CHAPTER 1

INTRODUCTION

1.1 OVERVIEW

India is a constitutional democracy with a parliamentary system of government, and at the heart of the system is a commitment to hold regular, free and fair elections. These elections determine the composition of the government, the membership of parliament. Elections are conducted according to the constitutional provisions, supplemented by laws made by parliament. Same as parliament and assembly elections the bar council and medical council are also conduct an election for every five years. The still conduct the election by traditional paper ballot system. Using paper ballot is time-consuming and it involves more manual power. The votes capture by paper ballot can be store for a limited period of time. This project provides a secured platform for voting system. E-Voting is a web-based voting system that will help to manage the elections easily and securely. This voting system can be used for casting votes during the elections in councils. Security provided through encryption algorithms and techniques. The major background knowledge of the algorithms and techniques used in this proposed work is discussed below.

1.2 E-VOTING

Electronic voting (also known as e-voting) is voting that uses electronic means to either aid or take care of casting and counting votes. Depending on the particular implementation, e-voting may use standalone electronic voting machines (also called EVM) or computers connected to the Internet. It may encompass a range of Internet services, from basic transmission of tabulated results to full-function online voting through common connectable household devices. The degree of automation may be limited to marking a paper ballot, or may be a comprehensive system of vote input, vote recording, data encryption and transmission to servers, and consolidation and tabulation of election results.

1.3 CRYPTOGRAPHY

Cryptography is the study of techniques for secrecy and authentication of message. Cryptographic algorithms entrench the security of the data by converting the data into unintelligent form. Modern cryptography is highly oriented with mathematics, computer science, electrical engineering, communication science and physics. Modern cryptography can be categorized into

- Symmetric- key cryptography (or) Private Key cryptography
- Asymmetric- key cryptography (or) Public key cryptography

Symmetric key cryptography deals with the usage of same key for encryption and decryption. Symmetric ciphers are mostly used for achieving cryptographic primitives than just encryption. Hence often a message authentication code is added to the cipher text to ensure that, changes to the cipher text will be noted by the receiver. Symmetric key cryptosystems are susceptible to attacks. Symmetric key cryptosystem may also be referred as Public key cryptosystems and can be classified into block cipher and stream cipher. In Asymmetric key cryptography, encryption can be performed by anyone with the public key, but decryption can be performed only by the holder of the paired private key. It is used as a method of assuring the confidentiality, authenticity and non-repudiation of electronic communications and data storage. Public key cryptosystems rely on cryptographic algorithms based on mathematical problems that currently admit no efficient solution. Because of the computational complexity of asymmetric encryption, it is used mostly for small blocks of data.

1.3.1 Encryption algorithm

The increased use of computers and communication system has increased the rise of proprietary information. Hence it has become imperative to protect useful information from malicious activities such as attacks. Encryption is an initial method of protecting valuable electronic information. Through the use of any algorithm, information is converted into meaningless cipher text. A key is used for transforming the data back into the original form. Some of the traditional encryption algorithms are Hill, Rail fence, Vignere, Blowfish, AES, RC5, etc.

1.3.2 Need for cryptosystem

Cryptosystem is required in this present technological era for, secure data transmission and protecting the information. Privacy is a basic requirement in any field. It may be personal or private to an organization. Any information in medical field or defense field of a country requires high confidentiality which when revealed out may cause wars. It is believed that such security can be provided effectively by cryptosystems.

1.3.3 Usage of cryptography in e-voting

Cryptography offers a number of benefits to electronic voting and counting Solutions. It may be used to perform tasks such as encrypting votes and digital ballot boxes, ensuring votes and software are unmodified, verifying the identity of a voter before he or she casts a ballot, and assisting in auditing and tallying the results of an election. Considering the paramount importance of ballot secrecy and fraud detection, cryptography has proved a useful tool for countries employing election technologies.

1.4 BENEFITS OF THE SYSTEM

The biggest advantage of e-voting is that it has the potential to make voting easier and more convenient. For those who have access to computers and the Internet, online voting would take little more effort than a few clicks. Related to administration, e-voting are claimed to produce faster and more accurate election results. E-voting systems are said to deliver a faster official ballot tabulation process and are alleged to be more accurate than other types of machine counting (such as punching cards) which are sometimes criticized for error. Over the long term all types of Internet voting have the potential to be less expensive to operate and execute than traditional paper ballots which require setting up and staffing polls.

1.5 MOTIVATION

All council elections such as bar council election, Medical council elections, etc. are conducted by traditional paper ballot election. The average of papers used for an election is approximately 1000,000 sheets of paper. When running an e-voting, no need of paper, printing, physical urns or staff may, therefore, lead to a lower monetary investment and you avoid the need for all the physical infrastructure usually required on a traditional voting.

1.6 OBJECTIVE OF THE SYSYTEM

The major objectives of this project work is listed below:

- To provide secured platform for e-voting.
- To reduce the complexity in voting.
- To overcome the traditional paper ballot system.

1.7 ORGANIZATION OF THE REPORT

The rest of the report is explained as follows, In chapter 2, related literatures to the proposed work are collected and presented.

In chapter 3, the system architecture and all of its components are briefly explained. In addition to it, the hardware and the software component required are also discussed.

In chapter 4, the system requirements and system specifications explained in detailed.

In chapter 5, the paillier encryption and paillier decryption techniques are briefly explained.

In chapter 6, the proposed e-voting system is explained elaborately along with its process.

