UNIVERSITY of RWANDA

Research and Postgraduate Studies (RPGS) Unit

Research Thesis Title: Secure Public Key Infrastructure Based System for Online Voting

Case study "Presidential Election in Rwanda"

By

AHIMANA Jean Marie Vianney

Reg_Number: 220020210

College of Science and Technology

School of Information and Communication Technology (SoICT)

Master of Science in Software Engineering.

A dissertation submitted in partial fulfilment of the requirements for the degree of Master of Science in software engineering.

August 2024

DECLARATION

I Jean Marie Vianney AHIMANA, hereby declare that to the best of my knowledge, this project entitled" Secure PKI Based System for online Voting" for the award of Masters degree in Software engineering is original and have never been presented or submitted for any academic award in university or institution as a whole or in part.

Jean Marie Vianney AHIMANA

Reg Nº 220020210

Date and signature……

CERTIFICATE

This is to certify that the project work entitled " Secure Public Key Infrastructure Based System for Online Voting" is a record of original work done by AHIMANA Jean Marie Vianney with Reg No: 220020210 in partial fulfillment of the requirement for the award masters of science in Software Engineering in College of Science and Technology, University of Rwanda during the academic year 2020-2022.

Signature……. Date ……../……../2024
Student name: AHIMANA Jean Marie Vianney

Supervisor **Postgraduate Cordinator School of ICT**

DR KABANDANA Innocent Dr NZANYWAYINGOMA Frederic

Signature:……. Signature:…….

TWAYIGIRA Joesph

Signature:…….

ACKNOWLEDGEMENT

I would like to express my deepest gratitude and appreciation to all those who have contributed to the successful completion of my final thesis titled "Secure PKI-Based System for Online Voting."

First and foremost, I am enormously grateful to my supervisors, Dr. KABANDANA Innocent and Joseph TWAYIGIRA for their exceptional guidance, unwavering support, and invaluable insights throughout the research process. Their expertise and mentorship have been instrumental in shaping this work and ensuring its quality.

I would also like to extend my heartfelt thanks to the lecturers at the University of Rwanda for their knowledge-sharing and dedication to education. Their passion for teaching and commitment to academic excellence have greatly enriched my learning experience.

To my classmates and friends, thank you for your support, encouragement, and collaborative spirit. The meaningful discussions, brainstorming sessions, and exchange of ideas have been invaluable in shaping the direction and depth of my research.

I am especially grateful to my beloved family for their unwavering love, encouragement, and sacrifices. Their constant belief in my abilities, patience, and understanding during the challenging times have been my greatest source of motivation and strength.

To everyone involved, I offer my heartfelt thanks for your contributions, support, and belief in my abilities. Without each of you, this achievement would not have been possible.

May God bless you abundantly.

ABSTRACT

This project describes the secure PKI based system for online Voting which refers to all those means which allow Voters to vote from locations other than the polling station assigned to their residence, either from abroad or from within the country. Online voting aims at increasing participation, lowering the costs of running elections and improving the accuracy and integrity of the results. Voter will use android phones, Tablet or using computer. System will use secure public key infrastructure (PKI) to secure every vote, the administrator will have privilege to register voters, candidates, party and Obsevers

The online voting system is designed using web architecture model, where there is a client, webserver and a database to store the records of the voters, candidates and the election result, which is realized in server and also runs on window based operating system. The final solution of this system implementation is to help in solving fraud problems, speed-up the voting process and the process of counting votes.

LIST OF ACRONYMS

PKI: public key Infrastructure

CA: Certification Authority

RA: Registry Authorities

CRL: Certificate Revocation List

NEC: National Electoral Commission

SDLC: Software development life cycle

IT: Information Technology

E-voting: Electronic Voting

NEC: National electoral commission

CPU: Central Processing Unit

RAM: Random Access Memory

CD-ROM: Compact Disc Read-Only Memory

DFD: Data Flow Diagram

UML: Unified Modeling Language

LIST OF FIGURES

Table of Contents

CHAPTER 1 INTRODUCTION

Democracy is very crucial in every society; one of the most important activities within a democracy is the election of representatives. Traditional Voting schemes have migrated from counting hands in early days to systems that include paper. Online voting systems provide some characteristic different from the traditional voting process that have various problems such as Time consuming, attempts of cheating of votes etc.

Online Voting System is a voting system by which any Voter can use his/her voting rights from abroad or anywhere in the country[1]. The detailed description of the functional and performance characteristics of online voting system will be provided. Candidates can vote from anywhere without visiting to voting stations, in highly secured way. That makes voting a fearless of violence and that increases the percentage number of voting.

In the last two decades, many researchers have focused their efforts towards the solution of the problem of online voting, or electronic voting, Voter authentication as well as controls of vote uniqueness are built around the notion of digital certificates and asymmetric cryptography. This is because most of the transactions carried out during an online voting must be non-repudiable in order to ensure the auditability and verifiability of the system.. Since all the voting protocols proposed use digital certificates and digital signatures, all implicitly rely on Public Key Infrastructures (PKI) for the managing digital certificates.

The public key infrastructure consists of three main entities.

1. **Certification Authority:**

The core of a Public Key Infrastructure (PKI), it is a trusted system that guarantees the connection between a public key and its owner through a certificate, whic h signs with its private key and makes it accessible to all users. Certificate management is completed with certificate revocation in the event of random events, such as compromise or loss of keys, that force the certificate to be revoked before its natural expiration date.

Certification authorities perform the following basic activities:

Issue end user certificates; cross-certify other CAs; Handle certificate revocation requests from end users and Registry Authorities (RA).

2.Registration authority:

Optional system component to which the CA can delegate certain functions, such as verifyin g user identity or providing proof of private key possession, to reduce access to the CA. Its a uthenticity is guaranteed with a certificate signed by the CA. All communications with the C A are digitally signed. RA performs the following operations: guarantees the identity of the e ntities that request the certification of their keys; identity verification

requiring entity to appear in person at the RA with a physical sign or through out-of-band mechanisms; verification of the user's possession of the private key; signing an electronic certificate request and sending it to the appropriate CA; requesting certificate revocations for user certificates issued by CAs that have accredited it.

3. Repository or Server:

system that stores digital certificates and Certificate Revocation Lists issued by the Certification Authority, and makes this information accessible to users for verifying the validity of certificates.

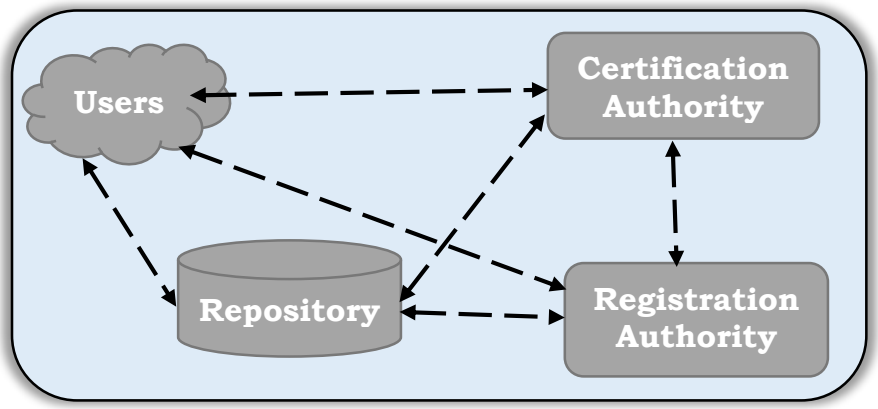

Figure 1 Main entities of PKI

I.1. Background of the study

Nowadays, information Technology (IT) is widely used rapidly becoming the common fixture of modern social and economic life. These technologies are opening opportunities to many people effectively. As the technology advances, Rwanda tries to be up to date and business has become more and more dependent on computer network data; the need for a correct and reliable system is obvious.

Enterprise, travel and hospitality industries, banks, education, training institutions, hospitals, Pharmacy, entertainment businesses and governments use large electronic scale web-based systems and some android applications to improve, enhance and /or extend their operations. Traditional legacy information and database systems are being progressively migrated to the web.

Rwanda use Paper-based Polling System, which have many problems including time consuming , errors during registering voters and candidates, every voter should be in voting station where he/she is registered etc. therefore many remain unregistered as well apart from low turnout of votes, but also difficult to make follow-up of election process, by looking at those problem (mentioned-above), there is no defendable reason to stick with paper polling system[4], secure Online voting system should be used to overcome those mentioned problems.

Even technology is best for make life easy and simplify the work there are many risks and dangers that can came from it especially for E-voting system such as The Security of Online Voting Systems that can be destroyed by the hackers, lack of transparency, …

Therefore, we need high level of security to overcome problems. This the reason why PKI technology is being chosen. As is one the basic essential element of data privacy, information integrity, authentication, and data access control.

I.2 Motivation of the study

My motivation for working on this project is due to the weakness with the paper based voting system currently used in Rwanda, those weakness includes: time consuming, counting the votes of every candidates takes a long time in the whole country, country invest more in electron commissions, buying all tools needed in election (papers, ink etc) but also transfer of election forms to the election site cost more. These weakness have inspired this thesis in which I was intend to propose an online voting scheme over a platform more secure than the paper based voting scheme[2] or a remote voting scheme over the internet like census[3] Citizen will vote from anywhere without visiting the voting stations, in highly secured way. That makes voting a fearless of violence and that increases the percentage of voting. And there might not be any other individual verifiability and accuracy of the tallying process due to human errors it is addressed using an electronic voting over a secure platform.

I.3 Problem description

In Rwanda election is done using paper-based voting system this has problems such as Time consuming, too much paper work, Counting the votes of every candidate, and some Less members were participating during election day but also it is expensive[6].

1.4. Study Objectives

1.4.1. General Objective

The aim of the study is to analyze the current election system and propose a secure online voting system with integrated PKI to enhance convenience for voters and facilitate quick reporting.

1.4.2. Specific Objectives

this study aims to achieve the following specific objectives:

2.Describe the existing voting system process.

3.Develop a prototype and design an online voting system with integrated PKI that ensures security, rapidity in tallying, casting votes, and displaying results.

4.Implement a server infrastructure capable of generating quick reports.

5.Ensure a high level of security and fraud prevention in the online voting system.

5.4. Scope of the study

The scope of a secure PKI voting system refers to the specific aspects and functionalities that are covered within the system. The following are key elements that fall within the scope of a secure PKI system for online voting

- **Key Generation and Management:**
  - ✓ Generation of cryptographic key pairs (public and private keys) for each voter.
  - ✓ Secure storage and management of keys, ensuring their confidentiality and integrity.
- **Authentication and Authorization:**
  - ✓ Verification of the authenticity and eligibility of voters through their public and private keys
  - ✓ Integration with voter registration databases to validate voter information.
- **Ballot Creation:**

  Creation of electronic ballots that accurately represent the choices available to voters.
- **Vote Tallying and Results:**
  - ✓ Secure and verifiable vote counting .
  - ✓ Aggregation of individual votes to determine the overall results.
  - ✓ Auditability and transparency measures to ensure the integrity of the tallying process.

- **Security and Privacy:**
  - ✓ Protection against various attacks, including tampering, impersonation, and ballot stuffing.
  - ✓ Safeguards for voter privacy, ensuring that votes cannot be linked back to individual voters.

5.5. Research organization

The study is organized into six chapters Introduction, Literature Review, Research Methodology, Systems Analysis and Design, Results and Analysis, and Conclusion and Recommendations. Each chapter serves a specific purpose.

