloud database and can be viewed remotely via computer or mobile device. Furthermore, this system can assure the user safety by sending an alert message immediately to the administrator via SMS and email when the user failed to reach the next checkpoint within predefined time. Therefore, by using this real-time recording system, it is possible to improve the tour performance as well as the safety level of the security personnel.

1.2 Problem Statement

During the patrol, some of the security officials may perform their duties alone and with a few other officials. Or even worse, in some cases there are no supervision from superior at all. Sometimes, they do not want to patrol according to the scheduled timetable. It may be particularly aggravating if bad weather conditions lead to patrols under rain, thunderstorm or fog. And even if they perform patrols, there may be some parts of the tour are hard to get into and urge them to patrol for another day/time.^[1]

The security guards may go to other place during the patrolling session. For example, supposedly they need to patrol in certain buildings, but they go to other places that are not related to their duties. Hence, none of the top security officials know whether they really patrol on a given schedule. Their dishonest action may allow intruders to do something that will cause the asset to be lost or will threaten the security risk.

The security touring system becoming very crucial in every place such as residential, business places, universities and schools as the number of crime rates is increasing day by day. However, the problem with the current security touring system is it is not cost-efficient, does not have real-time data recording and is not easy to establish. In the earlier system, when the security guards are start moving from one checkpoint to another, they must tag the specific tag in every checkpoint using RFID-based data loggers. The data recorded will not be available in main system automatically as they have to manually transfer the data after the patrolling is done. In this case, the problem is, sometimes all the data can be lost if the recorder has been dropped or the recorder is running out of battery. Besides, in most cases the system unable to retrieve the old data which is very important for management to track back all the guard patrolling information.

In addition, in the current market-ready system the guard can easily manipulate the security touring system by skipping the checkpoints or just transferring the data in main system without patrolling the respective area. Besides, the guard is unable to notify the superior if they are attacked by intruders during patrolling session. Apart from this, the current system will not be able to detect the current location of the guard where the emergency occurs. In a nutshell, the robbery is still valid because the constraints of the current system.

1.3 Objectives

The goals of this project are:

- To develop an Android based mobile application that monitor and record the movement of guard during the patrolling session.
- To create an Internet of Things (IoT) based application that can retrieve real time information remotely via mobile phone and computer.
- To build a system that automatically notifies an incident to main control center.

1.4 Scope of Project

Scope of project has been delegated into 3 major parts which are network, software and hardware. Firstly, the network need to be configured for the network system between server, android application and the web application. Android application is able to send the patrol arrivals to the server by using WiFi or Mobile Data or SMS. Second, the software development has been focused on android application. The function of the application is to record the patrol arrivals by scanning the NFC tags and then the arrivals will be sent to the server. Lastly the hardware need to be setup to make a connection between boards.

1.4.1 Network

The project is using internet connection between the server, the android application and web application. Therefore, for this framework project, internet connection is used to send data and data retrieval purpose. Once NFC tags are scanned, the information will be sent to the server through the internet and the data will be saved in the database. Prior to that, the server need to be created in order to receive the data from the phone and to access to the database. If there is no Internet connection when the security guards scanning the tag, SMS is going to become an alternative way for sending the patrol arrival to the server via SMS Gateway.

1.4.2 Software

For this project, the software development has been focused on android application, webpage application and computer application. The android application used to record the patrol arrivals and then send to the cloud. The webpage application has been developed for data retrieving purpose while for computer application is used for administrative management.

The mobile application (Android) has been developed by using a tool called Android Studio. This application must have a simple login system which can enter of identifier information into a system by a security guards in order to access that system. After the system has been logged in by the authorized user, the system is able to scan the NFC tags which are placed at the certain checkpoints. This system can record the tagged time, location, longitude and latitude after the NFC-smartphone has been touched to the NFC chips. The Android application is used to send the records into the cloud and the record can be retrieved remotely by superior in real time.

Next, the webpage which contents patrol arrivals and emergency records have been designed so that the administrator can go through the records from time to time. Administrator is also able to download the reports in the form of weekly, monthly or yearly basis.

Furthermore, a simple computer application called GUI has been created using Visual Studio 2015. The GUI must be able to prompt a simple register system, which is for the user registration and admin registration. Besides that, the developed GUI must be able to display information recorded from the remote database. The GUI also must include search functions so that superior can filter all the extra information.

1.4.3 Hardware

The hardware used in this project are NFC tags, NFC android phone and GSM modem. NFC tags has been inserted the name of the location. The android phone need to have NFC functions so that the android phone is able to scan the NFC tags when phone is placed near to it. Lastly, GSM modem has been setup to receive the SMS sent by the security guard.

CHAPTER II

LITERATURE REVIEW

This chapter provides an overview of previous knowledge sharing and intranet research. This paper introduces the case study framework, which includes the focus of the research described in this thesis.

2.1 Theoretical Research

Theoretical studies include concepts, as well as their definitions and references to relevant academic literature, for the existing theory of research. Theoretical research must demonstrate the understanding of theory and concepts, which are related to the broader field of knowledge that is being considered. This research will be fully focused on the NFC and attendance systems to understand the relationship between these principles and concepts better.

