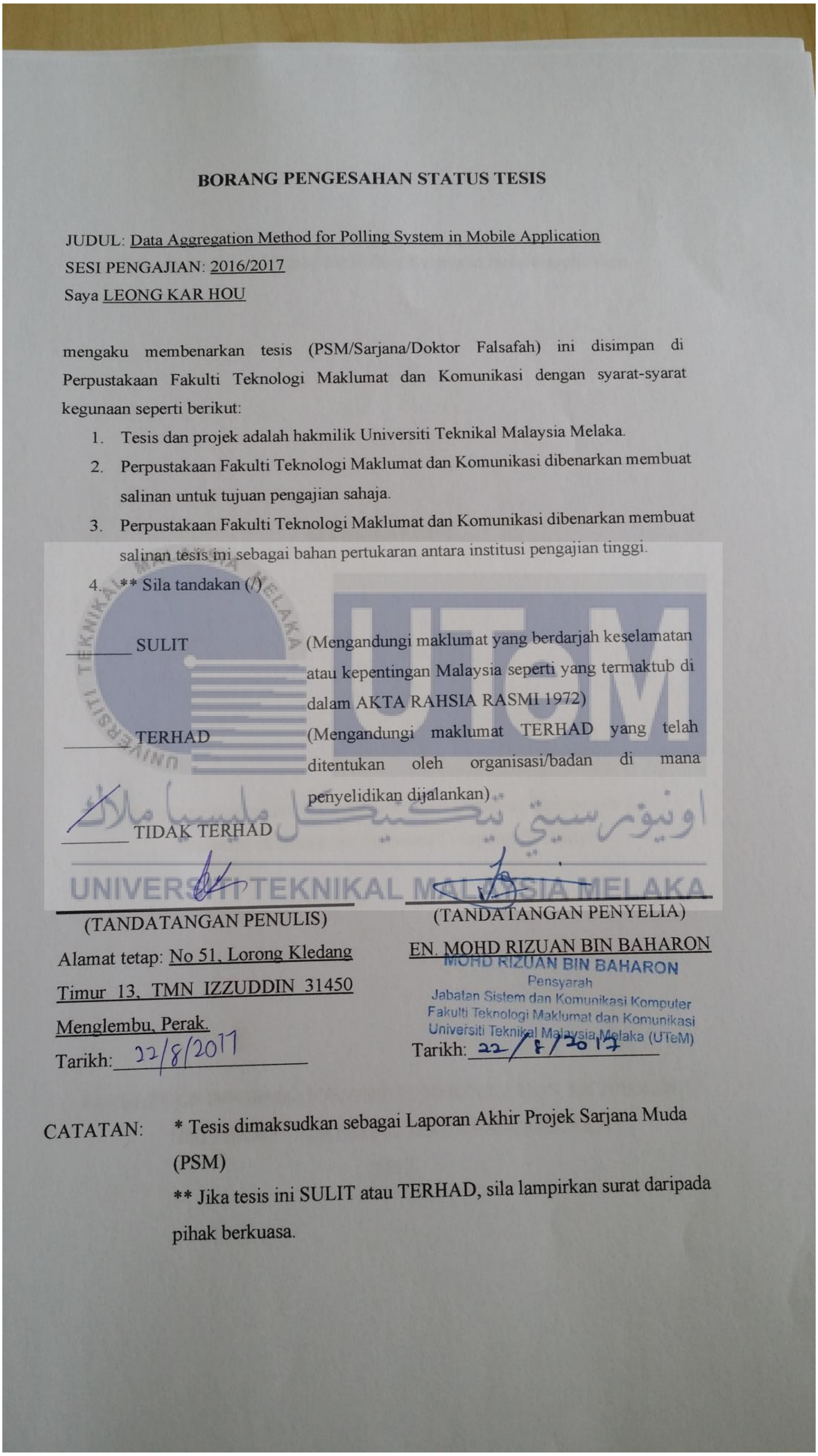
Data Aggregation Method for Polling System in mobile application

LEONG KAR HOU

UNIVERSITI TEKNIKAL MALAYSIA MELAKA



BORANG PENGESAHAN STATUS TESIS

JUDUL: Data Aggregation Method for Polling System in Mobile Application

SESI PENGAJIAN: 2016/2017

Saya LEONG KAR HOU

mengaku membenarkan tesis (PSM/Sarjana/Doktor Falsafah) ini disimpan di Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dengan syarat-syarat kegunaan seperti berikut:

1. Tesis dan projek adalah hakmilik Universiti Teknikal Malaysia Melaka.
2. Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dibenarkan membuat salinan untuk tujuan pengajian sahaja.
3. Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dibenarkan membuat salinan tesis 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]

(TANDATANGAN PENULIS)

Alamat tetap: No 51, Lorong Kledang Timur 13, TMN IZZUDDIN 31450 Menglembu, Perak.

