

Mobile Voting Application for Campus Election

Nugenthiran Muniandy¹, Dr Feresa Mohd Foozy^{1*}

¹Faculty of Computer Science and Information Technology,
Universiti Tun Hussein Onn Malaysia, Parit Raja, Batu Pahat, 86400, MALAYSIA

*Corresponding Author Designation

DOI: <https://doi.org/10.30880/aitcs.2023.04.01.016>

Received 16 January 2023; Accepted 13 June 2023; Available online 30 June 2023

Abstract: Campus election is one of the organised procedure elections that choose a student as one of the authorities in student council. Most of the institutes in past years performed the voting system using paper ballot system, which will take time to get the result and have the possibility to misplace the voting paper which lacks secure mechanisms. Apart from that, some universities use the electronic machine to vote for student affairs election. So as a solution the development of online platforms now acts as a base to student voting methodology. The online voting application is built using object-oriented analysis and design methodology which have requirement phase, design phase, implementation phase, verification phase and maintenance phase. The purpose to using online platforms is to reduce the workload and also to organise a stable election without any error. Apart from that, online elections can be secured with security features to prevent the confidentiality and integrity of the votes by applying multi-factor authentication and email verification. Mobile voting application is latest and secure technology to begin with if there are security mechanisms like MFA token and email verification. Full release APK application file will be tested by the (MMP) UTHM students. So, they can verify the functionality of the campus mobile voting application.

Keywords: Mobile Voting, Secure Mechanism, Voting

1. Introduction

Voting is an expression of one's views in response to a poll specially to exercise a political franchise presented by Merriam Webster (1828). Voting is also the fundamental right in the democracy of every country. Government is part of the democracy of the country. Through voting, the public of the country will handle the whole country. At the same time, not only governments of a country in some of the institutions or colleges also organised an election and apply a voting process to decide their student head and some other assistants. The most common method used in elections is voting based on paper. The paper ballots are used and the voters cast their vote physically. The counting mechanism in these elections is manual. The voter's intent is estimated from a physical ballot. The results are tabulated manually after the interpretation and reading of physical ballots. But some countries have become more

advanced and use the Electronic Voting Machine (EVM). Electronic Voting Machine (EVM) is an electronic device that is used to cast votes. This machine receives votes from voters, stores those votes and after completion of voting displays the candidate's name and respected candidate got how many marks.

Apart from that, many universities and also higher education institutions across the nation organised an election to select their respective head of student union. Student Union is a tokenism of student participation in school governance presented by Yan Wing Leung (2017). As the base of election process voting system conduct to identify which candidate is suitable for that position. Rapid technologies lead many universities and polytechnic students to use online platforms to cast their vote. The online election platform is a system where candidates name and picture appear on an online system and students have to vote through electronic devices like smartphones and laptops.

Universiti Tun Hussein Onn Malaysia (UTHM) also conducts online voting where students have to vote for their favourite candidate through Sistem Maklumat Aplikasi Pelajar (SMAP) platform. SMAP is not a standalone system. There are a lot of functions in that system. So, the processing time takes longer than expected. Apart from that, the SMAP system only has a login system as their security feature. But at the login feature also the username must be out matric number which can easily be identified by others. So, the security level is low. At the same time, students usually share their system password with their friends. This is probably because friends help to mark the attendance for them. So, the integrity of votes can't be secure.

So, to ease the voting process of student election a mobile application proposed to address the problem mentioned in Universiti Tun Hussein Onn Malaysia (UTHM). A mobile application with a Multi-Factor Authentication (MFA) is highly required, which can ensure the voting requirements in terms of uniqueness, fairness, privacy, and accuracy. First of all, students have to register their account, and perform some security features like multi-factor authentication and email verification to verify student identification, then choose the candidate and vote. If the student is eligible for voting, then the vote is accepted, if not the user cannot vote. The following are the objectives of this project:

1. To design a mobile voting application for campus election.
2. To develop the mobile voting application with multi-factor authentication and email verification.
3. To test the functionality of the mobile application for campus election.

2. LITERATURE REVIEW

2.1 Introduction to the system

Voting is one of the most important aspects of democracy and is essential to any society that operates on agreement. The use of mobile voting (m-voting) to allow voters to quickly and conveniently cast their ballots using the most widely used method of communication, a mobile device. The term "mobile voting" (or "m-voting") refers to a secure mobile application that simplifies the voting process for voters by allowing them to participate in elections using only a mobile device with an internet connection. The Literature review states the observation about problem statements, case study and the technology that was used in this project.

2.2 Background of Case Study

Student Union in universities is a tradition that has been followed from long ago. Every student has rights to vote for their selective candidate. But the method to vote is different from time to time, it's because of the technology evolution. The system or method used in Universiti Tun Hussein Onn Malaysia is SMAP. SMAP is a web application system for students to be aware about their academic status. As Conallen in 2018 says, "One of the most significant advantages of a web application is its deployment". That means a web application runs on a web server, unlike computer-based software programs that are run locally on the operating system of the device. Web applications are accessed by the user through a web browser with an active network connection. There are some other functions as

well, one of which is voting for the student union election. There is only a login credential security feature in the SMAP system.

The voting procedure in the SMAP system is easy and simple. Students have to log into their SMAP account and vote for their favourite candidates. There is only a login credential security feature to protect the confidentiality and integrity of the votes.