In chapter 7, the implementation and results are briefly explained.

In chapter 8, conclusion and future enhancements takes place.

CHAPTER 2

LITERATURE SURVEY

2.1 The Homomorphic Other Property of Paillier Cryptosystem [Ref: 3]

One example of Paillier's encryption schemes and homomorphic encryption was illustrated and the mathematical details, Subtraction, Multiply, Division binary operation of binary based integer number operands was explained.

2.2 A Java Implementation of Paillier Homomorphic Encryption Scheme [Ref: 2]

The implementation of Paillier homomorphic encryption (HE) scheme in Java as an API and analyze existing Pailler HE libraries and discuss their limitations then it explains the design a comparatively accomplished and efficient Pailler cryptosystem.

2.3 Implementation of Authenticated and Secure Online Voting System [Ref: 4]

It explains the creation of a voting system by providing a cost effective solution to the government along with ensuring non-traceability and integrity of the votes cast while providing great convenience to voters.

2.4 A Secure Verifiable Ranked Choice Online Voting System Based on Homomorphic Encryption [Ref: 1]

Ranked choice online voting system, which addresses some challenges in online voting. And it eliminates all hardwired restrictions on the possible assignments of points to different candidates according to the voters' personal preferences in order to protect the confidentiality of the votes, each cast ballot is encrypted using the exponential ElGamal cryptosystem before submission.

2.5 Passwords are dead Alternative authentication methods [Ref: 6]

It states that instead of requiring users to remember static login credentials, the one-time authentication scheme is deployed server side and communicated to the client requiring authentication.

2.6 A New Lightweight Symmetric Searchable Encryption Scheme for String Identification [Ref: 7]

It explains the details about an efficient and easy-to-implement symmetric searchable encryption scheme (SSE) for string search, which takes one round of communication, O(n) times of computations over n documents. Unlike previous schemes, it use hash-chaining instead of chain of encryption operations for index generation and encryption.

2.7 Homomorphic Tallying for the Estonian Internet Voting System Software Technology and Applications [Ref: 5]

The feasibility of using homomorphic tallying in the Internet voting system and it analyzes the security benefits provided by homomorphic tallying, the costs introduced and the required changes to the voting system it find that homomorphic tallying has several security benefits, such as improved ballot secrecy, public verifiability of the vote tallying server and the possibility for observers to recalculate the tally without compromising ballot secrecy.

2.8 Practical applications of homomorphic encryption [Ref: 8]

It provide a theoretical overview of various encryption techniques, namely those that range from changes in the position of a letter or word, to word transformations and transposition It may also include computer algorithms that have binary functions, which produce coding of a message.

2.9 A verifiable ranked choice internet voting system [Ref: 9]

Cryptography forms part of the science known as cryptology, which is comprised of two major fields: crypto-analysis and cryptography. The term cryptology comes from the Greek word criptos (hidden) and logos, which in this case means treatment.

2.10 A flexible e-voting scheme for debate tools [Ref: 10]

A flexible e-voting system for online discussion forums was proposed in where it was assumed that there is a trusted third party (registration server) it presented two diagrams with line graphs comparing only the time of the encryption operations.

2.11 A hybrid approach to vector-based homomorphic tallying remote voting [Ref: 11]

It contains three diagrams with line graphs representing the new experiments and comparing them with the results of for elections with various numbers of voters.

2.12 A threeballot-based secure electronic voting system [Ref: 12]

The study of electronic elections contributes to the more general area of privacy-preservation and relies on secure implementations of other aspects involved in e-voting.

CHAPTER 3

SYSTEM DESIGN

3.1 ARCHITECTURE

In this section, the architectural diagram of the e-voting system is presented. Since the system deals with many phases and process, the architecture of the system is presented in the section 3.1. The phases are explained after this section.