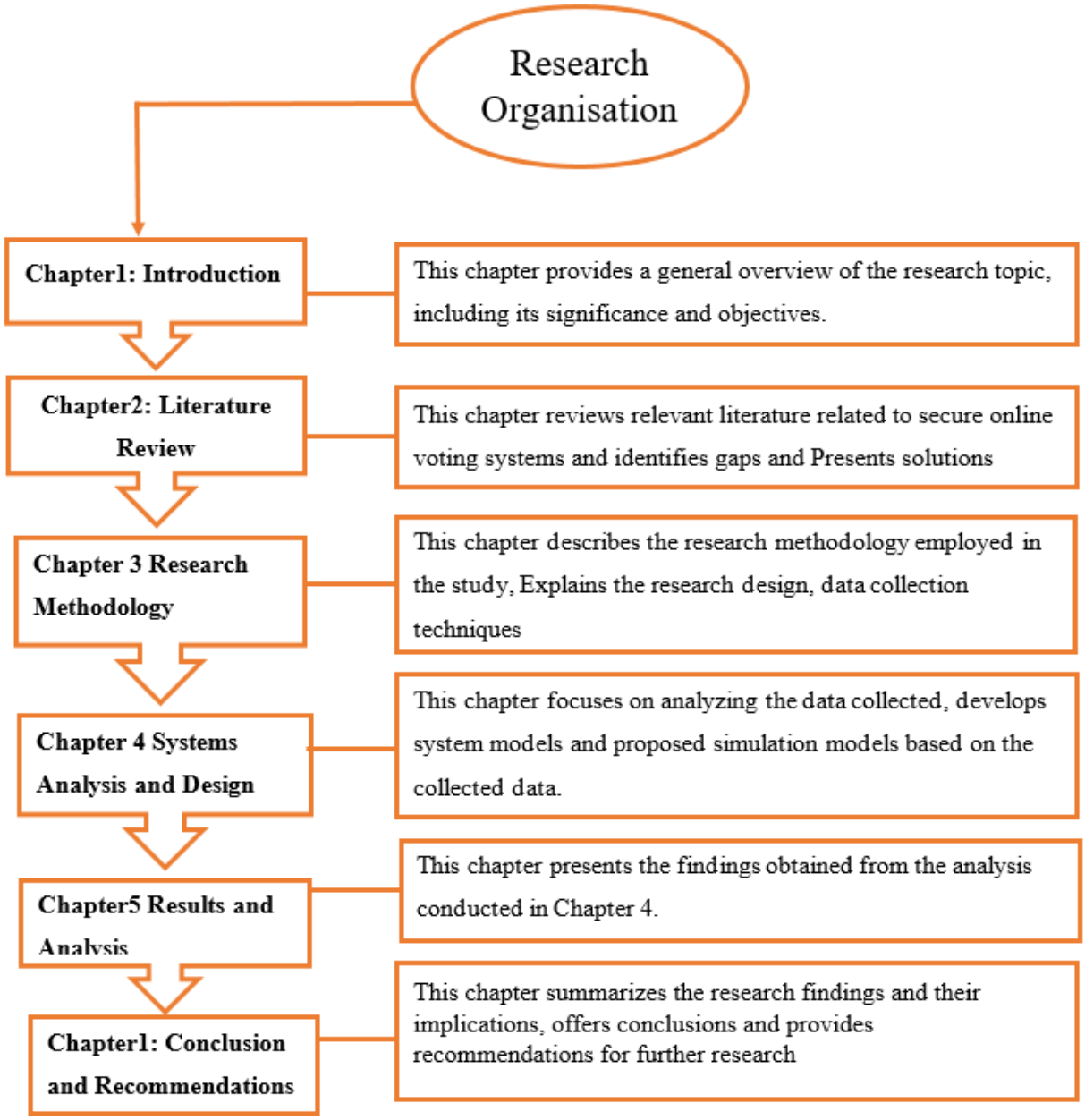

Figure 2 Research organization

CHAPTER 2. RELATED WORKS

2.1 Introduction

The literature review is a compilation of various authors' works in the field of online voting systems. The specific author(s) of the papers reviewed in this literature review may vary.

Online voting systems have gained significant attention in recent years due to their potential to revolutionize the democratic process. In this study, we will review some experiences of electronic voting that took place in various countries, presenting the techniques that have been used, the weaknesses encountered, and the solutions provided by a secure PKI system for online voting.

2.2 Online,Electronic Voting Systems or hybrid with paper based voting systems in Some Countries

Numerous countries have tried to replace traditional paper-based voting systems with advanced election techniques. These have included lever-arch machines, optical-scan machines, punch card voting, direct recording electronics (DREs), telephone, kiosk, online, and mobile voting systems. While electronic voting has been utilized or adopted in many countries, only some have proven their effectiveness [(Mpekoa & van Greunen, 2017)]. We will examine the experiences of a few nations with Online,Electronic Voting Systems or hybrid with paper based voting systems in Some Countries

2.1.1 The amercan presidential election in 2016

The United States presidential election took place on November 8, 2016. The electoral proces s involved voters in each state casting their ballots, with the most common techniques being v oting in person at polling stations and absentee/mail-in voting. There were concerns raised about potential voter fraud, as well as allegations of Russian interference through cyberattacks and social media manipulation. These issues sparked investigations and discussions about election security and integrity.

the 2016 election was a highly polarizing and consequential event that had a major impact on the political landscape in the United States. The voting techniques used, including in-person and absentee/mail-in ballots, were crucial to the democratic process despite the challenges faced.

2.2.2 Indian Electronic voting System

In 2004 indian election, about three hundred seventy million (370 millions) Indian voters (out of a total population of 675 million) cast their ballots using one million ele ctronic voting machines (EVMs) spread across 800,000 polling stations [(Chakrabarty & Haz ra , 2016)].These devices have been praised for their simple design, ease of use, and accuracy [(Kumar & Begum, 2012)]. However, concerns remain due to the lack of voter-verifiable paper trails, making it difficult to trace the outcomes [(Oo & Aung, 2014)]. Furthermore, software vulnerabilities have been identified, raising the risk of virus or hacking attacks [(Wolchok et al., 2010)].

2.2.3 Estonian Electronic voting System

In 2005, Estonia became the first country to allow its citizens to vote over the internet using their national ID cards. These cards, which serve as standard national identity documents, also function as smart cards that enable secure remote authentication and legally binding digital signatures [(Heiberg & Willemson, 2014)]. Between 2011 and 2019, the percentage of Estonian voters using the internet to cast their ballots steadily increased from 24% to 44% [(Toots & Idnurm, 2020)]. However, the system still faces vulnerabilities, particularly in terms of state-level attacks.

2.2.4 Norwegian Electronic voting System

In 2011 and 2013, Norway conducted trials of remote internet voting systems developed by the e-voting vendor Scytl for local and national elections. During the 2013 parliamentary election, more than 250,000 eligible voters had the opportunity to vote online [(Volkamer et al., 2011)]. However, in 2014, the internet voting initiative was discontinued due to security flaws, low voter turnout, and high costs [(Saglie & Segaard, 2016)].

2.2.4 Swiss federal election in 2022

The 2022 Swiss federal election was held on October 23, 2022 to elect all 200 members of the Federal Assembly, Switzerland's federal legislature. The main political parties contesting the

election were the Swiss People's Party (SVP/UDC), Social Democratic Party (SP/PS), Free Democratic Party (FDP/PLR), Christian Democratic People's Party (CVP/PDC), and Green Party (GPS/PES).

The election saw the Swiss People's Party maintain its position as the largest party, winning 54 seats. The Social Democrats came in second with 39 seats, followed by the Free Democrats with 37 seats. The Christian Democrats and Greens each won 26 and 28 seats respectively.

Swiss elections utilize a proportional representation system, with voters casting ballots for party lists rather than individual candidates. This helps ensure the federal legislature is representative of the electorate. Voters also had the option to vote early by mail or in-person on election day.

However, the 2022 election was not without its challenges. Concerns were raised about potential disinformation campaigns and foreign interference, which prompted increased efforts to secure the electoral process. There were also debates around issues like immigration, climate change, and the economy that polarized the electorate.

Table 1 Experiences of Online,Electronic Voting Systems or hybrid with paper based voting systems that took place in various countries The techniques used, the weaknesses encountered, and the solutions provided by a secure PKI system for online voting.

Country	Election Year	Voting System	Challenges Encountered	How Secure PKI System Using Public and Private Keys Helps Overcome Challenges
United States of Amerca (USA)	2016	Hybrid (Paper Ballots, Absentee/Mail-in, Online/Electronic Voting)	1.Concerns about the vulnerability of aging voting equipment to glitches or hacking 2. Allegations of foreign	1.Voters can use their private keys to digitally sign their ballots, ensuring the integrity and non-repudiation of their votes 2.Public keys can be used to verify the authenticity of the signed ballots, without

			interference through cyber-attacks and disinformation campaigns	revealing the voter's identity
India	2019	Hybrid (Paper-based Voting, Electronic Voting Machines)	1. Scaling electronic voting systems to a large and diverse population 2.Maintaining the integrity of the electoral process in the face of technological challenges	1.Public and private keys can be used to secure the transmission and storage of electronic votes, ensuring the integrity and non repudiation of the ballots 2.Voter-verified audit trails using public and private keys can improve transparency and build trust in the system
Estonia	2019, 2024	Hybrid (Secure ID Card with Digital Signature, Paper-based Voting at Polling Stations0)	1.Ensuring the integrity and verifiability of electronic votes 2.Maintaining voter privacy and preventing vote coercion	1.Voters can use their private keys to sign their ballots, ensuring the authenticity of their votes 2.Public keys can be used to verify the signatures without compromising the voter's privacy
Norway	2011-2013	Hybrid (Paper-based Voting at Polling Stations, Online Voting(Discontinued)	1.Concerns about the vulnerability of online voting systems to hacking and interference 2. Challenges in implementing a fully secure and	1.Public and private keys can be used to secure the transmission and storage of electronic votes, ensuring the integrity and non-repudiation of the ballots 2.Voter-verified audit trails using public and private keys can improve

			user-friendly e-voting solution	transparency and build trust in the system
Switzerland	2022	Hybrid (Paper-based Voting at Polling Stations, Secure Online Voting (mail-in)-)	1.Gaining public trust in the security and reliability of e-voting systems 2.Ensuring the secrecy of the ballot and preventing vote buying/coercion	1.Voters can use their private keys to digitally sign their ballots, which can then be verified using the corresponding public keys without revealing the voter's identity 2.The public key infrastructure can be used to authenticate voters and ensure the integrity of the voting process

CHAPTER 3. RESEARCH METHODOLOGY

3.1 Introduction

This chapter presents the research design, study population, sample size and sample selection, data collection methods, data collection tools, validity and reliability, data collection processes, data management and analysis, and measurement of variables, data structures used in studies for requirements determination, system analysis and design, and also system development, testing, and evaluation.[13]

3.1 Research Design

In Orodho (2003) and Ogula (2005), it is ascertained that research design is the scheme, structure, outline, plan or strategy of investigation used to give answers to the research questions.

3.2 Research Strategy

This project uses a case study strategy. A case study is a matter of investigation that will reveal an in-depth understanding of a "case" or bounded system, including an understanding of an event, activity, process, or personal number. (Creswell, 2002, p.61)

A case study is preferred because it gives the researcher an opportunity to analyze and understand the complex area. Case studies emphasize detailed contextual analysis of certain events or conditions and their relationships. This research is based on a case study at NEC Rwanda.

3.2 Target Population

Target Population refers to the entire group of individuals or subjects to whom researchers want to generalize their findings.

The target population often has different characteristics and is also known as the theoretical population. (Sekaran, 2010). In this study, the target audience includes voters and Rwandan Nation electoral commission(NEC).

3.3 Instruments of data collection

3.3.1 Interviews

According to D. S. Rodrigues [14], interviews are a data collection method that usually involves visiting individual respondents at their home or workplace .

During the interview process, the interviewer asks questions according to the interview schedule and records the respondents' answers. Interviews are useful because very specific data can be obtained in a very short period of time. The interview is also useful in giving an overview of people's thinking.

Interviews were used to interview the National Electoral Commission (NEC) in Rwanda and other Rwandan citizens about the process and challenges of the current paper voting system used in Rwanda.

3.3.2 Documentation

This is done by consulting relevant documents, specifically information from textbooks, websites, theses of other researchers and book reports.

This method verifies the information collected during the interview process.

3.4 System development methods

3.4.1. Software Development Life Cycle (SDLC)

SDLC is a framework that identifies the steps involved in software development at each stage. It includes a detailed plan for creating, deploying, and maintaining software.

SDLC defines the complete development cycle, i.e. all the tasks involved in planning, building, testing and deploying a software product.

3.4.2. SDLC Process

SDLC is a process that identifies the various steps involved in developing software to deliver a high-quality product. The SDLC steps cover the entire software life cycle, i.e. from creation to product retirement.

3.4.3. Objective of SDLC

The objective of SDLC is to provide high quality products that meet customer requirements.

SDLC has defined its phases as follows: requirements gathering and analysis, design, development, testing, and maintenance.