2.3 Existing Registration method for voting system

Paper ballot and electronic voting systems are still using manual registration. Manual registration is to register attendees for the event when they show up at the door or send in a paper registration form you can accommodate both, say by Paolo Contiero 2008. But for the online voting system there should be user registration by the institution itself. Figure 2.1 and figure 2.2 shows the SMAP registration in UTHM.

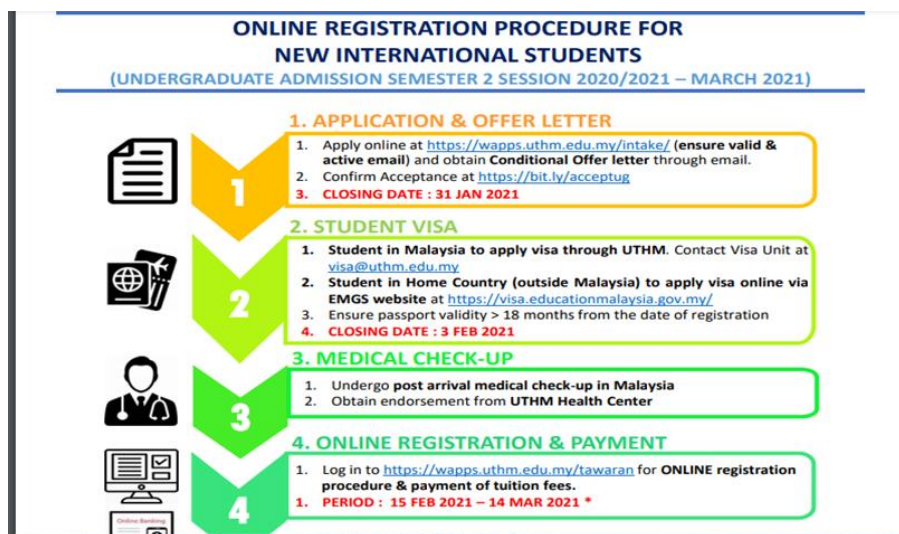


Figure 1: UTHM SMAP registration

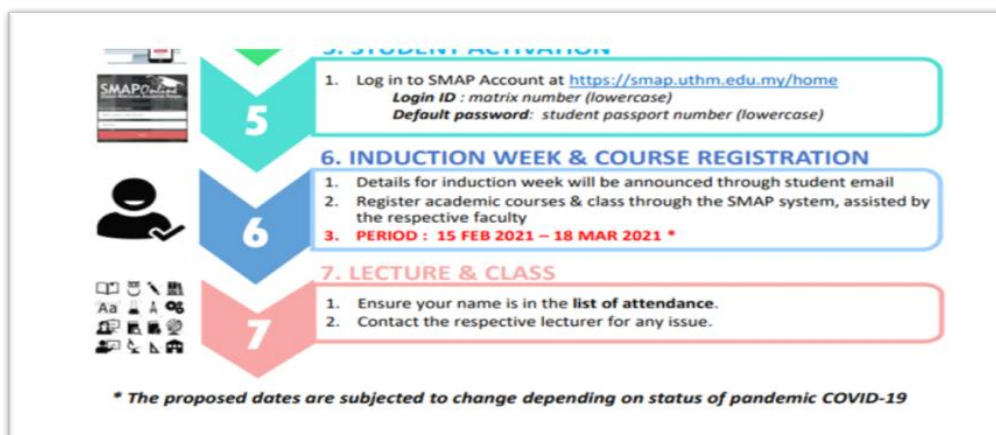


Figure 2: UTHM SMAP registration

2.3.1 Existing Login method of voting system

User authentication is a security process that covers all of the human-to-computer interactions that require the user to register and log in (Killoran, 2020). Apart from, paper ballot and electronic voting system, online SMAP voting system using login credential method to protect the confidentiality of students. The common ways of authentication are through passwords which is knowledge-based security that are used to restrict access to a number of systems (Shan et al., 2019) and SMAP platforms are still using the traditional method of authentication.

2.4 Study of existing related system

There are more ways for a person to cast their votes, but the universities just use some of the system. There are three existing systems that are studied and analysed to get more information to develop the online voting mobile application. The existing system studied including Paper Ballot Voting, Electronic Voting Machine (EVM) and Online Voting System.

2.4.1 Existing Related system

The three existing systems are studied and compared to the features of the proposed system. This includes the modules contained in the online voting Mobile application. The comparison results are shown in Table 1.

Table 1: Comparison between existing system and proposed system

Features/System	Paper Ballot System (Aziah 2019)	Electronic Voting System (Balvin 2017)	Online Voting System (Suryavanshi, 2020)	Proposed Voting Mobile Application
System Type	Offline	Offline	Online	Online
Login Module	Not Available	Not Available	Available	Available
Registration Module	Not Available	Not Available	Available	Available
Email Verification	Not Available	Not Available	Not Available	Available
Technology	Not Present	Machine	Web based and mobile application	Android Mobile application
Database	Not Present	Not Present	Unknown	Firestore
Programming language	Not Present	Not Present	Unknown	Java
Security feature	Not Present	Not Present	Login Credential	Login Credential, 2 factor-authentication.

By comparing all four systems, there are some advantages and also some disadvantages among all the systems. But in this pandemic situation online based voting systems is more convenient to all students. Thus, an online voting mobile application is the best solution to help students to cast their vote. Compared to the online voting system, mobile applications are more secure and reliable to the students.