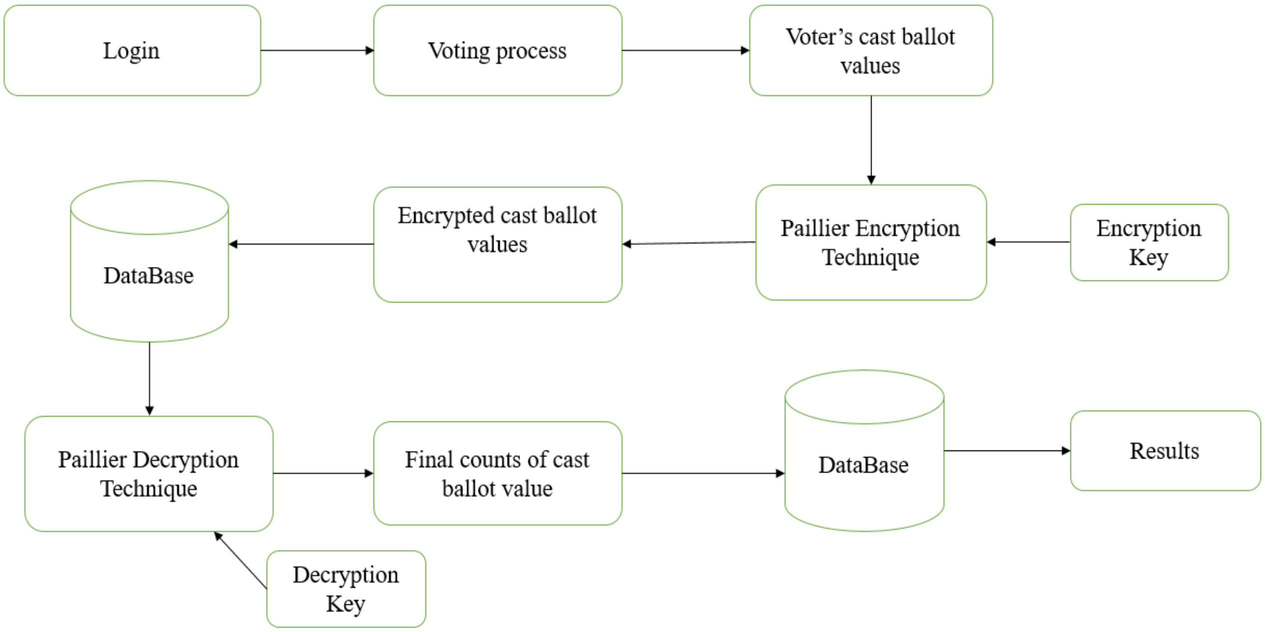

Login
Voting process
Voter's cast ballot values
DataBase
Encrypted cast ballot values
Paillier Encryption Technique
Encryption Key
Paillier Decryption Technique
Final counts of cast ballot value
DataBase
Results
Decryption Key

Figure 3.1 Architecture of proposed e-voting system

3.2 SYSTEM ANALYSIS

3.2.1 Login

In this system the voter must be an authorized person which means he must be signed up with details in the system. Voter must be an authorized person then only he can eligible to vote. The voter id and password is used for login process. After login the voter will allowed to vote.

3.2.2 Voting process

This is the major phase of our project the voter should allowed to vote for their desired candidate. The voter can choose the any one of the candidates from the list. It plays a vital role in the system. Once select the candidate, voter can submit their vote.

3.2.3 Voter's cast ballot value

Cast ballot is nothing but the small piece of box which contains the vote. This is the output of the voting process phase. It contains the vote value of the voter. This will be going to encrypt in the next phase.

3.2.4 Encryption key

An encryption key is typically a random string of bits generated specifically to scramble and unscramble data. Encryption keys are created with algorithms designed to ensure that each key is unique and unpredictable. The longer the key constructed this way, the harder it is to break the encryption code.

3.2.5 Paillier encryption technique

The Paillier cryptosystem, is a probabilistic asymmetric algorithm for public key cryptography. The problem of computing *n*-th residue classes is believed to be computationally difficult. It is the algorithm which is used to encrypt the vote value. It uses two public keys to encrypt the vote value. It produces the encrypted vote value with the help of two public keys.

3.2.6 Encrypted cast ballot value

It is the encrypted cast ballot which contains the encrypted vote values. It is the output of the last phase. The vote values are encrypted by paillier encryption technique.

3.2.7 Database

A database is an organized collection of data, generally stored and accessed electronically from a computer system. Here it stores the vote values which is encrypted. It supports storage and manipulation the data.

3.2.8 Decryption key

Decryption key is the code that you need to transform an encrypted message, document, or other data into a form that can be freely read (is decrypted). Security Management. Private keys are called decryption key in paillier cryptosystem

3.2.9 Paillier decryption technique

Decryption is used for un-encrypting the data with keys or algorithm. Cryptography uses the decryption technique to obtain the original value. Using the paillier decryption technique the encrypted vote value is decrypted with the help of two private keys.

3.2.10 Final count of cast ballot values

It is the final phase of the e-voting system. It count the all ballot values and get the vote values of every candidates. It count the all decrypted values in the database. It contains the results of the election.

3.2.11 Results

The winner of the election is announced according to the final counts. The winner candidate name should be declared in this process.