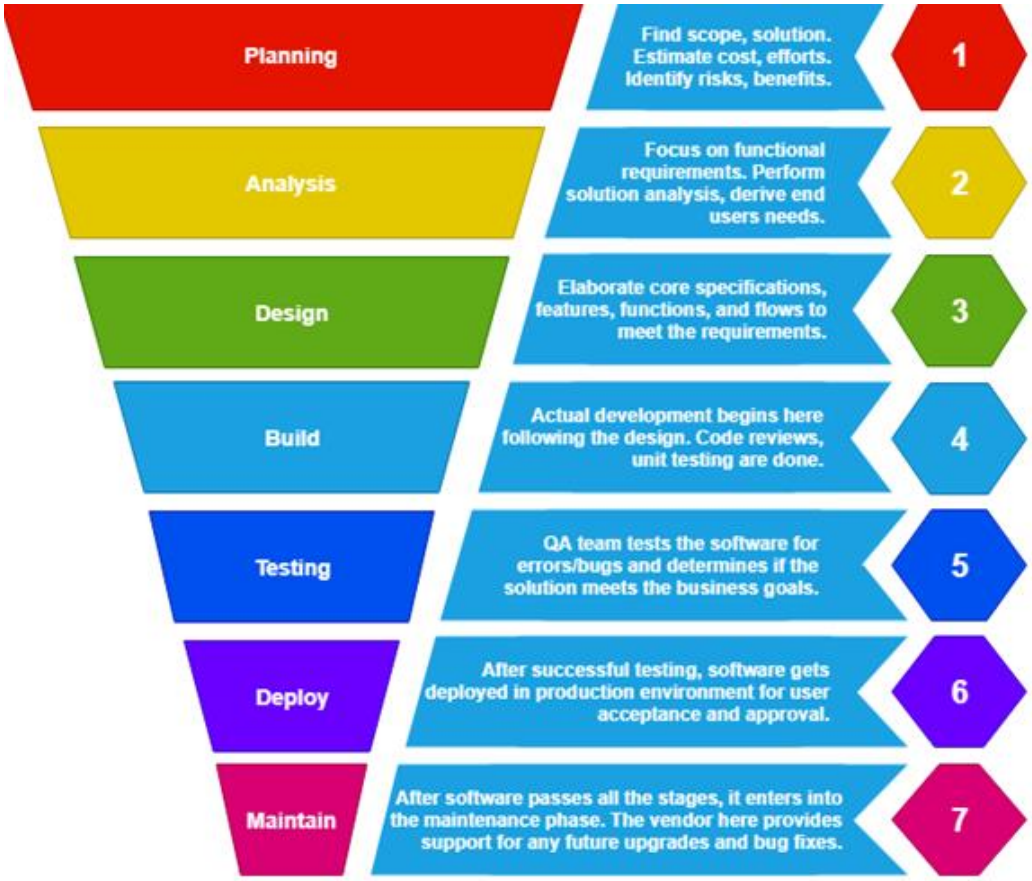

Figure 3 SDLC Phases

By following the SDLC, software development teams can ensure efficient project management, improved communication, higher quality software, and increased customer satisfaction.

There different SDLC methodology includes waterfall, V model, agile, Spiral etc. In this study, Agile was preferred

3.4.4 Agile Model

Agile software development [15] refers to software development methodologies centered aro und the idea of

iterative development, where needs and solutions evolve through collaboration between self-organized cross-functional teams.. The ultimate value of Agile development is that it enables teams to deliver value faster, with better quality and predictability, and with better ability to respond to change

Agile methods or processes Agile processes often promote a disciplined project management process that encourages regular testing and adaptations, a leadership philosophy that encourages teamwork, self-organization and accountability, a set of engineering best practices

intended to enable the rapid delivery of high-quality software and a business approach aligned with evolving customer needs and business or organizational goals.

Figure 4 Agile Model

3.4.5 Steps Followed During development of this project

Within the development of this thesis I used agile methodology as mentioned above, Agile SDLC is the method of Software development involving continuous iterative and incremental process, which focuses on the final customer satisfaction.

3.4.6.1. Phases of the agile life cycle

As mentioned earlier, the Agile software development life cycle consists of six phases

1. **Concept**

This phase involves defining the goals and high-level project requirements. It determines the direction and purpose of the development effort.

In the context of a PKI-based system for online voting, the concept phase involves understanding the need for secure online voting, defining key features, and identifying the role of Public Key Infrastructure (PKI) in ensuring the security of the system.

2. **Inception**

Inception focuses on defining the project scope, objectives, and initial requirements.

It helps in laying the groundwork for the development effort.

In the inception phase, we outline the specific security requirements related to PKI, such as digital signatures, to ensure the integrity and confidentiality of the online voting process.

3. Iteration

Agile development is characterized by iterative cycles of planning, implementation, and evaluation. The iterations involved developing and testing specific PKI-related features, such as implementing digital signatures to authenticate voters and encryption to ensure votes are transmitted. Continuous feedback and adjustments are made based on each iteration.

4. Release

The release phase involves packaging and delivering a set of features or enhancements to end users. This marks the completion of a development cycle.

During the release phase, a version of the online voting system with PKI functionality will be deployed. This can include features such as secure user authentication, encrypted data transmission, and strong verification mechanisms.

5. Maintenance

Maintenance includes ongoing support, bug fixes and updates to ensure the system remains secure and in good working order.

The maintenance phase of the PKI-based online voting system will include addressing any security vulnerabilities, updating encryption algorithms, and ensuring compliance with evolving standards to maintain a secure voting platform.

6. Retirement

Retirement phase involves decommissioning a system that is no longer in use or has been replaced by a newer version. When an online voting system reaches end of life, the decommissioning phase shall include securely decommissioning the PKI infrastructure, ensuring proper handling of cryptographic keys, and performing migration plan allows users to migrate to the new system.

3.4.7 Architecture design of Secure PKI based system for online voting

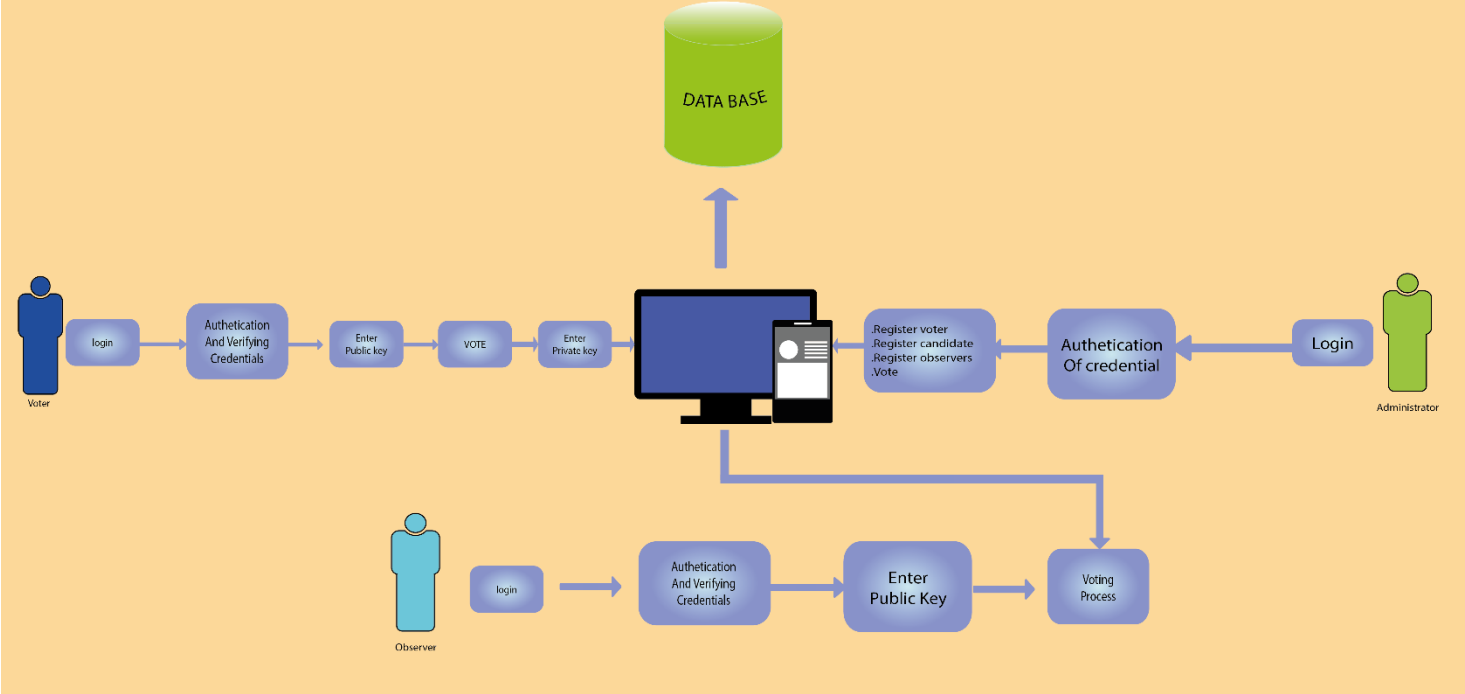

Figure 5 Architecture design of Secure PKI based system for online voting

The architecture design for the security of a Public Key Infrastructure (PKI) system for online voting involves various components and processes to ensure the integrity, confidentiality, and authentication of users and data. Below is an overview of the security architecture for both voters and administrators in the context of online voting:

3.4.7.1 Security Architecture for Voters:

- **Authentication:**

Voter Authentication:

For web-based logins, voters need to provide valid credentials, a username and password and provide public key to get candidate List

- **Voting Process:**

Once authenticated, voters access the voting interface to cast their votes securely. The system ensures the anonymity of the votes, separating the identity of the voter from the actual vote.

- **Private key for Integrity:**

Before casting a vote, a private key is applied to the vote to ensure its integrity.

The private key helps in verifying that the vote has not been tampered with during transmission or storage.

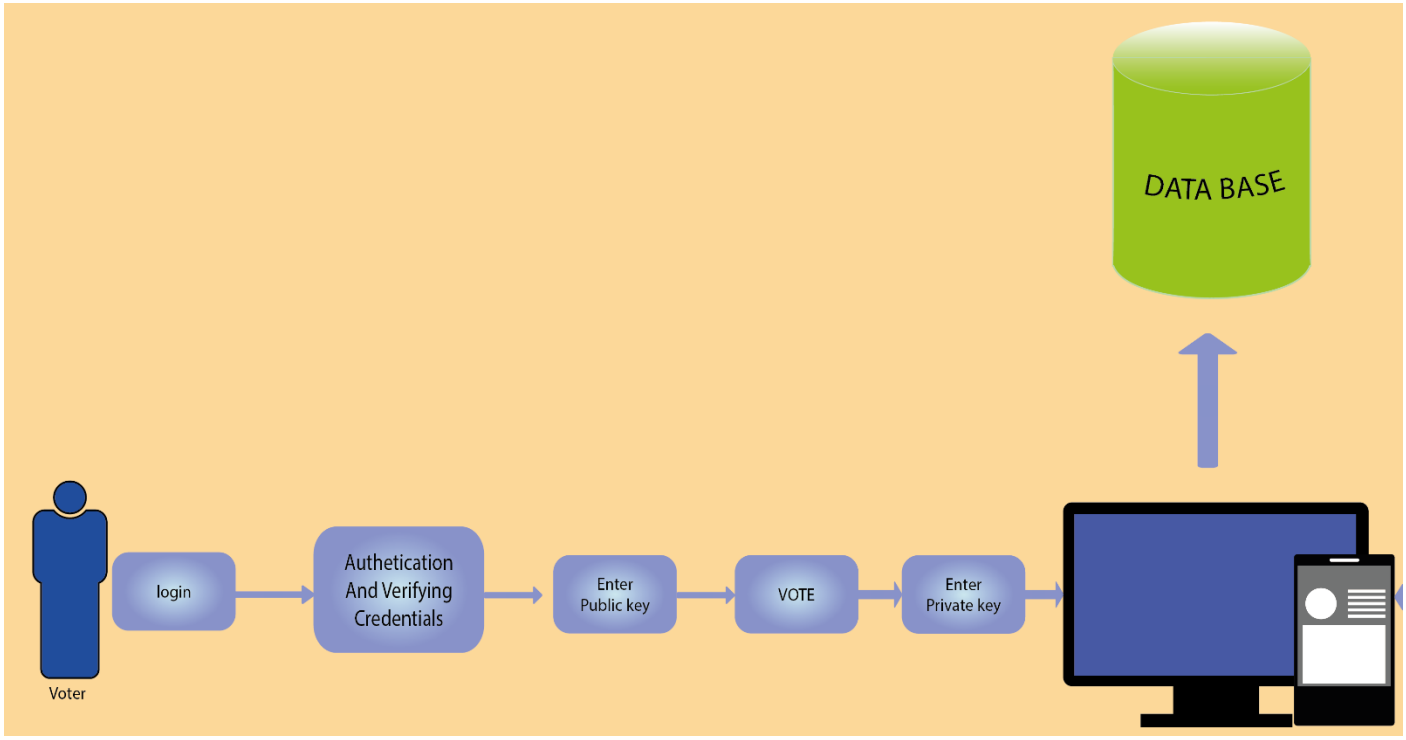

Figure 6 Security Architecture for Voter

3.4.7.2 Security Architecture for Administrators (NEC Member):

Authentication:

Adminstrator Authentication:

For web-based access, administrators must provide valid credentials for authentication.