2.5 Multi-Factor Authentication (MFA) and reCAPTCHA

Two Factor-Authentication or Multi-Factor Authentication (MFA) method that requires the user to provide two or more verification factors to gain access to a resource. A strong Identity and Access Management (IAM) policy must include Multi-factor Authentication as a fundamental element. Because Multi-Factor Authentication demands one or more extra verification elements in addition to a username and password, which lessens the possibility of a successful cyberattack. The main advantage of MFA is that it will increase the security of a system by forcing users to provide identification other than a login and password. Although crucial, usernames and passwords can be stolen by other parties and are subject to brute force assaults. When required the usage of an MFA element, such as a physical hardware key or thumbprint, may be more confident that the system will be protected from cybercriminals.

MFA functions by requesting extra verification data. One-time passwords (OTP) are among the most typical MFA elements that users come across. OTPs are the four to eight-digit codes that you frequently get via email, SMS, or a mobile app. OTPs create a fresh code every so often or each time an authentication request is made. The seed value, which is given to the user when they initially register, and another factor which could just be an increasing counter or a time value, are used to construct the code. Knowledge based multi-factor authentication is used in this project. The database will generate a one-time password and send it to the user smartphone via SMS. Before the OTP generates the application requires reCAPTCHA verification. Google offers reCAPTCHA as a free service to assist safeguard websites against spam and abuse. A "CAPTCHA" is a Turing test to distinguish between humans and robots. It is simple for people to figure out but challenging for "bots" and other harmful software. By including reCAPTCHA on a website, it can prevent automated software from entering while facilitating user entry.

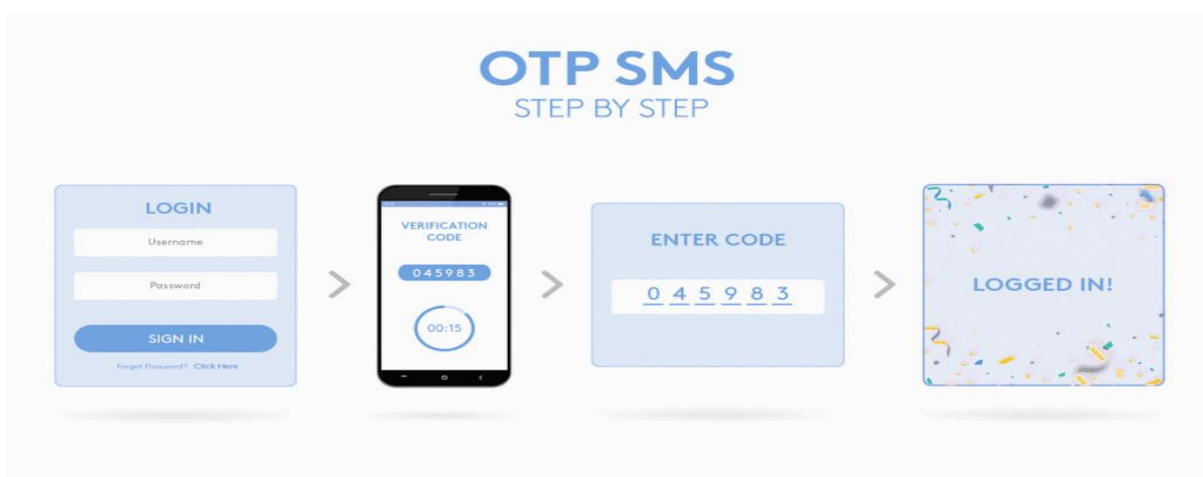


Figure 3: Function of OTP

3. Methodology

In this project, object-oriented analysis and design (OOAD) method (Mukherjee, 2016) is used as the project development methodology.

3.1 Object-Oriented Analysis and Design (OOAD)

In software development life cycles (SDLC), the system development of a system development process is divided into several phases. The phases present different activities in the development such as gathering requirements, planning, design, implementation, testing, deployment, and maintenance phases. In this development methodology, each phase is sequential and needs to be completed separately from one another. There will be some limitations or problems that will be faced in the testing and deployment phases, which are the decisions already made in the planning and design phases. The main difference between traditional approaches and object-oriented analysis and design is the way the problem is decomposed. In traditional approaches, decomposition of the problem is in the form of process-centric or data-centric, because the processes and data are too closely related. But the object-oriented analysis and design use Unified Modeling Language where the conditions are use case-driven, architecture-centric, and iterative with incremental.

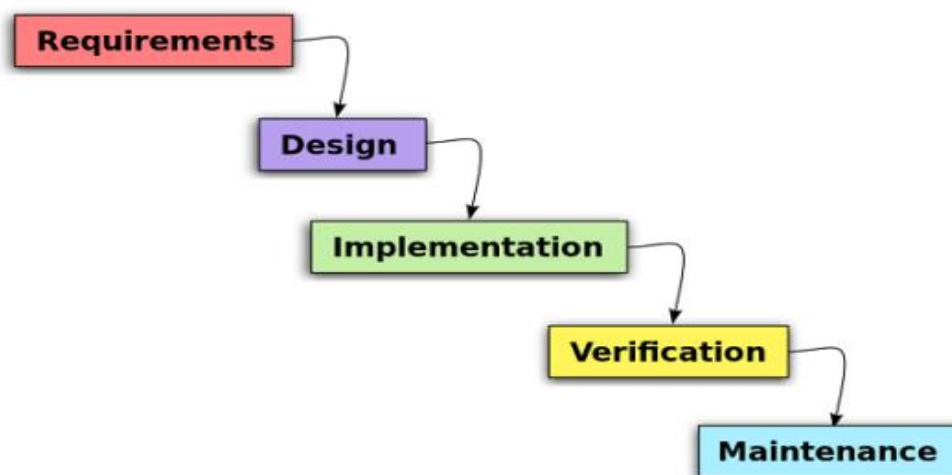


Figure 4: Object - Oriented Analysis and Design (OOAD)