CHAPTER 4

SYSTEM REQUIREMENTS

4.1 HARDWARE UTILIZED

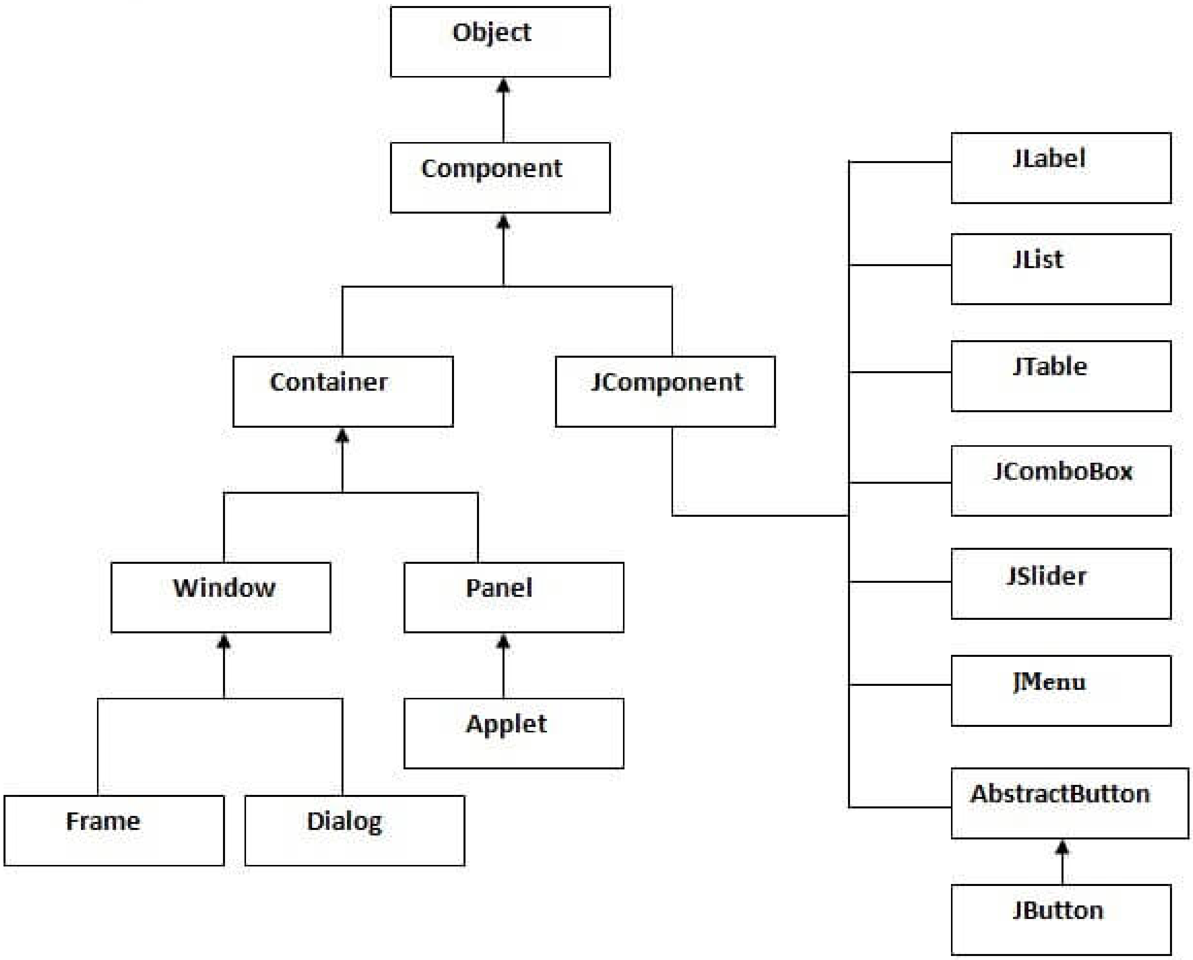
Processor	: Any processor above 2.00GHz
RAM	: 4 GB
Hard Disk	: 10 GB
Input Device	: Standard Keyboard, Mouse
Output Device	: VGA Monitor

4.2 SOFTWARE UTILIZED

- Java Swing
- XAMPP
- MySQL
- Apache Server
- NetBeans 10.0

4.3 JAVA SWING

Swing is a GUI widget toolkit for Java. It is part of Oracle's Java Foundation Classes (JFC) – an API for providing a graphical user interface (GUI) for Java programs. Swing was developed to provide a more sophisticated set of GUI components than the earlier Abstract Window Toolkit (AWT). Swing provides a look and feel that emulates the look and feel of several platforms, and also supports a pluggable look and feel that allows applications to have a look and feel unrelated to the underlying platform. It has more powerful and flexible components than AWT. In addition to familiar components such as buttons, check boxes and labels, Swing provides several advanced components such as tabbed panel, scroll panes, trees, tables, and lists. Unlike AWT components, Swing components are not implemented by platform-specific code. Instead, they are written entirely in Java and therefore are platform-independent. The term "lightweight" is used to describe such an element.



4.3.1 The hierarchy of java swing

4.4 XAMPP

XAMPP is a free and open-source cross-platform web server solution stack package developed by Apache Friends, consisting mainly of the Apache HTTP Server, MariaDB database, and interpreters for scripts written in the PHP and Perl programming languages. Since most actual web server deployments use the same components as XAMPP, it makes transitioning from a local test server to a live server possible. XAMPP's ease of deployment means a WAMP or LAMP stack can be installed quickly and simply on an operating system by a developer. With the advantage a number of common add-in applications such as Word press and Joomla can also be installed with similar ease using Bitnami.

4.5 MYSQL

MySQL is free and open-source software under the terms of the GNU General Public License, and is also available under a variety of proprietary licenses. MySQL was owned and sponsored by the Swedish company MySQL AB, which was bought by Sun Microsystems (now Oracle Corporation). In 2010, when Oracle acquired Sun, Widenius forked the open-source MySQL project to create MariaDB. MySQL is a component of the LAMP web application software stack (and others), which is an acronym for Linux, Apache, MySQL, Perl/PHP/Python. MySQL is used by many database-driven web applications, including Drupal, Joomla, phpBB, and Word Press. MySQL is also used by many popular websites, including Google (though not for searches), Facebook, Twitter, Flickr, and YouTube.

4.6 APACHE SERVER

The Apache HTTP Server, colloquially called Apache is free and open-source cross-platform web server software, released under the terms of Apache License 2.0. Apache is developed and maintained by an open community of developers under the auspices of the Apache Software Foundation. The vast majority of Apache HTTP Server instances run on a Linux distribution, but current versions also run on Windows and a wide variety of Unix-like systems. Past versions also ran on OpenVMS, NetWare, OS/2 and other operating systems.

4.7 NETBEANS

NetBeans is an integrated development environment (IDE) for Java. NetBeans allows applications to be developed from a set of modular software components called modules. NetBeans runs on Windows, macOS, Linux and Solaris. In addition to Java development, it has extensions for other languages like PHP, C, C++, HTML5, and JavaScript. Applications based on NetBeans, including the NetBeans IDE, can be extended by third party developers. The NetBeans Platform is a framework for simplifying the development of Java Swing desktop applications. The NetBeans IDE bundle for Java SE contains what is needed to start developing NetBeans plugins and NetBeans Platform based applications; no additional SDK is required. Applications can install modules dynamically. Any application can include the Update Center module to allow users of the application to download digitally signed upgrades and new features directly into the running application. Reinstalling an upgrade or a new release does not force users to download the entire application again.