2.1.1 NFC

Near field communication (NFC) is a set of protocols that allows two electronic devices to exchange information. Two NFC devices can establish radio data communication in a range of 10cm from each other. An NFC-enabled device can read information stored in electronic tags. Short-range communications using the technology in the past that are proprietary to the manufacturer, for applications such as a stock ticket, payment readers, and access control. ^[2]

The techniques involved are seemingly simple. From the radio frequency identification (RFID) evolution of technology, NFC chip as a wireless link operation.^[2] When it is activated by another chip, a small amount of data can be transferred between the two devices while keeping a few centimetres from each other. It does not require a pairing code to connect, and is less power efficient than other types of wireless communications because it uses a chip that operates at a very low amount of power (or passively, more or less).^[3] At its core, NFC is used to identify us through cards and devices (as well as extensions, bank accounts and other personal information).^[4]

NFC communication can be established between two NFC-enabled devices or between devices and tag. The communication process consists of 2 devices, one is active while another one is passive. Active device is responsible for reading, sending, or writing the database. On the other hand, a passive device owns the characteristics in such a way that NFC tag possesses likewise, consists of readable information but unable to read any information itself. Passive devices (such as NFC tags) contain information that other devices can read but do not read any information itself. Other people can read the information, but even though the information sent to the authorized device, the logo itself does not perform any operation.^[4] There are three main modes of operation:

- Reading and writing: A device reads from a tag or writes data to a tag.
- Host Card Emulation (HCE): The device acts the behavior of a tag/card. For example, one smartphone can be consisted of several payment cards or attendance cards.^[5]
- Peer to Peer (P2P): A connection is established between two NFC devices.

The tag dispatch system like Android-powered devices can read NDEF data from the NFC tag. The tag dispatch system analyzes the discovered NFC tags, classifies the data appropriately, and starts an application that is interested in data categorized. Applications that want to process scanned NFC tags can declare an intent filter and request to process the data.^[6]

Unless NFC is disabled in the device's Settings menu, Android devices typically find NFC tags when the screen is unlocked. When an Android device discovers an NFC tag, the required behavior is to allow the most appropriate activity to process the intent,

without requiring the user to use any application. Since the device scans the NFC tag in a very short range, it is likely that the user manually selects an activity to force them to remove the device from the label and disconnect it.

2.1.2 Security Guard Monitoring System

The patrol system helps companies and clients monitor their guards in several daily tasks, such as building, asset and equipment protection. The system proves that the guard has been sent from a specific checkpoint within a predetermined time and has sent an event report describing the situation or the risk of its occurrence.^[7]

The security patrol system ensures high reliability and security levels. It can raise awareness of the incident and provide documentation. As a result, security companies are more efficient with upgraded and improved security, inadvertently enhance the reliability of customers and partners.

The software solution automates tasks and increases productivity. Therefore, the world's most secure company specializing in patrol navigation software using software security guard monitoring system to complete the inspection mission. By using the monitoring system, the company can record the date and time of the event location, take pictures of any suspicious behavior, record any details and inform all persons associated with it.

The guard tour monitoring system provides historical data on all tours. Information about the tour is recorded and reported in real time. Real-time and accurate data provides no doubt about any aspects of events and security activities patrols.

NFC-enabled security monitoring systems that can be found on the market, such as Incentive Lynx Security, inViu NFC-tracker, and NFC Patrol. Basically, an NFC tag is mounted on a checkpoint in a building to represent a location. By scanning a tag using an NFC-enabled phone with a dedicated application to retrieve the tag UID and then sending this UID to the application server over the Internet in real time. A security guard can prove that he is present at the checkpoint at the time the tag is tapped.^[8] At the time tapping (hereafter we call it a tag event), UID tags are collected and sent to the server in real time via the Internet. Some systems, such as Incentive Lynx Security, also uses the Global Positioning System (GPS) in the phone to detect the position of the security guards. Although these solutions add more precision to the monitoring, it does not always work since the GPS signal is not available in the buildings.

the status of patrol after the security guard completed all the checkpoints. Therefore, this antique system does not provide real time arrival checking and does not create automatic reports. Besides that, the paper tape inside the box need to be changed everytime after the patrol is done.

1. Advantages of Watchman's Clock System
2. Least expensive type of system
3. Simple and easy to use

Disadvantages of Watchman's Clock System

1. Limited number of key can be used in system (maximum 30)
2. Watchman's clock is bulky to carry around
3. Need to spend a lot of paper tape
4. No ability to generate weekly, monthly or yearly reports
5. Require high maintenance fee
6. Does not provide real-time reporting of guard's activity

2.2.2 RFID-based Data Logger

RFID-based data logger is a system that is most commonly used by the security guard at the moment. Even though it has same functionality with the watchman's clock but it uses electronic rather than mechanical components. Since it is using electronic component, the patrolling records will be in the term of digital form. Therefore, the size of the data is smaller compared to watchclock's paper tape. ^[9]



Figure 2.2 RFID-based data logger components