3.1.1 Object-Oriented Requirement Phase

The object-oriented needs requirement phase is known as the planning phase. In this project, project planning is supported by various sources of relevant information. This project focuses on the problems in the voting system of student associations at the University. Much of the information about the online voting system is collected using Internet media such as Google, Google Scholar, YouTube and Journal Research Papers. Information findings were collected and analysed.

From the requirement analysis, this project idea was created. A lot of voting systems have been invented using web development, Arduino microprocessors and also mobile applications. The analysis phase gives the idea of using strong encryption inside the voting system. The result of the gathering requirement and analysis phase gives hint to propose a multi-factor authentication with email and reCAPTCHA verification.

3.1.2 Object-Oriented Design Phase

When the OOA phase is ended, the object-oriented design (OOD) process takes the concepts in theoretical and planned ideas from the OOA phase, then finds the way to design and implement these concepts and ideas via confirmed programming language and platform. Basically, the OOA is “What” and the OOD is “How” the concept is transformed into a complete project.

In this phase the mobile voting system developed which included the module for each function, multi-factor authentication and programming language used to for the flow of the system The proposed mobile application user interface includes 5 major modules. There is a login module, registration module, multi-factor authentication module (OTP), voting module and result module. The proposed mobile application will be developed using android studio. The programming language will be Java. The database to store the user data will be in Firebase.

3.1.3 Object-Oriented Implementation Phase

In object-oriented implementation, it can be separated into two parts. One is the front end and the other one is the backend. For backend side coding, the database created using Firebase platform and the backend language used for the project is Java programming language. For the security features multi-factor authentication, email and reCAPTCHA verification is added.

For front end side scripting, extensible markup language (XML) is used for the user interface design. Besides that, the Gradle function is used to enhance the design of the user interface. All the designs used in a simple way so that the user can easily attach with the system.

3.1.4 Object-Oriented Verification Phase

Verification means testing part. In the testing part, positive testing and negative testing will be carried out once the mobile voting system is developed completely. The positive test performed for the upgradation process for any valid reasons. For the negative test, it is very useful to identify the limitations of the system. Besides that, security features will be checked so that the tool is assured for the security features.

3.1.5 Object-Oriented Maintenance Phase

After this system is developed, a maintenance process is entered, it includes making videos tutorials about the system, documentation improvement, solving simple problems, documenting errors or bugs, recording requests for enhancement of the system.

3.2 System Development Workflow

There are a total of 5 phases from the Object-oriented analysis and design (OOAD). As shown in Table 3.1, each phase has its own assignment and output that need to be produced during the entire project development. Besides that, the output had been completed within the specific days that have been given.

Table 2: Software development activities and their task

Phase	Task	Output
Requirement / analysis	<ul style="list-style-type: none"> • Problem identified from the case study • Proposed the project • Determined the project schedule, activities and output • Identify software and programming language needed 	<ul style="list-style-type: none"> • Project proposal • Gantt chart • Framework of fingerprint module
Design	<ul style="list-style-type: none"> • User interface is designed • Database is designed • System with basic functionalities is designed. • All the module is designed 	<ul style="list-style-type: none"> • Flowchart diagram • UML diagram proposed • Prototype • Database
Implementation	<ul style="list-style-type: none"> • Mobile voting system is fully developed • All module is ready to use • MFA applied. 	<ul style="list-style-type: none"> • Full fledge mobile voting system present.
Verification / Testing	<ul style="list-style-type: none"> • Unit testing • Integration testing, acceptance testing was conducted 	<ul style="list-style-type: none"> • System user manual

Maintenance	<ul style="list-style-type: none"> • Improve or enhance the project • Mobile voting system with new features available.
-------------	---

4. Analysis and Design

4.1 Functional Requirement Analysis

A functional requirement defines what has been done by identifying the necessary activity, task or action that must be accomplished (Pohl, 2010). It describes the process of inputs transformation to the desired output for the user.

Table 3: Functional requirement of the proposed system.

No	Modules	Functionalities
1	Login module	<ul style="list-style-type: none"> • The application should allow the user to log in into the system using username and password. • The system will alert the user for invalid input. • The system should redirect the user to the respective dashboard once successful login.
2	Registration module	<ul style="list-style-type: none"> • The system allows new users to register before login. • The system shows if any empty field is found. • The system will show an error if the password didn't meet the criteria. • The user must use siswa email.
3	Email verification	<ul style="list-style-type: none"> • There will be a verification email send to user who register. • Sometimes the verification email will fall under the siswa email spam folder.
4	Multi-factor authentication and reCAPTCHA authentication	<ul style="list-style-type: none"> • The system will send an OTP number to the registered phone number. • Before the system processes the OTP number it will verify the BOT verification or reCAPTCHA Verification.
5	Voting module	<ul style="list-style-type: none"> • Before voting, user can view the candidate's profile.