Tarikh: 22/8/2017

(TANDATANGAN PENYELIA)

EN. MOHD RIZUAN BIN BAHARON

MOHD RIZUAN BIN BAHARON
Pensyarah
Jabatan Sistem dan Komunikasi Komputer
Fakulti Teknologi Maklumat dan Komunikasi
Universiti Teknikal Malaysia Melaka (UTeM)

Tarikh: 22/8/2017

CATATAN: * Tesis dimaksudkan sebagai Laporan Akhir Projek Sarjana Muda (PSM)

** Jika tesis ini SULIT atau TERHAD, sila lampirkan surat daripada pihak berkuasa.

Data Aggregation Method for Polling System in mobile application

LEONG KAR HOU

This report is submitted in partial fulfillment of the requirements for the

Bachelor of Computer Science (Computer Security)

FACULTY OF INFORMATION AND COMMUNICATION TECHNOLOGY

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

2017

DECLARATION

I hereby declare that this project report entitled

DATA AGGREGATION METHOD FOR POLLING SYSTEM IN MOBILE APPLICATION

is written by me and is my own effort and that no part has been plagiarized without citations.

STUDENT : ______________________ Date: 22/8/2017

(LEONG KAR HOU)

I hereby declare that I have read this project report and found this project report is sufficient in term of scope and quality for the award of Bachelor of Computer Science (Computer Security) With Honours.

SUPERVISOR: ______________________ Date: 22/8/2017

(MR. MOHD RIZUAN BIN BAHARON)

MOHD RIZUAN BIN BAHARON
Pensyarah
Jabatan Sistem dan Komunikasi Komputer
Fakulti Teknologi Maklumat dan Komunikasi
Universiti Teknikal Malaysia Melaka (UTeM)

DEDICATION

I would like to special thanks to my project supervisor, Mr. Mohd Rizuan Bin Baharon who supported and provided many suggestion for my project development. He mentally and physically gave me a guidance to complete this project successfully. Furthermore, I also want to thanks to my parents and my friends who are willing to help me and gave me opinion whenever I face problem in the project.

ACKNOWLEDGEMENTS

I would like to express my gratitude to my supervisor of this project, Mr. Mohd Rizuan Bin Baharon who always guide me with patience and support, lead me from the project development beginning to complete it and constructive comments on the development of the project. He also providing me with useful materials related to the project that help me to done this project smoothly. This is my pleasure to work with my supervisor.

I am hugely indebted to my friend who are willing to spend their time to reply to my message and to be as a tester in implementing and testing the system. Their precious kind advices help me to finish my final year project on time.

ABSTRACT

Polling system is a complex system that provides a voting and election management service in a digital platform. This system allows an election administrator to manage election information and results systematically and efficiently. Even though this polling system performs better than the traditional paper based approach, most of the online polling system are not enclose their voter response in the election result. Thus, this system aim is to protect and enclose the voter privacy during election result transmission. This system implements data aggregation technique to mix all the voter response so as to prevent the exposure of the voter privacy. Furthermore, this system implements homomorphic encryption scheme to allow the voter response processing in encrypted form without the need for decryption. For the system development, this system is divided into two platforms such that the one is for an administration that is web based application and the other is to provide voter election service in android platform. This system implements waterfall model, which also known as linear-sequential life cycle model for it methodology. This system can provide security feature to protect voter privacy in election such as the voter response. The system keeps the individual voter decision confidential and protected from public to achieve the privacy preservation.