Multi-factor authentication can be implemented for added security.

- **Administrator Privileges:**

Upon successful login, administrators have specific privileges, such as voting,registering candidates,votersand Observers, viewing election results, and publishing election outcomes.

Candidate and Voter Registration:

The administrator can register candidates and voters securely through the system.

Results Viewing and Publication:

Administrators can securely view election results through a dedicated interface.

The system ensures confidentiality and integrity of the results data.

When ready, administrators can publish the election results, making them available to the public.

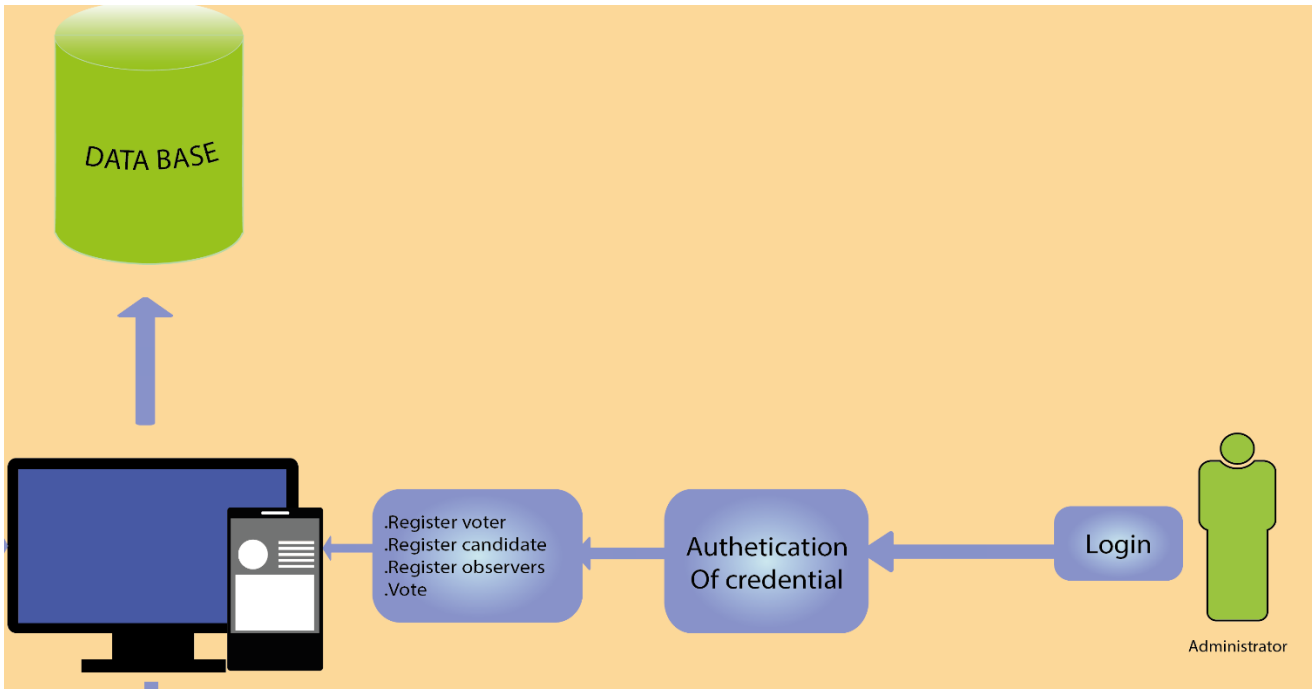

Figure 7 Security Architecture for Adminstrator(NEC)

CHAPTER 4.SYSTEM ANALYSIS AND DESIGN

4.1 Introduction

The main purpose of this chapter, is to analyze the data obtained through questionnaires, interviews, and used them to compute answers to the research and gives a detailed explanation about the requirements of the system.

4.2. Security Requirements

According to D. G. Thomas E. Carroll [10] the way elections are conducted have the biggest impact on any society and citizens can lose trust in the system if there are any discrepancies or foul play in the electoral process, so security is very important for an electronic voting system. Electoral fraud is by default a malicious threat to electronic voting[11] so security is very important to prevent the realization of this threat. The sensitivity of the electronic voting scheme also goes a long way in determining the security requirements they need to meet, for example an electronic voting scheme needed to choose the winner of a talent show (American got talent, Big Brother Africa) would not be the same as the security requirements for an electronic voting scheme required for a large scale general election in a country.

4.3 Software Requirements

One of the most difficult tasks is software selection, once the system requirements are known, after the initial selection, additional security measures are needed to determine the suitability of a particular software compared to other candidates. This section first summarizes the issues related to application requirements and then proposes more detailed comparisons.

- ✓ Operating System -------- Windows Version 10 Pro , 11 Pro
- ✓ Browser -------- Google Chrome
- ✓ Web/Application Server -------- Xamp server Version 5.3
- ✓ Database Server -------- MySQL Version 2.2
- ✓ Programming Languages -------- Laravel
- ✓ Text editor---------- Visual Studio

4.3 Hardware Requirements

The selection of hardware is very important in the existence and proper working of any software. In the selection of hardware, the size and the capacity requirements are also important. Running powerful operating systems like Windows 10,11 and so on requires a substantial amount of RAM and CPU capability. The PKI based system for online voting can be efficiently run-on Pentium system with at least 128 MB RAM and hard disk space of at least

10 GB. Floppy disk drive of 1.44 MB and 14-inch color monitor suits the information system operation. (A Printer is required for printing hard copy outputs).

- ✓ Pentium processor -------- 233 MHZ or above
- ✓ RAM Capacity -------- 128MB
- ✓ Hard Disk -------- 10GB
- ✓ Floppy disk -------- 1.44 MB
- ✓ CD-ROM Drive -------- 32 HZ
- ✓ Keyboard -------- 108 Standard

4.4 Performance Requirements

Performance is measured by the results provided by the application. Requirements specification plays an important role in analyzing a system. Only when the requirements specifications are accurately defined can a system be designed to suit the required environment. The majority of users of the current system have the power to define the requirements specifications because they are the ones who ultimately use the system. This is because the requirements must be known at an initial stage so that the system can be designed according to these requirements. It is difficult to modify a system once it has been designed and on the other hand, there is no point in designing a system that does not meet user requirements.

The system is completely dependent on the user to perform all the duties.

Table 2 Product used and their details

Network	Rooters Hubs Home or school network set up(hubs and switches)
Computing devices	Laptop or desktop,tables and smart phones

4.5 User requirement

We have mainly three users of this system

a. Administrator (should be a member of electoral commission)
b. Voters
c. Observers

4.6 Feasibility Study

4.6.1 Operational Feasibility

Operational feasibility is a measure of how a well proposed systems solves the business problems of the organization and how it satisfies the requirements analysis phase of the system development.To determine this feasibility, it is important to know if management is committe d to the proposed system. if the request is made by management, this means there is management support and the system is likely to be accepted and used. However, it is important that employees accept change. Operational feasibility can be calculated using different frameworks but we will analyze it using the PIECES framework.

i. P – performance

It determines whether the system provides sufficient throughput and response time

In our case, implementing a PKI-based online voting system provide better management as previously most of the work was done manually, so the throughput, i.e. The work was completed within the specified time, not very good but after implementing our proposed system the throughput will definitely increase because all the work in our proposed system will be done using computers making things happen very fast. The system would consume less time in keeping view to the candidate, voters, results of election etc. The voters will get response to their queries and problems much faster as compared to earlier manual systems

ii. I – information

It determines whether the system provides end users and managers with timely, relevant, accurate, and usefully formatted information. In the proposed system, all records will be kept on one server

iii. E- economic

It determines whether the system offers adequate service level and capacity to reduce the cost of business or increase the profit of the business or not. During the implementation of the proposed system, manual work will be reduced and will be replaced by IT methods because our system is completely software-based

iv. C- Control

Control refers to security and ensuring that the system will provide protection against fraud and misappropriation of data and information. After implementing the proposed system, the data will become completely safe as the entire data will be protected and only authorized persons will be able to access

v. E- Efficiency

Efficiency refers to the ability of a system to make full use of resources available to it along with giving full output. The proposed system is fully automated and will make full use of all its facilities that the system will provide

vi. S-Services

It determines whether the system provides desirable and reliable services to those who need it (users) and whether the system is flexible and expandable. The proposed system is very much flexible and we can incorporate various related components to it for better efficiency and performance of the voting process

4.6.2 Economic feasibility

A system request is economically feasible if the projected benefits of proposed system outweigh the estimated cost involved in developing or purchasing, installing and operating it. The proposed system should reduce cost and provide benefits[16]. Economic feasibility evaluates the extent and areas in which cost reductions can be achieved and to what extent. This is also an increase in company revenue. The proposed new system is expected to yield more information or less better results. Besides financial benefits, economic feasibility also analyzes service growth and customer satisfaction[17].

4.7 System Design

This section includes the system architecture, process and data modeling of the secure PKI system for online Voting.

4.7.1 Data Flow Diagram

Data flow diagrams show how information flows through a process or system. It includes the input and output data, the data store, and the various subprocesses through which the data passes. DFDs are constructed using standardized symbols and notations to describe different entities and their relationships.

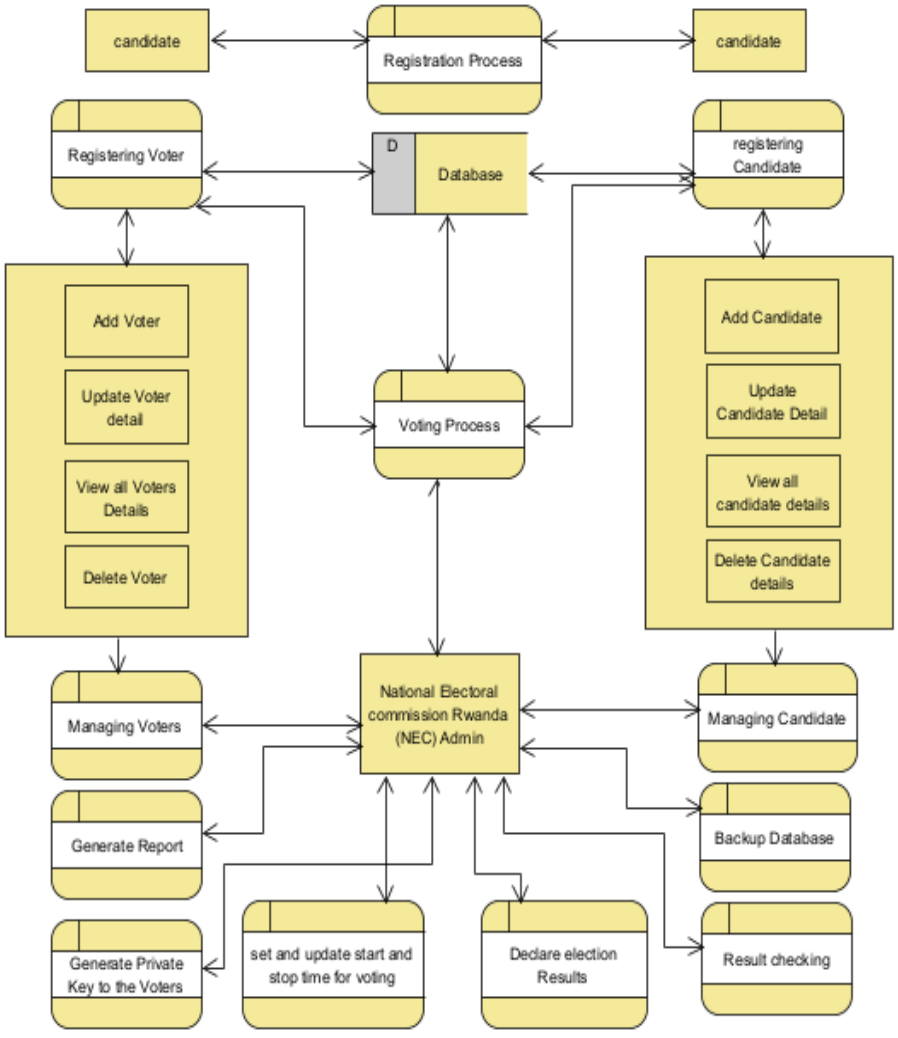

Figure 8 data flow diagram

4.7.2 Use Case Diagram

Use case diagrams are used to describe the main processes and functionality of the electronic voting System[18]. The purpose of having use case diagram is to identify the scope of the system.