		<ul style="list-style-type: none"> • After that, vote for the candidate.
6	Report Result	<ul style="list-style-type: none"> • Announce the winner of the election.

4.1.2 Non-Functional Requirement Analysis

Non-functional requirements specify the criteria that can be used to judge the operation of a system, rather than specific behaviours (Pohl, 2017).

Table 4: Non-functional requirement of proposed system

No	Requirement	Description
1	Performance	<ul style="list-style-type: none"> • The system should be able to be used at any time. • The email verification and OTP number should be functions to enhance the security feature.
2	Operation	<ul style="list-style-type: none"> • The system should be user friendly. • The system should be easily maintained and updated. • The system should work on smartphones.
3	Security	<ul style="list-style-type: none"> • User can only login into the system by entering their username and password. • Email verification is used to secure the integrity of the votes. • OTP function is applied to enhance the system confidentiality among the users.

4.1.3 Software Requirement Analysis

Software requirements analysis required to define what is the software needed to support the system.

Table 5: Software requirement specification

No	Type	Software	Functionality
1	Programming language	JAVA	Develop an environment for voting systems and compounds using the Java programming language.
2	Markup language	Extensible Markup Language (XML)	XML is designed to store and transport data.
3	Design tool	Android studio	Design the mobile voting application.

4	Database	Firebase	Design and build database.
---	----------	----------	----------------------------

4.1.4 User requirement Analysis

User requirements show what users require from the system in detail. In other words, user requirement presents user’s expectation about what the software will be able to do (functionality).

Table 6: User requirements of proposed system.

No	User requirement
1	All users should be able to input the user id and password for registration and login purpose respectively.
2	All users must input their siswa email to get email verification from the system.
3	Users phone number must be accurate because the system will send the OTP number to the given phone number.
4	When user clear all security features, user can vote for the candidates.

4.3 Use Case Diagram

As shown in the use case diagram below User (student) can register the application first. Users must register with name, password, email, matric number and phone number. After successful registration, the user will get a verification email in inbox or spam folder. After the user verifies, the email user can log in to the system. After the user successfully types in the user credential the system will redirect to the reCAPTCHA verification. After the system verifies, the reCAPTCHA user will get an OTP code via phone number. Then users need to key-in their OTP number into the system. Finally, users will get to view the candidate and vote for their favourite one. As for Admin, it can provide system maintenance. Admin also handle the database also the final result announcing.

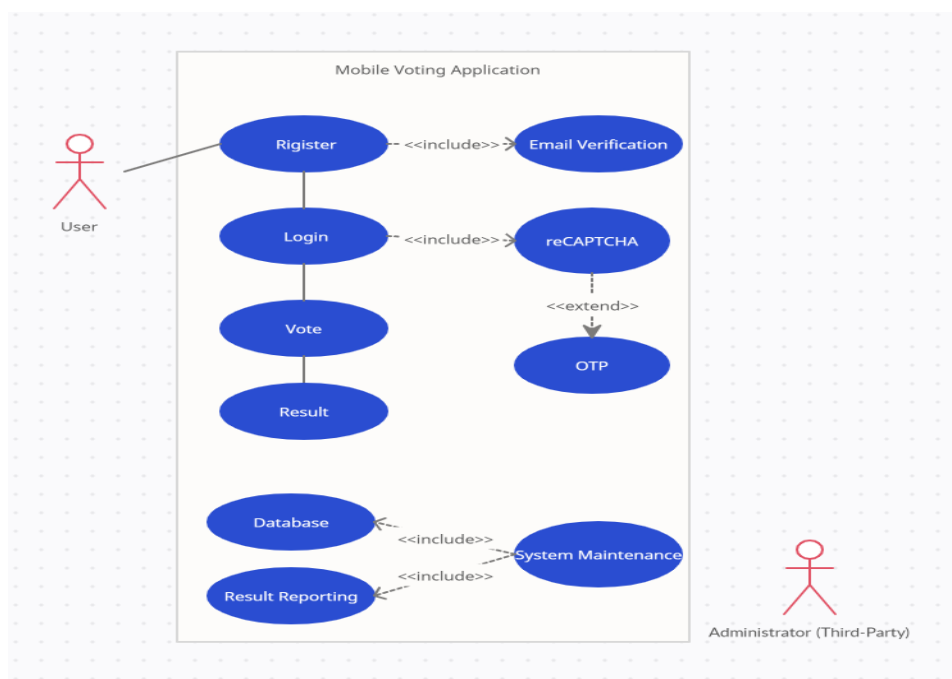


Figure 5: Use case diagram of proposed system.

4.4 Class Diagram

The class diagram describes the structure of a system by showing the system's classes, their attributes, operations (or methods), and the relationships among objects. Class diagram is basically a graphical representation of the static view of the system and represents different aspects of the application. Below figure shows the UML class diagram of the mobile voting application.