ABSTRAK

Sistem undian adalah sistem yang kompleks yang menyediakan perkhidmatan mengundi dan pengurusan pilihan raya dalam platform digital. Sistem ini membolehkan pihak berkuasa pilihan raya untuk menguruskan maklumat pilihan dan hasil secara sistematik dan cekap. Walaupun sistem pengundian ini lebih baik daripada sistem tradisional yang berasaskan kertas, kebanyakan sistem pengundian dalam talian tidak melindungi tindak balas pengundi mereka dalam keputusan pilihan raya. Oleh itu, matlamat sistem ini adalah untuk melindungi dan menyulitkan privasi pemilih semasa penghantaran keputusan pilihan raya. Sistem ini melaksanakan teknik agregasi data untuk mencampur semua tindak balas pengundi untuk mengelakkan pendedahan privasi pengundi. Selain itu, sistem ini melaksanakan skema penyulitan homomorfik untuk membolehkan pemprosesan tindak balas pengundi dalam bentuk yang disulitkan tanpa memerlukan penyahsulitan. Untuk pembangunan sistem, sistem ini dibahagikan kepada dua platform, iaitu satu untuk pentadbiran yang merupakan aplikasi berasaskan web dan yang lain adalah untuk menyediakan perkhidmatan pemilih pengundi dalam platform android. Sistem ini menerapkan model air terjun, yang juga dikenali sebagai model kitaran hayat linear untuk metodologi. Sistem ini boleh menyediakan ciri keselamatan untuk melindungi privasi pemilih dalam pilihan raya seperti tindak balas pengundi. Sistem ini memastikan keputusan pengundi individu sulit dan dilindungi daripada orang ramai untuk mencapai pemeliharaan privasi.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ATTACHMENTS

CHAPTER I

INTRODUCTION

1.1 Introduction

Information security nowadays are main issue during the communication process between a digital devices to another digital device in digital world. Even a small wide area like restaurant also will to be target where adversary track or theft the victims' privacy for illegal purpose. Similar to polling system is also known as electoral system that consist a set of rules for candidate or parties election. Polling system are contain a lot of the privacy information like voter's vote privacy. The privacy election data may cause threaten for the voter if his/her voting choice had expose to opposite candidate. Since that a Polling System Mobile Application is proposed to develop using the data aggregation method in data handling and cryptography technique for protect the confidential of data transmitted.

This system are plan to make a solution for cover the limitation of the current polling system. Data aggregation method are used to make the voter's privacy in unknowing condition and addition to enhance the confidential and integrity level during the communication between transmission process we have implemented an asymmetric cryptography system which is the public key encryption scheme and also homomorphic encryption scheme in data processing.

Aim to protection on polling system’s data transmission, this polling system had design a three stage network structure consist of the main server, voting collector in local area, and mobile platform for voter. There are using data aggregation concept to collect a group of vote before process result of voting. The voter will sign in into the mobile application for access to get the election list and then make a selection of candidate from the election in first stage of mobile platform. At second stage, the voting collector act as a collector to store all the vote in encrypted form and act as aggregator to total up all the vote collected in encrypted form before submit to the main server. The main server are the final station for manage the election and candidate in addition also to decrypt the result of the election submitted by collector at the third stage.

Once the voter sign in into their mobile application to voting, the main server will authenticate whether voter are in list or not and if authenticated successfully it will implement the public key cryptography scheme used a pair of key in data transmission. There are generate a public key and a private key. The key are generate using the 1024bits big integer with a set of parameter which is *P*, *Q*, *R*, and *S*. The public key will send to voter at the same time while he/she request to sign in mobile application whereas the private key will hold by the main server for decrypt the final result after received the cipher text form result. The public key will used to encrypt the selection of the voter when voter submit their vote to collector.

While the homomorphic encryption is implant in the vote processing at second stage. This encryption scheme is provide a feature that able to carry out data computation even the data are encrypted form. It allow the aggregator in second stage to do summation for the vote’s result in unreadable form without decrypt the data. Homomorphic encryption method able to decrypt the data even through the data are already processing. This technique able to provide a scheme that to protect the privacy of the target without exposure even the privacy need some processing during reach the final destination.

1.2 **Problem Statement**

Time consuming issue during the voting event running. Most of the polling event are using the traditional polling system which is use the collector box at a voting hall to allow voter to put their vote into the box manually and they need to queue to voting. The voting hall may not enough to available a large number of the voter to going the voting event at one time. Thus the voters may spend their time to voting, this may make inconvenient for them and also not efficient to process large number of vote to get the final result.