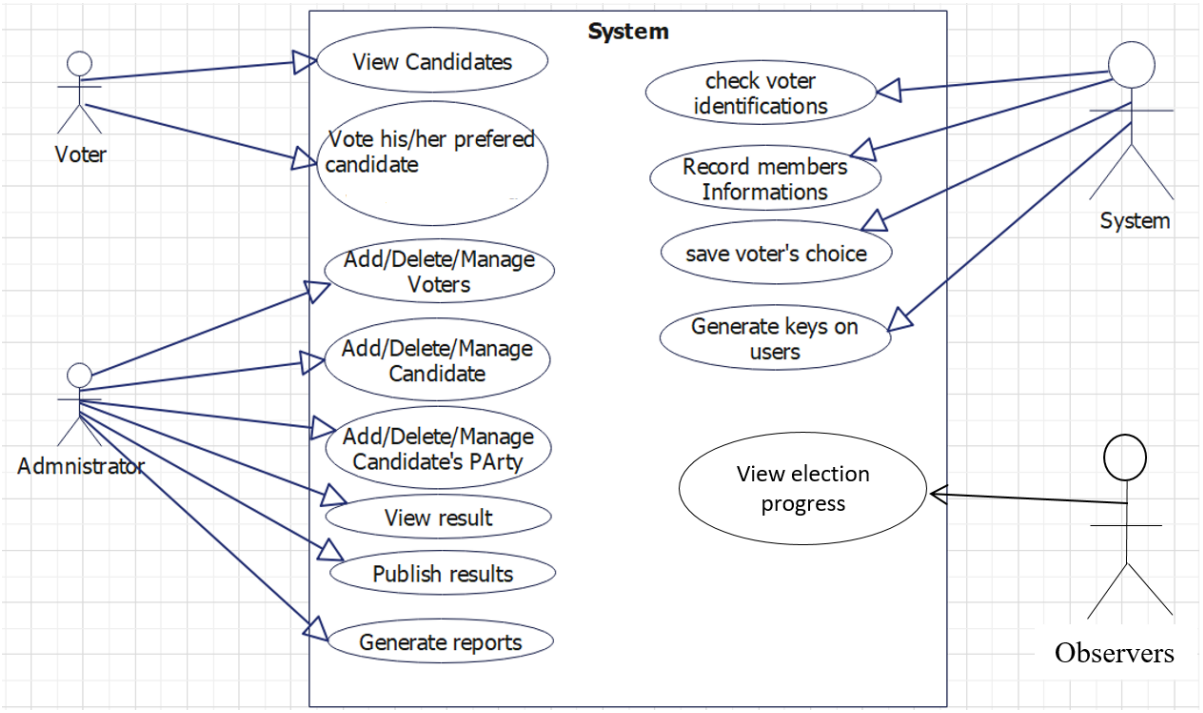

Figure 9 Use case diagram

4.7.3 Sequence Diagram

A Sequence Diagram is a UML diagram that depicts the interactions and message flow between different objects or components within a system over time, showing the sequence of messages exchanged and the duration of an object's involvement in the interaction. It is commonly used to visualize and document the dynamic behavior of a system, understand the flow of control and information between components, and communicate the design of a system with stakeholders and team members.

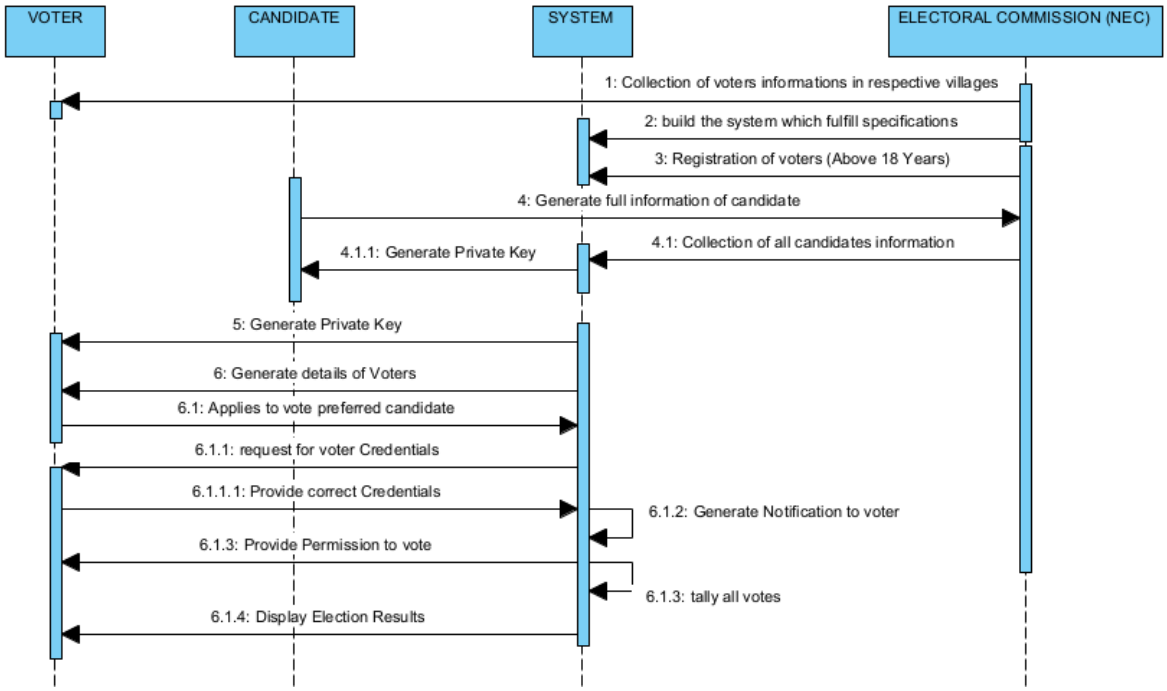

Figure 10 Sequence Diagram

4.7.4 Activity Diagram

Activity diagram is another important diagram in UML to describe the dynamic aspects of a system. An activity diagram is essentially a diagram that shows the flow from one activity to another. The flow of control flows from one activity to another. This stream can be sequential, branching, or concurrent. Activity diagram handles every type of flow control using different elements like fork, join, etc.

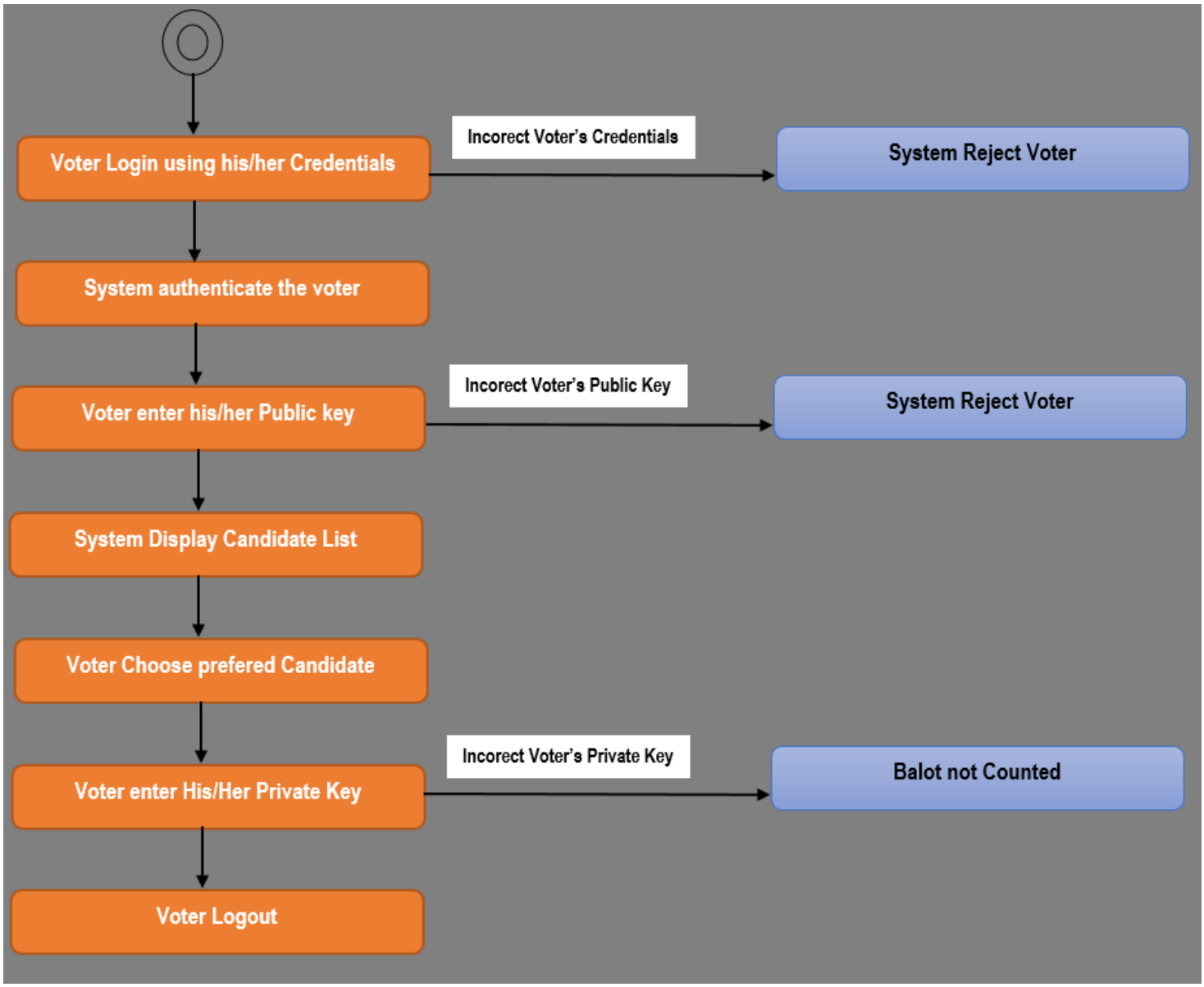

Figure 11 Activity Diagram for Voting Process

4.7.5 Entity Relationship Diagram

An ERD visualizes the relationships between entities such as people, objects or concepts in a database. An ERD also allows you to visualize the attributes of these entities.

An ER model also provides a means of communication.