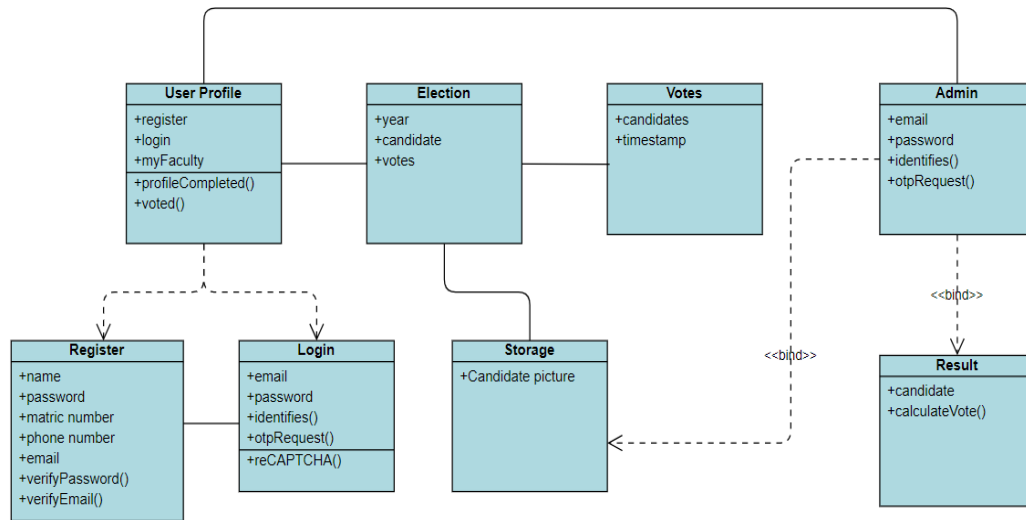


Figure 6: Class Diagram of Mobile Voting System.

4.5 Entity Relationship Diagram (ERD)

Entity Relationship Diagram (ERD) shows the relationship with the dataset within the mobile application. The first entity is a user profile which has data about the matric number, email, name, password and phone number. The email should be the primary key. The next entity is election which has data regarding candidate name and Votes. Apart from that, vote entities contain data about candidates details and timestamp of vote casting. The storage entity stores the candidate’s picture. Finally there will be a result set to shown the end function of the mobile voting application.

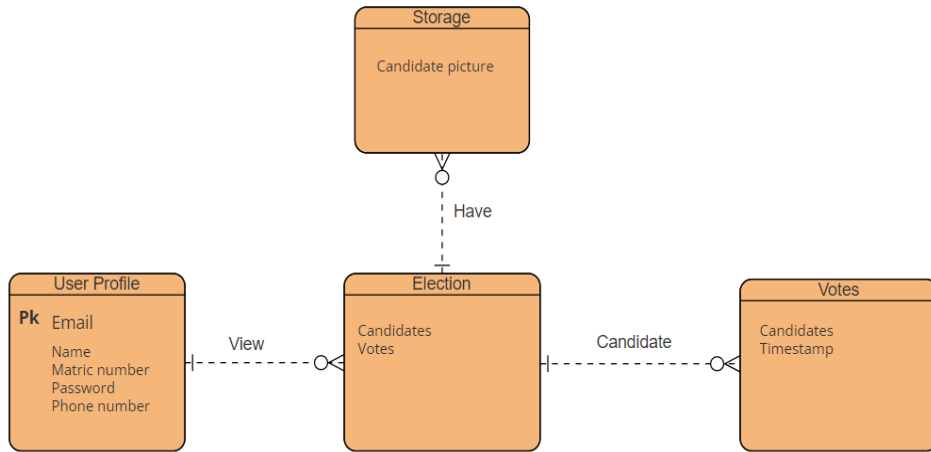


Figure 7: Entity Relationship Diagram (ERD) of the developed mobile application.

4.6 System Design: Flowchart

Flowchart is said to be important criteria in IT project development. The mobile voting application flowchart begins with a user register using name, password, matric number, email and also phone number. Then the user will get an email verification. User have to verify the email to login. After the user successfully key-in valid credentials and log in the system there will be reCAPTCHA verification and an OTP will be send out to the user phone number. After user key-in the OTP user can view the candidate and vote for them. After the voting process the system will show the highest voting candidates.