CHAPTER 5

PAILLIER CRYPTOSYSTEM

In this chapter we will see the paillier encryption and decryption techniques, key generation of public keys and private keys and algorithms for encryption and decryption techniques.

5.1 INTRODUCTION

The Paillier cryptosystem, invented by and named after Pascal Paillier in 1999, is a probabilistic asymmetric algorithm for public key cryptography. The problem of computing *n*-th residue classes is believed to be computationally difficult. The decisional composite residuosity assumption is the intractability hypothesis upon which this cryptosystem is based.

5.1.1 Key Generation

1. Choose two large prime numbers *p* and *q* randomly and independently of each other such that gcd (pq, ((p-1) (q-1))). This property is assured if both primes are of equal length.
2. Compute n=pq and λ=lcm (p-1, q-1).Lcm means least common measure.
3. Select random integer g where gϵ Z*n^2.
4. Ensure n divides the order of g by checking the existence of the following modular multiplicative inverse: μ=(L(g pow λ mod n^2))^-1 mod n. where,

   L(x) = x-1/n
5. The Public keys are (n, g) which is used in encryption.
6. The Private Keys are (λ, μ) which is used in decryption.

5.1.2 Paillier Encryption

1. Let m be a message to be encrypted where 0 <= m <= n.
2. Select random integer r where 0 < r < n
3. Compute Cipher text as : c= (g^m . r^n) mod n^2

   Where,

   g = public key,

   m = message,

   r = random integer number,

   n = public key.

5.1.3 Paillier Decryption

1. Let c be the cipher text to decrypt, where c ϵ Z*n^2.
2. Compute the plaintext message as: m=L(c^ λ mod n^2) .µ mod n

   Where,

   L (x) = (x-1) / n,

   λ and µ = private key

CHAPTER 6

PROPOSED E-VOTING SYSTEM

6.1 DATA FLOW DIAGRAM

A data-flow diagram (DFD) is a way of representing a flow of a data of a process or a system (usually an information system) The DFD also provides information about the outputs and inputs of each entity and the process itself. A data-flow diagram has no control flow, there are no decision rules and no loops. Specific operations based on the data can be represented by a flowchart. The data-flow diagram is part of the structured-analysis modelling tools. A special form of data-flow plan is a site-oriented data-flow plan. Data-flow diagrams can be regarded as inverted Petri nets, because places in such networks correspond to the semantics of data memories.

6.2 LEVELS OF DFD

Level 0

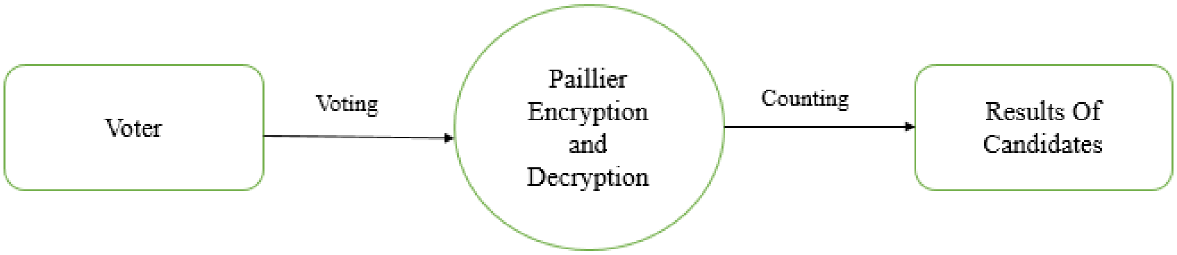


Fig 6.1 Level 0 DFD

Authorized users allow to voting in the system. After finish the voting process. The vote value will be encrypted by using paillier encryption technique. The encrypted value will be stored in the local database. The encrypted vote value will be decrypted after all voter submit their vote. Finally the vote values are decrypted and count the vote values. Based on the vote value the winner candidate should be selected.