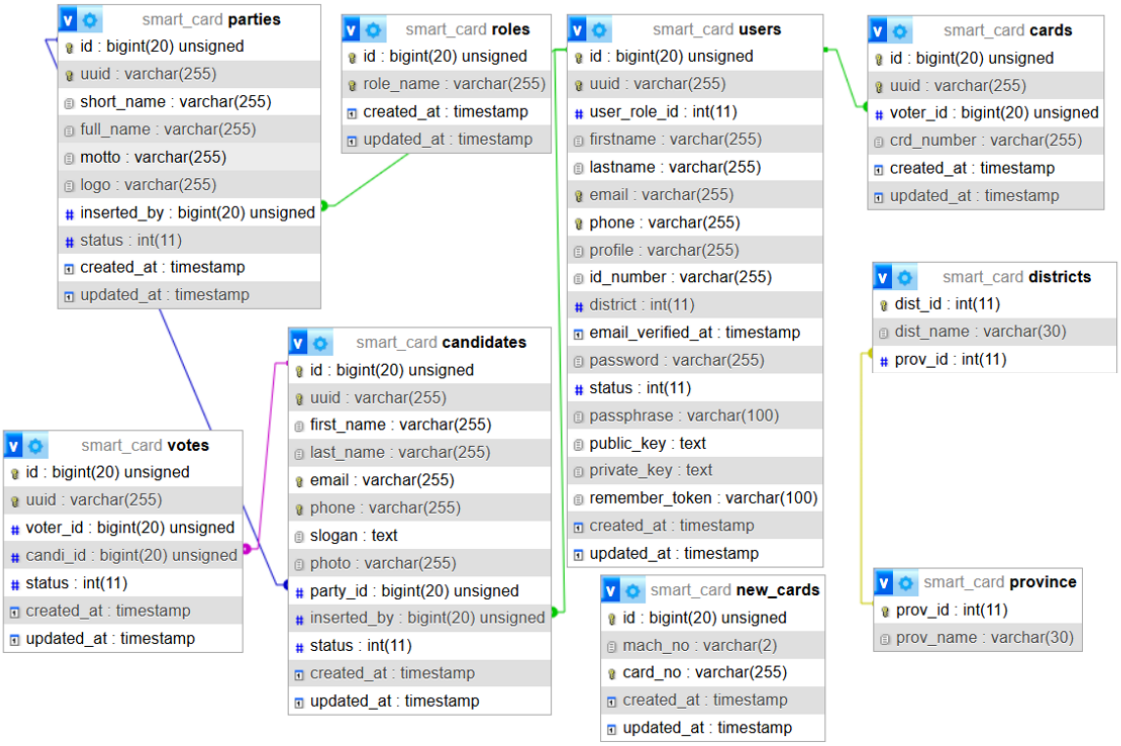

Figure 12 Entity Relationship Diagram

4.7.6 Data Dictionary

A data dictionary in a database is a centralized repository that contains metadata about the database, including information about the structure, organization, and usage of the data. It typically includes details such as data types, constraints, relationships between tables, and definitions of entities and attributes. This resource serves as a reference for database administrators, developers, and users to understand and manage the data effectively. It ensures consistency, accuracy, and clarity in data management processes and facilitates communication among stakeholders involved in database design, implementation, and maintenance.

users

Column	Type	Null	Default	Links to	Comments	Media type
id *(Primary)*	bigint(20)	No				
uuid	varchar(255)	No				
user_role_id	int(11)	No				
firstname	varchar(255)	No				
lastname	varchar(255)	No				
email	varchar(255)	No				
phone	varchar(255)	Yes	*NULL*			
profile	varchar(255)	No	https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcTpCKq1XnPYYDaUIlwlsvmLPZ-9-rdK28RToA&usqp=CAU			
id_number	varchar(255)	No				
district	int(11)	No				
email_verified_at	timestamp	Yes	*NULL*			
password	varchar(255)	No				
status	int(11)	No	1			
passphrase	varchar(100)	Yes	*NULL*			
public_key	text	Yes	*NULL*			
private_key	text	Yes	*NULL*			
remember_token	varchar(100)	Yes	*NULL*			
created_at	timestamp	Yes	*NULL*			
updated_at	timestamp	Yes	*NULL*			

Figure 13 system user identification

parties

Column	Type	Null	Default	Links to	Comments	Media type
id *(Primary)*	bigint(20)	No				
uuid	varchar(255)	No				
short_name	varchar(255)	No				
full_name	varchar(255)	No				
motto	varchar(255)	No				
logo	varchar(255)	No				
inserted_by	bigint(20)	Yes	*NULL*	users -> id		
status	int(11)	No	1			
created_at	timestamp	Yes	*NULL*			
updated_at	timestamp	Yes	*NULL*			

Figure 14 Parties information’s

candidates

Column	Type	Null	Default	Links to	Comments	Media type
id *(Primary)*	bigint(20)	No				
uuid	varchar(255)	No				
first_name	varchar(255)	No				
last_name	varchar(255)	No				
email	varchar(255)	No				
phone	varchar(255)	Yes	*NULL*			
slogan	text	No				
photo	varchar(255)	Yes	https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcTpCKq1XnPYYDaUIlwlsvmLPZ-9-rdK28RToA&usqp=CAU			
party_id	bigint(20)	Yes	*NULL*	parties -> id		
inserted_by	bigint(20)	Yes	*NULL*	users -> id		
status	int(11)	No	1			
created_at	timestamp	Yes	*NULL*			
updated_at	timestamp	Yes	*NULL*			

Figure 15 candidates identifications

CHAPTER 5. RESULTS AND ANALYSIS

5.1TESTS

5.1.1 Introduction

Software testing is an investigation conducted to provide stakeholders with information about the quality of the product or service being tested. Software testing can offer an impartial and unbiased perspective on the software, as the testing activities are carried out independently from the development process.

This independent evaluation helps to identify issues and assess the software's quality objectively. Software testing involves running a software component or system component to e valuate one or more properties of interest.

In general, these properties indicate how well the component or system under test:

1.meet the requirements that guide its design and development,

2.respond correctly for all types of input,

3.Perform its functions within an acceptable time limit,

4.is usable enough,

5.Achieves the overall results desired by stakeholders.

Software testing can be conducted at any stage when executable software is available, even if the software is partially completed. The timing and approach to software testing are often determined by the overall software development methodology being used. Testing is not limited to a specific phase and can be performed throughout the software development lifecycle.

5.1.2. Functional Testing:

Functional testing is focused on verifying that the system functions as intended, and it involves testing the various functions or features of the software.

1.User Authentication:

Verify that users can securely log in using their PKI credentials.

Test the registration process to ensure that users can enroll and receive their digital certificates.

2.Voter Registration:

Test the voter registration process to ensure that eligible users can register and receive the necessary PKI credentials for voting.

3.Ballot Generation:

Verify that the system generates accurate and secure digital ballots for each voter.

4.Vote Casting:

Test the process of casting votes to ensure that the system accurately records and encrypts each vote.

5.Results Verification:

Confirm that the system accurately tallies votes and produces correct election results.

6.Security Features:

Test encryption and decryption processes to ensure the security of transmitted data.

Verify that only authorized users can access sensitive information.

7.Usability Testing:

Ensure that the user interface is intuitive and easy to navigate for all users, including those with limited technical expertise.

5.1.3 Non-Functional Testing:

Non-functional testing focuses on aspects other than specific behaviors of the system.

For a PKI-based online voting system, the following non-functional testing aspects are considered:

1.Performance Testing:

Test the system's performance under normal and peak loads to ensure it can handle the expected number of simultaneous users.

Evaluate response times for key operations.

2.Scalability Testing:

Verify that the system can scale to accommodate a growing number of users and transactions.

3.Security Testing:

Conduct penetration testing to identify and address vulnerabilities in the system.

Verify that encryption and decryption processes are robust and secure.

4.Reliability and Availability Testing:

Test the system's reliability by simulating various failure scenarios.

Ensure the system is available and responsive during scheduled and unscheduled times.

5.Compatibility Testing:

Confirm that the system works seamlessly with different web browsers, operating systems, and devices.

6.Load Testing:

Assess how the system performs under various load conditions to identify potential bottlenecks.

By conducting thorough functional and non-functional testing, you can ensure that the PKI-based online voting system is not only feature-rich but also robust, secure, and capable of handling real-world usage scenarios.

5.2 Results

The development of a Public Key Infrastructure (PKI) based system for online voting involves implementing a secure and robust framework to ensure the integrity, confidentiality, and authenticity of the voting process. The following are the results from our developed PKI based system for online voting

1. Security

Encryption: This PKI system ensures that communication between the voter and the voting server is encrypted. Public and private key pairs are used to encrypt and decrypt sensitive data, preventing unauthorized access.

Digital Signatures: Digital signatures, generated using private keys, authenticate the source of the vote and ensure that the vote has not been tampered with during transmission.

2. Authentication:

Voter Identification: PKI enables a strong authentication process. Each voter has a unique pair of public and private keys. The public key is used to encrypt the vote, and the private key is used to decrypt it. This ensures that only the authorized voter can cast a vote.

3. Non-repudiation:

Accountability: Digital signatures provide non-repudiation, meaning that a voter cannot deny casting a vote. This is crucial for the integrity of the election process.

4. Tamper Resistance:

Immutable Transactions: The use of cryptographic techniques in PKI ensures that once a vote is cast, it cannot be altered or deleted without detection. This adds a layer of tamper resistance to the voting system.

5. Accessibility:

User-Friendly Interfaces: Despite the complex cryptographic processes underlying the system, the user interfaces can be designed to be user-friendly, ensuring accessibility for a wide range of voters.

Compatibility: The PKI system can be integrated with various devices, making it accessible through computers, smartphones, or other platforms.

6. Scalability:

Handling a Large Number of Voters: PKI systems can be designed to handle a large number of voters simultaneously, making them scalable for elections of different sizes.

7. Trust and Transparency:

Public Key Infrastructure: The transparent use of PKI instills trust in the voting process. The public nature of the infrastructure allows for independent verification of the system's security.

8. Challenges:

Key Management: Ensuring secure key management is crucial. Lost or compromised private keys could lead to unauthorized voting.

Voter Education: Proper education is essential to make voters aware of the security features and processes involved in the PKI-based voting system.

Conclusion on the results:

A PKI-based system for online voting offers a high level of security, authentication, and tamper resistance. It provides a foundation for building a trustworthy and transparent online voting infrastructure.

5.3. Graphical User Interface

5.3.1. Login page

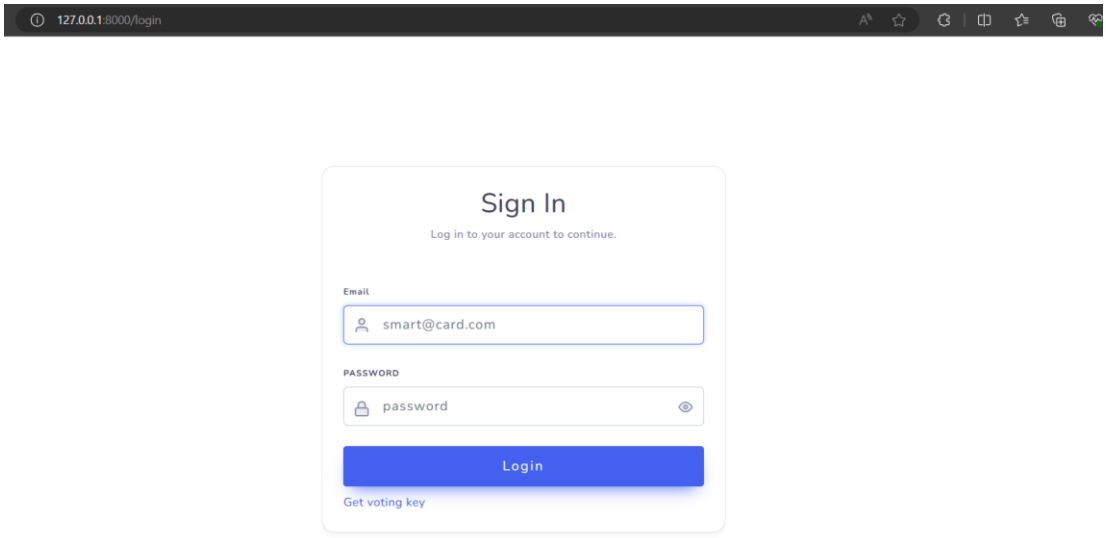

Figure 16 Login page

The above login form for a PKI system for online voting is designed to securely authenticate users using digital certificates. Functionality typically found in this login form:

Username/Identification Field:

Users enter their unique identification, often associated with their digital certificate. This could be a username, voter ID, or any other identifier linked to their PKI credentials.

5.3.2. Candidate Registration Form

A candidate registration form for a Public Key Infrastructure (PKI) system in the context of online voting would typically include various fields to collect essential information from the candidates. The PKI system ensures secure and authenticated communication, and the registration form plays a crucial role in gathering accurate details for the electoral process.