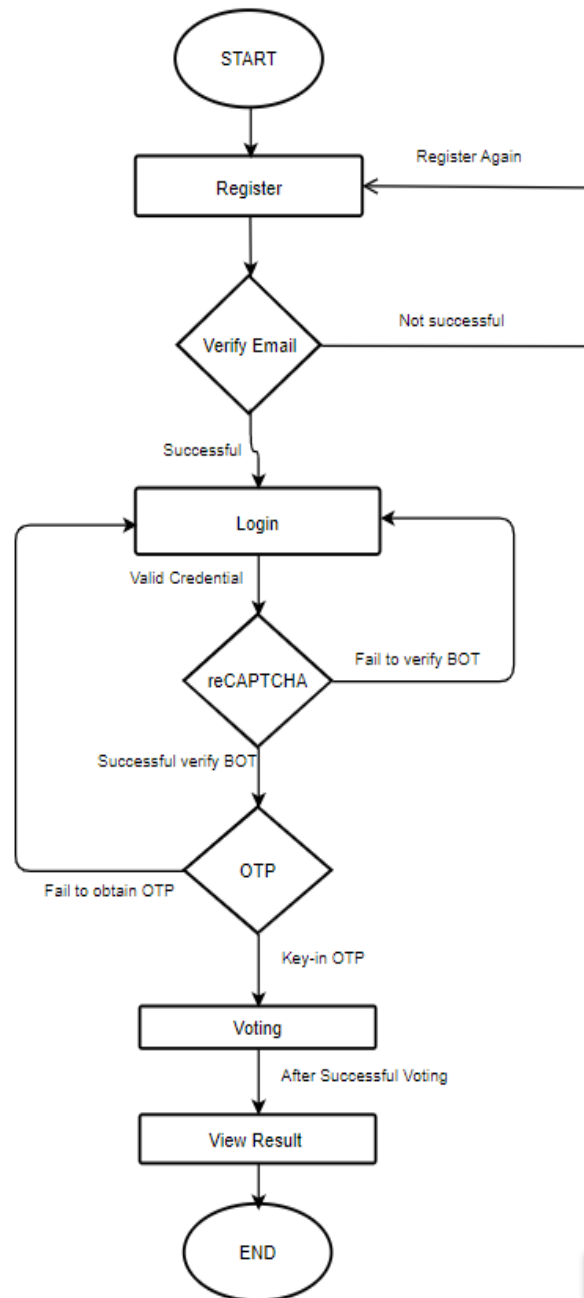


Figure 8: Flowchart USER of online voting application

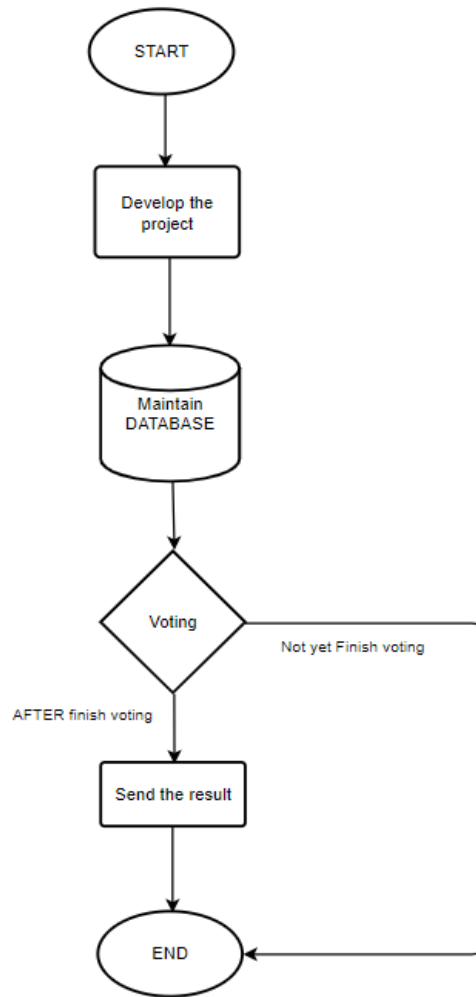


Figure 9: Flowchart ADMIN of online voting application

Figure above shows the flowchart for the ADMIN. Admin just maintains the database and also releases the voting result after the voting period has end.

4.7 Interface Design

Mobile voting application is made by android studio. When user login for the first time there will be a registration function to register an account

Register an Account

Full Name
Full name as matric card

Password

Must contain lowercase [a-z] Must contain UPPERCASE [A-Z]
Must contain numbers [0-9] Must contain symbols
Atleast 10 characters

Matric Number
e.g: CI123456

Siswa Email
Matric Number @siswa.uthm.edu.my


Phone Number
01XXXXXXXX

REGISTER **BACK**

Figure 10: Register module in mobile voting application

After user successfully registered, user needs to verify the email. So the email verification page is shown below.

Email Verification

 **UTHM**
Universiti Tun Hussein Onn Malaysia

Email verification link has been sent to
your registered email. Check your inbox.

Your Email

LOGOUT

Figure 11: Email verification module in mobile voting application

If the user already verifies the email, then the system will redirect to the login page.

Login

Siswa Email
xxxxxxxx@siswa.uthm.edu.my

Password


LOGIN REGISTER

BACK

Figure 12: Login module in mobile voting application.

After successfully key-in the login credential the system will ask for an OTP number.

Enroll for MFA

 **UTHM**
Universiti Tun Hussein Onn Malaysia

Enrolling Multi Factor Authentication is required to continue voting. OTP is sent to the registered phone number.

Your Phone Number

6 digit OTP

ENROLL

LOGOUT

Figure 13: The MFA module

After the face detection the system move to the voting page, where users have to choose the candidate.

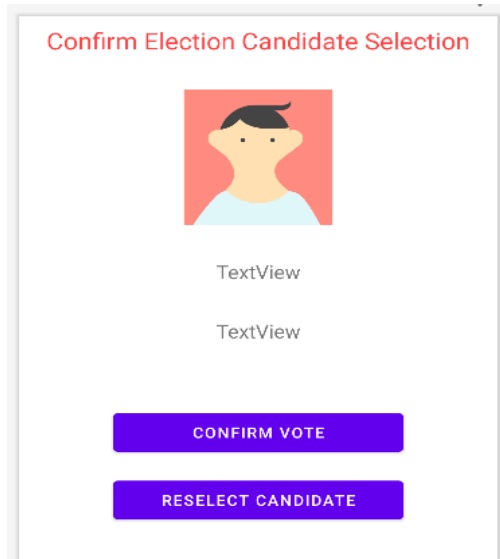


Figure 14: Voting module of online mobile voting application

5. Testing

5.1 Test Case

The functionality of the application is conducted in table below. The system will work according to its requirements and it will have some special criteria. Once all the criteria meet the requirement the voting process will be easy.