Level 1

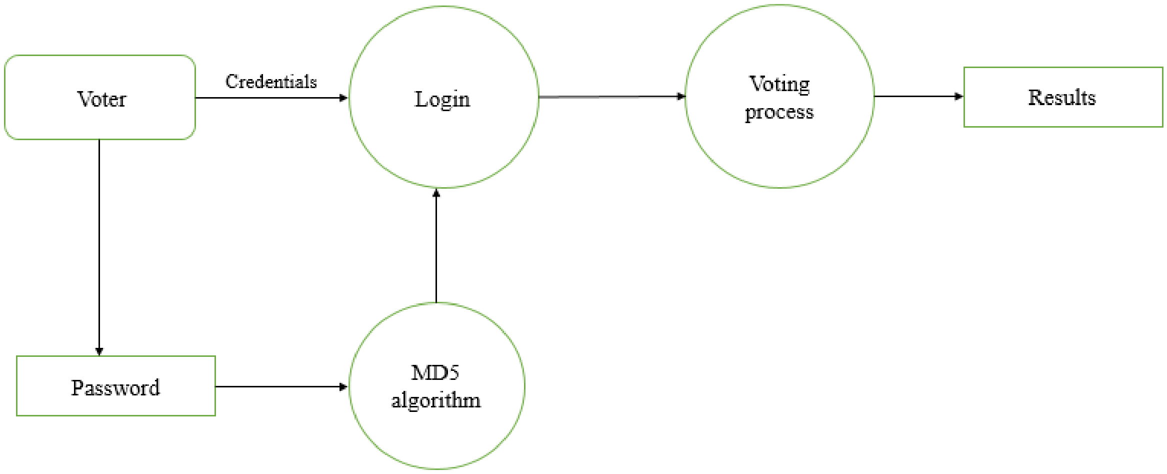
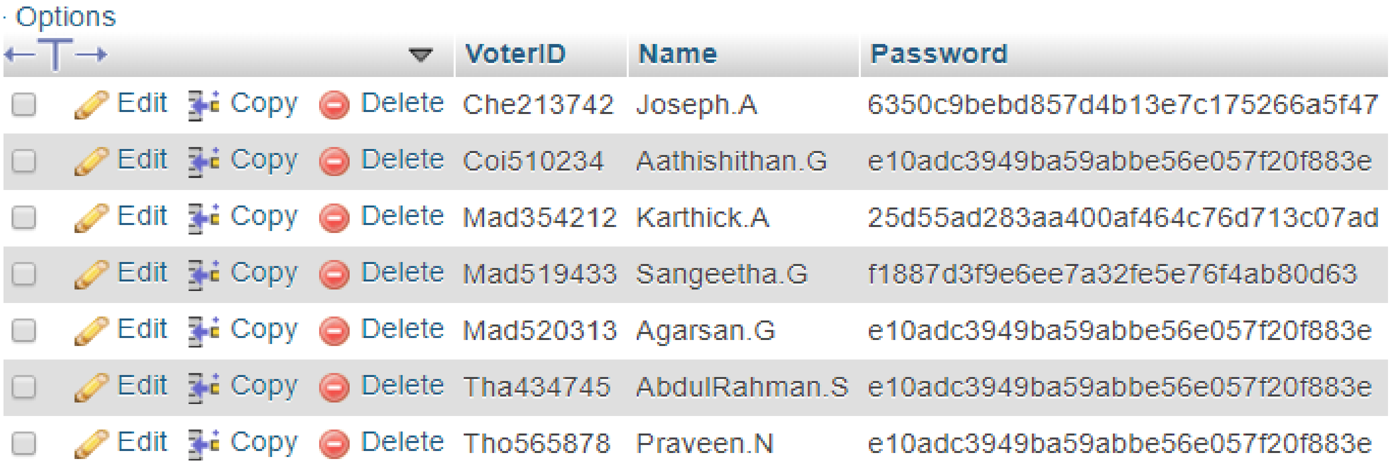


Fig 6.2 Level 1 DFD

Every voter have unique voter id and password for login. Voter id will be automatically generated by the system when user signup. The voter id is necessary to login. Password is created by user. When password is created, that will be encrypted using md5 algorithm. The encrypted password will stored in the database. Because of security purpose the passwords are encrypted using md5 algorithm. When login, the given password should encrypted and compare with the existing encrypted password, if the password matched the use will allowed to vote otherwise the voter can't to login.

The authorized voter can only allow to vote. The voter can sign up with their details. Based on the signup details the voter id should be automatically generated. Voter must login with their unique voter id.



Options

←T→			▼	VoterID	Name	Password
□	Edit	Copy	Delete	Che213742	Joseph.A	6350c9bebd857d4b13e7c175266a5f47
□	Edit	Copy	Delete	Coi510234	Aathishithan.G	e10adc3949ba59abbe56e057f20f883e
□	Edit	Copy	Delete	Mad354212	Karthick.A	25d55ad283aa400af464c76d713c07ad
□	Edit	Copy	Delete	Mad519433	Sangeetha.G	f1887d3f9e6ee7a32fe5e76f4ab80d63
□	Edit	Copy	Delete	Mad520313	Agarsan.G	e10adc3949ba59abbe56e057f20f883e
□	Edit	Copy	Delete	Tha434745	AbdulRahman.S	e10adc3949ba59abbe56e057f20f883e
□	Edit	Copy	Delete	Tho565878	Praveen.N	e10adc3949ba59abbe56e057f20f883e

Fig 6.3 Encrypted Password Using MD5

The above fig 6.2.3 explains how the password will be stored after using encryption algorithm md5.

6.2.1 MD5

The MD5 message-digest algorithm is a widely used hash function producing a 128-bit hash value. Although MD5 was initially designed to be used as a cryptographic hash function, it has been found to suffer from extensive vulnerabilities. It can still be used as a checksum to verify data integrity, but only against unintentional corruption. It remains suitable for other non-cryptographic purposes, for example for determining the partition for a particular key in a partitioned database. One basic requirement of any cryptographic hash function is that it should be computationally infeasible to find two distinct messages which hash to the same value. MD5 fails this requirement catastrophically; such collisions can be found in seconds on an ordinary home computer. The MD5 hash function was originally designed for use as a secure cryptographic hash algorithm for authenticating digital signatures.