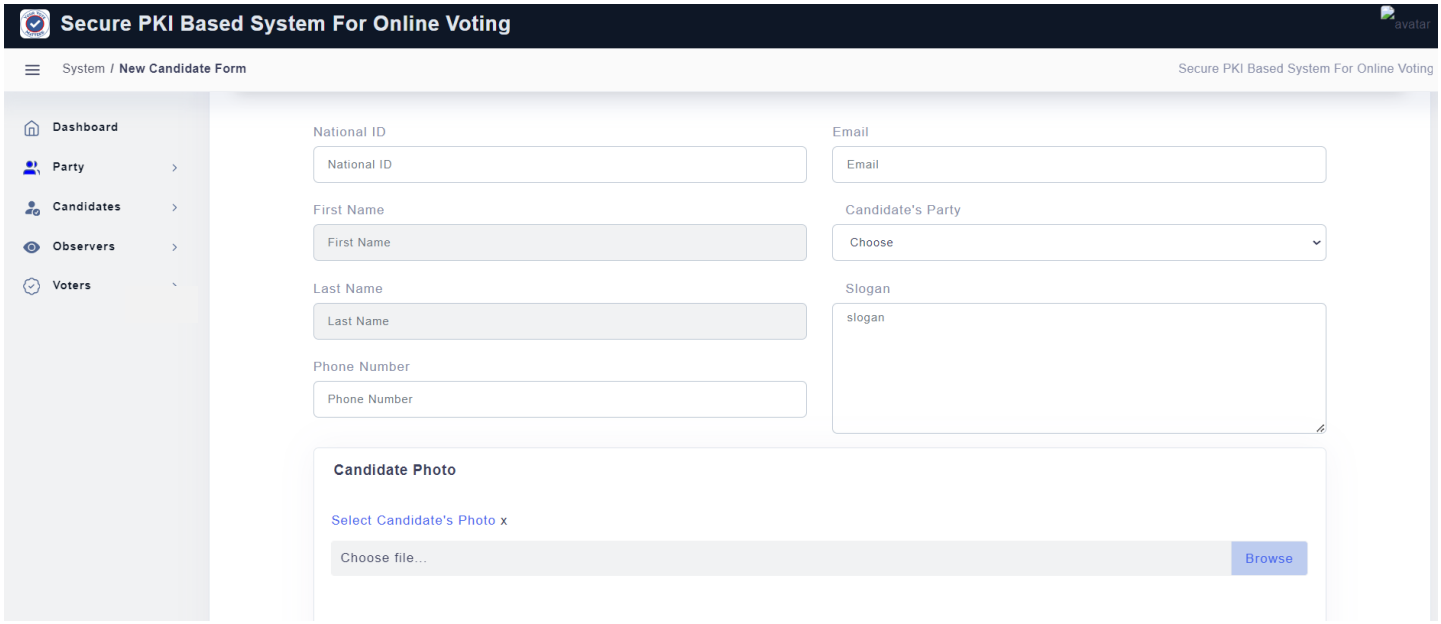

Figure 17 Candidate Registration Form

5.3.3. Managing Candidate

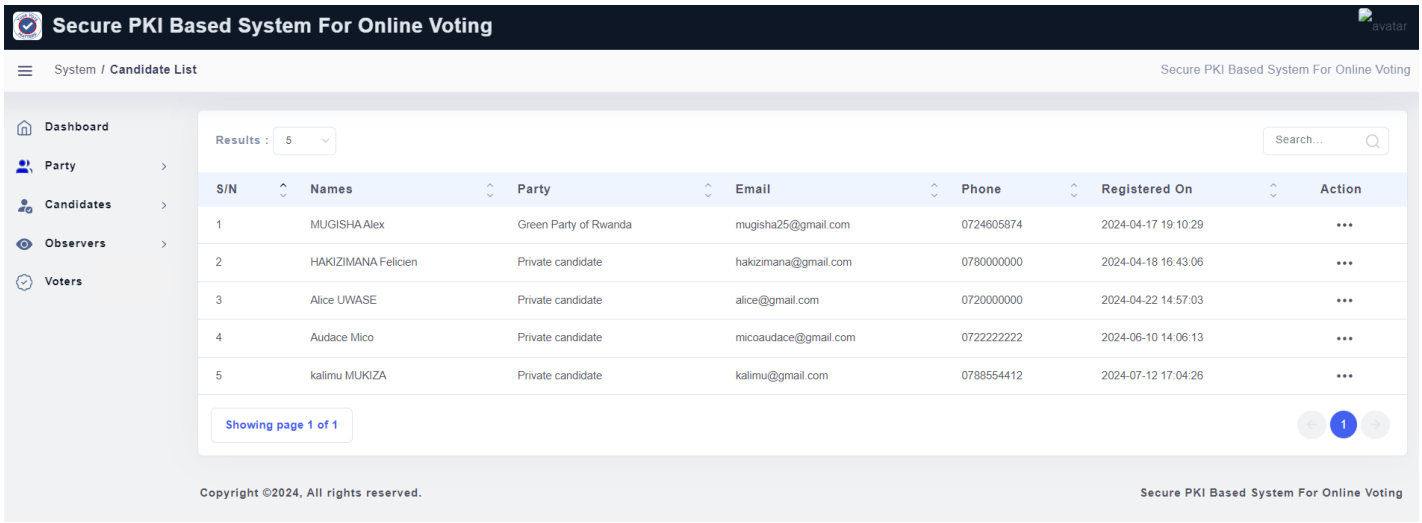

Figure 18 form for Managing Candidate

Managing candidates for this Public Key Infrastructure (PKI) system for online voting involves overseeing the digital certificates and associated user credentials. The following is a description of the key features and functionalities that an administrator might have in managing candidates for a PKI-based online voting system:

Election Activation/Deactivation:

Activation: The administrator should have the ability to activate voting allowing users to participate in the online voting process.

Deactivation: at the end of voting, administrator should be able to deactivate voting process, preventing them from participating in online voting.

User Update:

Profile Information: The system should allow administrators to update user information, including details such as candidate names, contact information, and other relevant data.

User Deletion:

Account Removal: The administrator should have the capability to delete a user's account entirely. This might be necessary if a candidate withdraws from the election or for other administrative reasons.

Certificate Revocation: In this PKI system, if a user is deleted, their digital certificate should be revoked to ensure that it is no longer valid for authentication or encryption purposes.

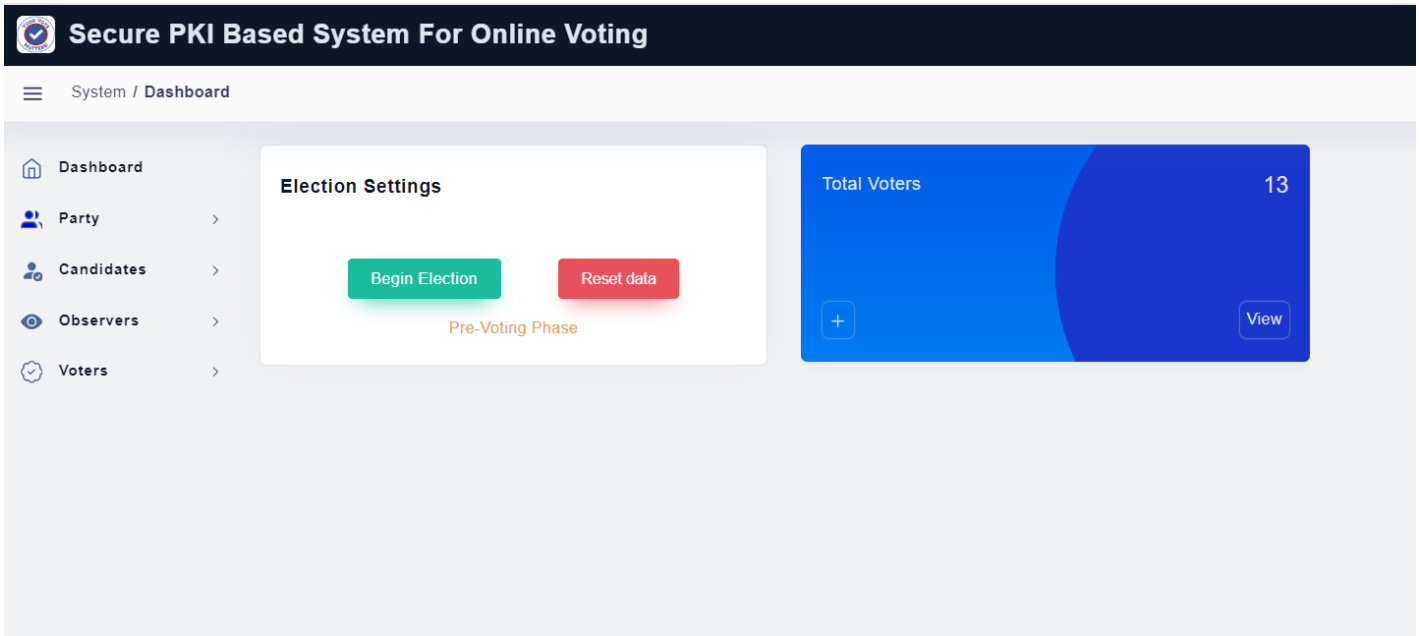

Figure 19 administrator dashboard

5.3.4. Form of administrator for election progress

This form provides administrator with a comprehensive information about the election process like Real-time updates on voting counts and results.

CHAPTER 6. CONCLUSIONS AND RECOMMENDATIONS

6.1 Conclusions

In conclusion, this project introduces a secure PKI-based system for online voting, offering a decentralized electronic voting solution. The system is designed to safeguard user data, prevent tampering, and uphold the integrity of the voting process. It can be implemented in various contexts, including governmental and private institutions, with the aim of replacing traditional methods and enhancing the efficiency of online voting.

Overall, this project contributes to advancing the field of online voting systems by providing a secure, efficient, and user-friendly solution for democratic elections.

6.2 Recommendations

Implement Biometric Voter Identification: Integrate a biometric voter identification module, such as facial recognition or iris scanning, to enhance the security and reliability of the voter authentication process. This can help mitigate the risks of impersonation or unauthorized access.

Allow Sufficient Time for Project Implementation: It is crucial to allocate an adequate timeframe for the implementation of the secure PKI-based system for online voting. The technical development and integration of PKI infrastructure, including the necessary encryption protocols and digital certificate management, require careful planning and execution. Allotting enough time will ensure the quality, reliability, and transparency of the system.

Plan for Training, Professional Development, and Voter Education: To ensure the successful adoption and acceptance of the secure PKI-based system, comprehensive training programs should be designed for election officials and staff responsible for managing the online voting process. Additionally, voter education initiatives should be implemented to familiarize voters with the new system, its benefits, and the security measures in place. This will empower voters to have confidence in the technology and take ownership of their voting experience.

Obtain Buy-in from Key Stakeholders: Garnering support from key stakeholders, including political parties, is crucial for the successful implementation of the secure PKI-based system. Engage in dialogue and address any concerns or objections raised by stakeholders to build consensus and trust. Anticipate potential opposition and proactively address objections and weaknesses by providing clear explanations of the system's advantages, security measures, and

integrity safeguards. This will help mitigate skepticism and political disputes related to the technology.

LIST OF REFERENCES

[1] "https://aceproject.org/ace-en/topics/es/onePage."

[2] S.-L. N. and S. S.-G. Yang Feng, *"An Electronic Voting System Using GSM Mobile Technology". Technical Report. RHUL-MA-2006-5. (Department of Mathematics, Royal Holloway, University of London, 2006),. .*

[3] L. C. and R. Cytron, *Sensus: A security-conscious electronic polling system for the Internet. In Proceedings of the Hawaii International Conference on System Sciences. Wailea, Hawaii, 1997. .*

[4] N. A. of Sciences, "https://www.nap.edu/read/25120/chapter/7."

[5] "https://searchdatacenter.techtarget.com/definition/IT."

[6] W. Paper, P. Overview, and T. Impact, "The problems with a paper based voting system," *Int. J. Eng. Technol.*, vol. 4, no. 2, pp. 1–5, 2015, [Online]. Available: http://www.sciencepubco.com/index.php/ijet/article/view/4441.

[7] P. G. Neumann, "'Risks in Computerized Elections (Inside Risks)'. Comm. ACM 33, 11, p. 170, November 1990."