High resource usage are the limitation of the current polling system. Even some of the current polling system had improvement by using the digital device to provide a platform for voter. But there still need voter to reach the polling hall and voting. The place resource and the human resource are consuming to make sure the event running smooth. Like a lot of committee needed to manage the event and computing the vote result if polling event are using paper based voting.

The confidential issue for current polling system such as all the voting information are in plaint text form may threat the privacy of the voter themselves. The voting privacy may exposure to public and this may cause unfair for the voting competition. The voter's privacy are not protected and they might voting without their will. The voting process without confidential will attract and allow the adversary to theft the privacy of the voter for malicious purpose.

1.3 Project Question

Table 1.1: Summary of Project Question

No.	Project Question
1.	How a mobile platform polling system provide an efficient way to handling the polling event?

2.	How the data aggregation method be used to keep secret of the voter's privacy during the voting event?
3.	How can the homomorphic encryption and public key encryption scheme work together to protect the confidential and integrity of data and process the data without any distortion in cipher text form.

1.4 Project Objective

Table 1.2: Summary of Project Objective

No.	Project Objective
1.	To provide the voting's platform on mobile application and auto-count function to process the vote to increase the efficiency.
2.	To design an online system with feature voting to overcome the availability of the voting station.
3.	To improve and secure the vote detail in polling system by using the data aggregation method to processing user's vote to keep confidential of user privacy.
4.	To protect and prevent adversary from tampering and disclose the voter's privacy in polling event for malicious activities.

1.5 Project Scope

1. Data Transfer

- Vote information protection by using cryptography method.
- System backend will generate keys within public key encryption scheme.
- Public key and private key will publishes for secure data transferring.

- Public key will send to voter device to encrypt vote information.
- Private Key will use to decrypt the result of vote.

2. User / polling application in mobile platform

- User act as voter for voting.
- User will sign in into the mobile application to voting
- User will access the application and enter their vote.
- Application will receive public key from system server to encrypt the vote of user.
- The encrypted vote will send to data aggregator.

3. Data Aggregator

- Collect all vote information from voter in a specific area.
- It will processes all the encrypted data before sending to system server.
- Aggregator will total up the vote result in encrypted form and submit the final result in cipher text form to the system server.

4. System Server

- System Application

i. Voter management module

- Voter name list file import and auto-registration function
- Name list display function

ii. Candidate management module

- Registration of candidate
- Update and View candidate information

iii. Polling event management module

- New event create and candidate assigning
- Event modification and result display function

- Key Provider

i. Generate both public key and private key for polling system use

ii. Decryption process for result of vote.

1.6 Project Contribution

Table 1.3: Summary of Project Contribution

No.	Project Contribution
1.	Provided an online mobile platform to focus on convenient of voter in polling event.
2.	Polling system provide automat feature to handle the voting's data as auto-counting the vote result for each event.
3.	Polling system enclose the vote information using data aggregation scheme and homomorphic encryption scheme in data processing to ensure that voting data are always confidential.
4.	This system provided a public key encryption method to protect the voting data confidential and integrity to avoid the man in middle attack while data transferring.

1.7 Thesis Organization

The summary of each chapter are declared in this part of the report. Each chapter content summary are presented in this section included the introduction, literature review, project methodology, analysis and design, implementation of the system, system testing and conclusion

Chapter 1: Introduction

The requirement of the system development is identified in this chapter. This chapter will discuss about the current issue related to the system and solution purpose to implement in these system. And also the difference of current system and proposed system to overcome the problem and limitation will be stated.

Chapter 2: Literature Review

In part of the literature review are discuss about the previous similar project or research that which technique and method had been used. In addition, the contribution of previous related project will stated and act as reference for the improvement of the proposed project. This chapter also will discuss the limitation discover from the others related research for support current propose project need to develop and implement discover solution.

Chapter 3: Project Methodology

Project methodology is act as a rule or guideline that to guide the process to carry out the project development. It is defined each phase of the project development and describe task and activities of each phase that need to achieve which related to the project.

Chapter 4: Analysis and Design

The result of problem analysis will be declared and find out the solution in this chapter. The project scope will design in the section to fulfil the requirement for this project.