Table 7: Test case of the mobile campus election application

No	Test Case	Expected Output	Pass I
1.	Register a user must use email and also password that has specific criteria and login by email and password.	I. New user can register without a problem. II. The passwords also must be created using the given criteria. III. User must login into account by entering email and password.	Pass
2.	User can get their email verification via SISWA mail.	I. Users must get verification email from the firebase. II. Sometimes the email will considered as spam by SISWA mail.	Pass
3	The application will perform the reCAPTCHA verification then only	I. Application redirect to reCAPTCHA verification after login	

	can move to next module		Pass
4	Users will receive an OTP number through their phone number.	I.	OTP code will send through SMS to the user. Pass
5.	The candidate picture and the position must be clearly stated.	I.	The candidate's picture and their position are very clear and neat.
		II.	If you want to change the candidate in the middle of voting also can be changed. Pass
6.	Students can know their voting status and result.	I.	The application will be show the result to the student when applied to some changes in Voting status in Firebase. Pass

6. Conclusion

This project is all about creating a voting platform for UTHM students for their campus election. As per state in objective, full functional mobile voting application has been developed and tested. The Multi-Factor Authentication and email verification that has been added is working without any problem. Users that have test the mobile voting application is satisfy with the security features and also functionality of the application. This project can be upgraded in future because campus voting is one of the important events in every university including UTHM. Maybe in future this project can be upgraded using biometric features or can use the blockchain technology. Other than that, this project can be use as future research material for some students. As for as now MFA verification method that used in this project provide required confidentiality and integrity to the votes.

Acknowledgment

The authors would like to thank the Faculty of Computer Science and Information Technology, Universiti Tun Hussein Onn Malaysia for its support and encouragement throughout the process of conducting this study.

References

- [1] Mahajan, M., Pawar, Y., Wagh, M., Alai, S., & Biswas, P. (2018). M-Vote (Online Voting System).
- [2] Specter, M. A., Koppel, J., & Weitzner, D. (2020). The ballot is busted before the blockchain: A security analysis of voatz, the first internet voting application used in us federal elections. In *29th {USENIX} Security Symposium ({USENIX} Security 20)* (pp. 1535-1553).

- [3] Pawade, D., Sakhapara, A., Badgujar, A., Adepu, D., & Andrade, M. (2020). Secure online voting system using biometric and blockchain. In *Data Management, Analytics and Innovation* (pp. 93-110). Springer, Singapore.
- [4] Prasad, P. Y., & Malathi, S. (2019, March). M-Voting with Government Authentication System. In *International Conference on Emerging Current Trends in Computing and Expert Technology* (pp. 1244-1259). Springer, Cham.
- [5] Abirami, P., Jothi, R. A., & Palanisamy, V. (2018). A Survey on Biometric E-Voting System Using Retina. *International Journal of Pure and Applied Mathematics*, 118(7), 647-654.
- [6] Abayomi-Zannu, T. P., Odun-Ayo, I., Tatama, B. F., & Misra, S. (2020). Implementing a Mobile Voting System Utilizing Blockchain Technology and Two-Factor Authentication in Nigeria. In *Proceedings of First International Conference on Computing, Communications, and Cyber-Security (IC4S 2019)* (pp. 857-872). Springer, Singapore.
- [7] Qin, J., Tang, S., Han, C., & Guo, T. (2018, April). Partial fingerprint identification algorithm based on the modified generalized Hough transform on mobile device. In *Ninth International Conference on Graphic and Image Processing (ICGIP 2017)* (Vol. 10615, p. 106150Z). International Society for Optics and Photonics.
- [8] Ghosh, D., Banerjee, A., Chowdhuri, P. R. R., Gupta, A. S., Pal, B., & Khatun, S. (2018). FINGERPRINT BASED ELECTRONIC VOTING MACHINE: A REVIEW.
- [9] Abayomi-Zannu, T. P., Odun-Ayo, I. A., & Barka, T. F. (2019, December). A proposed mobile voting framework utilizing blockchain technology and multi-factor authentication. In *Journal of Physics: Conference Series* (Vol. 1378, No. 3, p. 032104). IOP Publishing.
- [10] Varshitha, K. S., & Shivanand, N. (2021). Android Mobile Based Voting System through Facial Recognition. *JNNCE Journal of Engineering & Management (JJEM)*, 4(2), 1.
- [11] Arora, S., & Bhatia, M. S. (2019). Fingerprint spoofing detection to improve customer security in mobile financial applications using deep learning. *Arabian journal for science and engineering*, 1-17.
- [12] Al-Habeeb, N. A. J., Goga, N., Ali, H. A., & Al-Gayar, S. M. S. (2020, October). A New M-voting System for COVID-19 Special Situation in Iraq. In *2020 International Conference on e-Health and Bioengineering (EHB)* (pp. 1-4). IEEE.
- [13] Abayomi-Zannu, T. P., Odun-Ayo, I. A., & Barka, T. F. (2019, December). A proposed mobile voting framework utilizing blockchain technology and multi-factor authentication. In *Journal of Physics: Conference Series* (Vol. 1378, No. 3, p. 032104). IOP Publishing.
- [14] Oke, B. A., Olaniyi, O. M., Aboaba, A. A., & Arulogun, O. T. (2017, October). Developing multifactor authentication technique for secure electronic voting system.
- [15] Banyal, R. K., Jain, P., & Jain, V. K. (2013, September). Multi-factor authentication framework for cloud computing. In *2013 Fifth International Conference on Computational Intelligence, Modelling and Simulation* (pp. 105-110). IEEE.