[8] M. J. M. Chowdhury, "Comparison of e-voting schemes: Estonian and Norwegian solutions," *Int. J. Appl. Inf. Syst.*, vol. 6, no. 2, pp. 47–54, 2013.

[9] N. (Ed). Baldersheim, H. & Kersting, "'Electronic voting and democracy: a comparative analysis'. Palgrave Macmillan, New York. 2004."

[10] D. G. Thomas E. Carroll, *"A secure and anonymous voter-controlled election Yr:, scheme". Journal of network and computer applications [1084-8045] Carroll 2009, 2009 vol:32 iss:3 pg:599. .*

[11] S. Kırbıyık, "Implementation_issues_in_secure_E-voting_schemes," *Экономика Региона*, p. 32, 2004.

[12] P. P. M. P. Fauzi, *Journal of Islamic Civilization, vol. 1, no. 1 SE-Articles, pp. 4048, Apr. 2019, doi: 10.33086/jic.v1i1.918. .*

[13] 2011 Rehamn and Sultana, "No Title *مجلة العربية*",كتاب المجامع, vol. 2, no. 5, p. 255, 2009.

[14] a D. S. Rodrigues, "Chapter Five Research Methods : the Literature Review , Conducting Interviews and," pp. 99–110, 2009.

[15] C Prime Inc, “What is AGILE? - What is SCRUM?,” *Https://Www.Cprime.Com/Resources/What-Is-Agile-What-Is-Scrum/*, no. 877, 2021.

[16] D. Yoon, “Economic Feasibility Analysis Model,” *Prelim. Feasibility Public Res. Dev. Proj.*, no. November, pp. 31–48, 2021, doi: 10.1108/978-1-80117-266-020211020.

[17] T. C. Morphology, “No 主観的健康感を中心とした在宅高齢者における 健康関連指標に関する共分散構造分析Title.”

[18] S. Lwomwa Joseph, “A STUDENT e-VOTING SYSTEM A case study of College of Computing and Information Science (CoCIS),” 2019.

[19] (Abu Idrisa,Rohana Yuso, 2015) https://core.ac.uk/download/pdf/42984224.pdf

APPENDICES

Appendix1:Questionnaire used during interview for the project titled "Secure PKI-based System for Online Voting"

Section 1: General Information about Voting

1. Have you participated in any voting processes before (e.g., elections, surveys)?

    a) Yes

    b) No

2. How frequently do you participate in voting processes?

    a) Every election

    b) Occasionally

    c) Rarely or never

3. What factors do you consider most important when choosing a voting method? (Select up to three)

    a) Security

    b) Convenience

    c) Accessibility

    d) Anonymity

    e) Transparency

4. Are you familiar with the concept of online voting?

    a) Yes

    b) No

5. Would you be willing to try online voting as an alternative to traditional paper-based voting methods?

   a) Yes

   b) No

   c) It would depend on other factors

Section 2: Current Voting System (Paper-based)

6. How confident are you in the accuracy of paper-based voting systems?

   a) Very confident

   b) Somewhat confident

   c) Not confident

7. Have you ever encountered difficulties or inconveniences while participating in a paper-based voting process?

   a) Yes

   b) No

8. How concerned are you about potential issues such as lost or mishandled paper ballots in the current voting system?

   a) Very concerned

   b) Somewhat concerned

   c) Not concerned

9. Do you believe paper-based voting systems adequately protect the privacy and anonymity of voters?

    a) Yes

    b) No

    c) Not sure

10. Would you be open to exploring alternative voting systems that offer enhanced security and convenience compared to paper-based systems?

    a) Yes

    b) No

    c) It would depend on the alternative system

Section 3: New Proposed System (Secure PKI-based System for Online Voting)

11. Are you familiar with the concept of a Public Key Infrastructure (PKI)?

    a) Yes

    b) No

12. How important is the security of the voting system to you when considering the transition to an online voting system?

    a) Very important

    b) Somewhat important

    c) Not important

13. Would you trust an online voting system that utilizes PKI ?

    a) Yes

    b) No

    c) It would depend on other factors

14. Are you concerned about potential cybersecurity threats or hacking attempts targeting online voting systems?

    a) Yes, very concerned

    b) Somewhat concerned

    c) Not concerned

15. Would you be more likely to participate in an online voting ?

    a) Yes

    b) No

    c) It would depend on other factors

Appendix2: Web.php

In Laravel, the web.php file is the default routing file for defining web routes. It is located in the routes directory of your Laravel project. The web.php file is responsible for handling HTTP requests for your application's web interface.

```
<?php
```

```php
use Illuminate\Support\Facades\Route;
use App\Http\Controllers\MainController;
use App\Http\Controllers\AuthController;


Route::get('/login', function () {
    return view("files.auth.login");
})->name('user.login');
Route::post('/authenticate',[AuthController::class,'authenticate'])->name('user.logged');


// Route::get('/system', function () {
//     return view("files.main.maintainance");
// })->name('system.maintainance');

Route::get('/changepassword', function(){
    $title="Change Password";
    return view("files.auth.changepass",  compact('title'));
});
Route::get('/check-key', [MainController::class,'checkkey']);
Route::get('/check-key2', [MainController::class,'checkkey2']);
Route::get('/check-key3', [MainController::class,'checkkey3']);
Route::get('/unlock-key', [MainController::class,'unlockkey']);
Route::get('/unlock-key2/{pass}/{id}', [MainController::class,'unlockkey2']);

Route::get('/',[MainController::class,'dashboard'])->name('dashboard.index');
// Route::get('/dashboard',[MainController::class,'dashboard2']);

Route::get('/getkey', function(){
    return view('files.key.getkey');
});
Route::get('/getid',[MainController::class,'getID']);
```

```
Route::get('/fetchvote',[MainController::class,'fetchvote']);
Route::get('/fetchuser',[MainController::class,'fetchuser']);

Route::post('/savekeys',[MainController::class,'savekeys']);
Route::post('/comparekeys',[MainController::class,'comparekeys']);
Route::post('/compareprivate',[MainController::class,'compareprivate']);
Route::post('/comparepublic',[MainController::class,'comparepublic']);
Route::get('/confirmkeys',[MainController::class,'confirmkeys']);
Route::get('/getvoters',[MainController::class,'getvoters']);
Route::get('/deleteuser',[MainController::class,'deleteuser']);

Route::group(['middleware' =>['auth']],function(){

   // Route::get('/dashboard',[MainController::class,'dashboard'])->name('dashboard.index');
   // Voter route

   // Route::post('/changepass',[AuthController::class,'changePassword']);
   Route::get('/voter-create',[MainController::class,'new_voter'])->name('voter.new');
   Route::post('/voter-store',[MainController::class,'voter_store'])->name('voter.save');
   Route::get('/voter-list',[MainController::class,'voterList'])->name('voters.list');
   Route::get('/voter/{id?}',[MainController::class,'voterListById'])->name('voter.view');
   Route::get('/voter-edit/{id?}',[MainController::class,'voterEdit'])->name('voter.edit');
       Route::put('/voter-update/{id}',[MainController::class,'voterUpdate'])->name('voter.edi-
tOp');
                           Route::get('/voterDelete/{uuid}',[MainController::class,'voterDelete'])-
>name('voter.delete');

   // candidate route
         Route::get('/candidate-create',[MainController::class,'new_candidate'])->name('candi-
date.new');
        Route::post('/candidate-store',[MainController::class,'candidate_store'])->name('candi-
date.save');
   Route::get('/candidate-list',[MainController::class,'candidateList'])->name('candidate.list');
```

```
    Route::get('/candidate/{uuid}',[MainController::class,'candidateListById'])->name('candidate.view');
    Route::get('/candidate-edit/{uuid}',[MainController::class,'candidateEdit'])->name('candidate.edit');
                Route::put('/candidate-update/{uuid}',[MainController::class,'candidateUpdate'])->name('candidate.update');
                 Route::get('/candidateDelete/{uuid}',[MainController::class,'candidateDelete'])->name('candidate.delete');

  // Election routes
       Route::get('/election-progress',[MainController::class,'electionProgress'])->name('election.progress');
      Route::get('/election-result',[MainController::class,'electionResult'])->name('election.result');
  Route::get('/voter-vote/{uuid}',[MainController::class,'vote_store'])->name('voter.vote');

  Route::get('/partyList',[MainController::class,'partyList'])->name('party.list');
  Route::get('/party-create',[MainController::class,'newparty'])->name('party.new');
  Route::post('/party-store',[MainController::class,'party_store'])->name('party.save');
  Route::get('/party-show/{id?}',[MainController::class,'party_show'])->name('party.show');

  // Route::get('/options',[MainController::class,'newOptionForm'])->name('option.new');
  // Route::get('/options',[MainController::class,'newOptionForm'])->name('option.new');
  // Route::post('/option',[MainController::class,'newOption'])->name('option.save');
  // Route::get('/logs',[MainController::class,'logs'])->name('logs.report');
  // Route::get('/getOption/{id?}',[MainController::class,'getOption'])->name('get.option1');

  Route::get('party-edit/{id}',[MainController::class,'party_edit'])->name('party.edit');
      Route::put('party-update/{id}',[MainController::class,'party_update'])->name('party.update');
  Route::get('party-delete/{id}',[MainController::class,'party_delete'])->name('party.delete');

   //  Route::post('UpdateSetting',[MainController::class,'UpdateSetting'])->name('update.setting');
```

```
    Route::post('UpdatePassword',[MainController::class,'UpdatePass'])->name('change.pass');
    // Route::get('getOptionById/{id?}',[MainController::class,'opt'])->name('change.pass');
    // Route::get('optionEdit/{id?}',[MainController::class,'optEdit'])->name('edit.option');
    // Route::post('optionEditOp',[MainController::class,'optEditOp'])->name('option.update');
    // Route::get('gateEdit/{id?}',[MainController::class,'updateGate'])->name('gate.update');
     // Route::post('gateEditOp/{id?}',[MainController::class,'updateGateOp'])->name('gate.up-
dateOp');

    // Activate and disactivate election
      Route::get('activate/disactivate',[MainController::class,'activateDisactivate'])->name('acti-
vate.disactivate');

    Route::get('/setting', function () {
        $title = "Setting";
        return view("files.auth.setting", compact('title'));
    })->name('user.setting');
    Route::get('/logout',[AuthController::class,'logout'])->name('user.logout');
});
});

Route::post('/getInfo',[MainController::class,'getInformation'])->name('voterInfo');
Route::get('/voter-vote1/{uuid}/{user}',[MainController::class,'vote_store1'])-
>name('voter.vote1');

Route::get('/getdistrict',[MainController::class,'getDistrict']);
Route::get('/report',[MainController::class,'report'])->name('report.index');
```

Appendix3 letter

UNIVERSITY of RWANDA

COLLEGE OF SCIENCE AND TECHNOLOGY

SCHOOL OF ICT

Kigali, 14th April 2023

Dear Sir/Madame;

TO WHOM IT MAY CONCERN

RE: INTRODUCTORY LETTER FOR JEAN MARIE VIANNEY AHIMANA, REGISTRATION NUMBER 220020210

The above subject refers.

We take this opportunity to introduce to you **Mr. Jean Marie Vianney AHIMANA,** a master's student at University of Rwanda - College of Science and Technology (UR-CST) in the department of Computer Science, Masters of Software Engineering.

As part of the requirement for Master's program, he is required to complete thesis in a given field. **Mr. Jean Marie Vianney** is currently undertaking research in Software Engineering with the topic "***Secure PKI Based System for Online Voting***". It's against this background that you are kindly requested to assist him in providing earnest response to the questions contained in the questionnaire either online or face to face interview. All information provided will be strictly treated as confidential and purely academic.

It will be grateful if positive response is given to him to work on his research project in your esteemed organization. Please don't hesitate to contact us in case you need further clarification.

Yours faithfully,

Dr. Frederic Nzanywayingoma
Postgraduate Programmes Coordinator, School of ICT
College of Science and Technology
University of Rwanda
Tel: +250780310446
E-mail: f.nzanywayingoma@ur.ac.rw

Dr. Uwitonze Alfred
Dean, School of ICT
College of Science and Technology
University of Rwanda
Tel: +250788549588
Email: alfruwitonze@gmail.com

COMMISSION ELECTORALE NATIONALE
Accusé de réception
Date 14 APR 2023
Nom et Prénom CS
Signature