Level 2

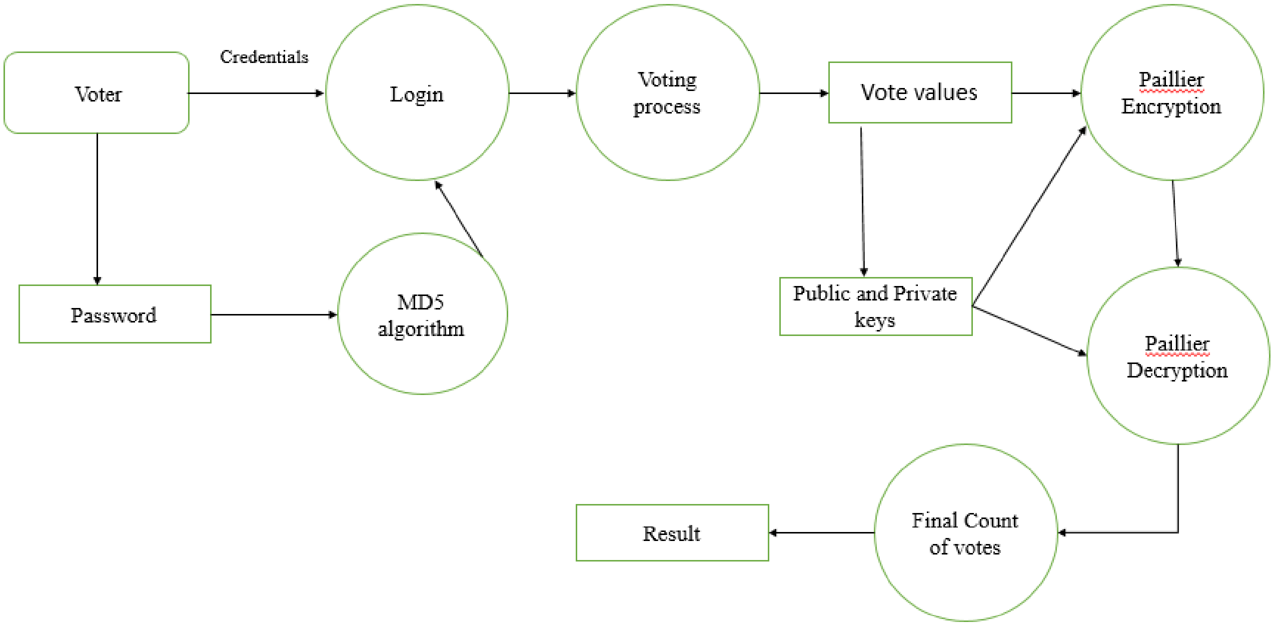


Fig 6.4 Level 2 DFD

In level 2 diagram, the paillier encryption and decryption is showed. The vote value should be encrypted by paillier encryption technique. The encrypted values stored in the local database. Once all voter submit their vote the encrypted values will be decrypted by paillier decryption technique. Publickeys are used to encrypt the vote value and private keys are used to decrypt the vote values. Finally the decrypted vote should be counted and results will be announced. Based on the algorithms the keys will be generated and it used to perform the encryption and decryption process.

CHAPTER 7

IMPLEMENTATION AND RESULTS

In this chapter, the system implementation and the results will be explained in follows.

7.1 HOME FRAME

It is the main page of the e-voting system. It contains login page for both admin and voter. Using the choices you can go to the next pages.

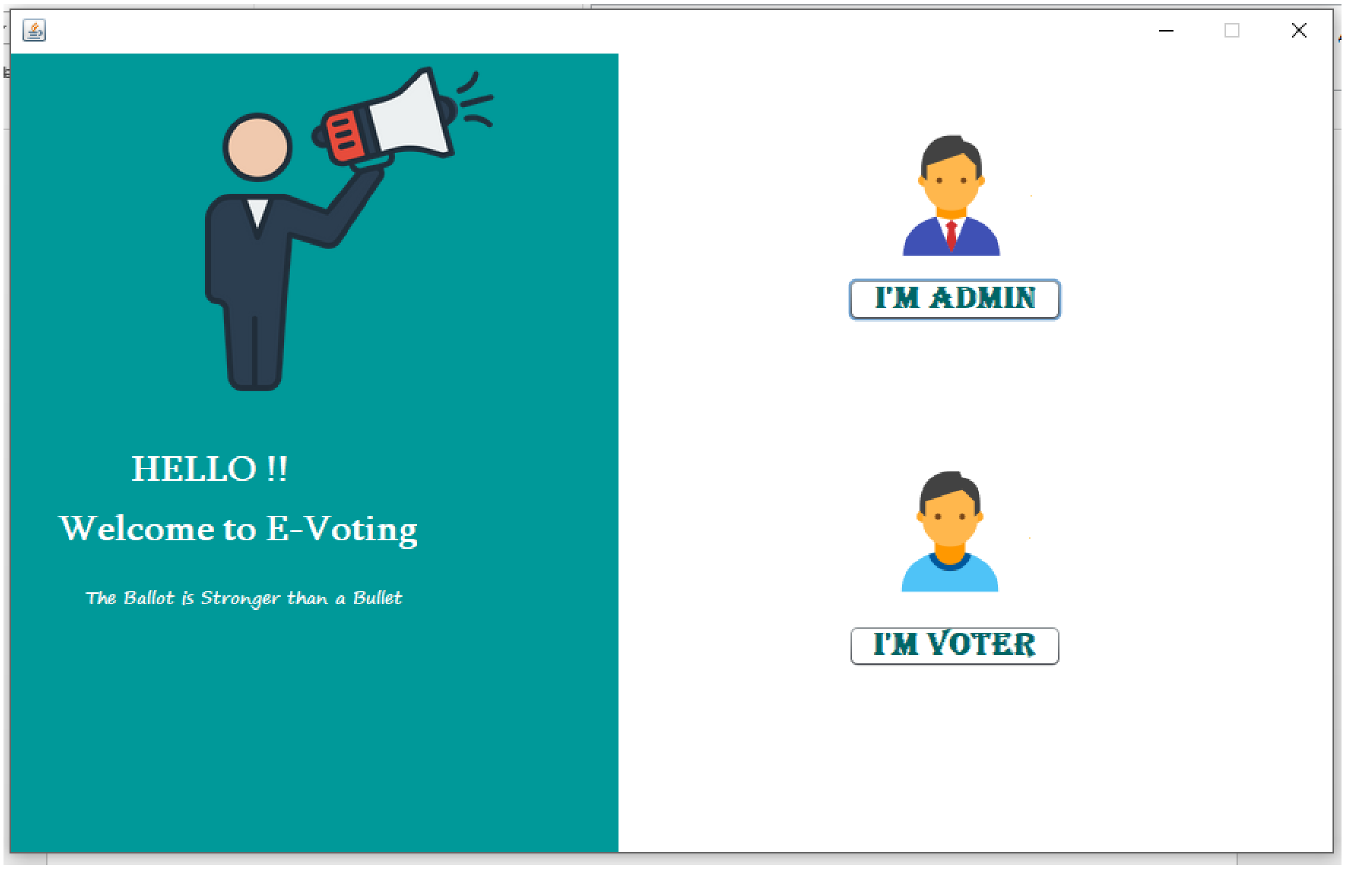


Fig 7.1 Home Frame

7.2 Login

Every voter and admin must have to login in the system. Every voter have unique id and password and every admin have unique admin id and password.

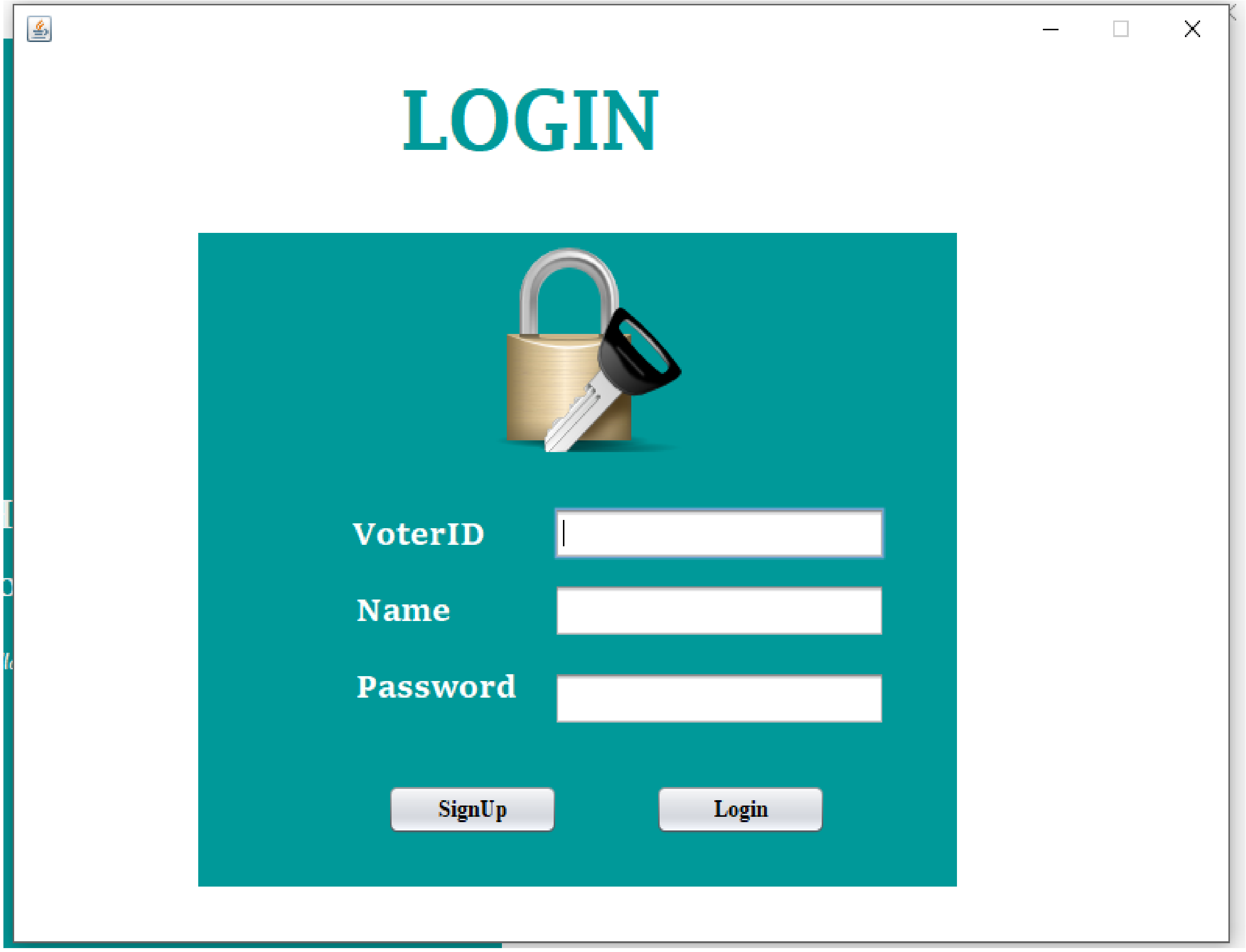
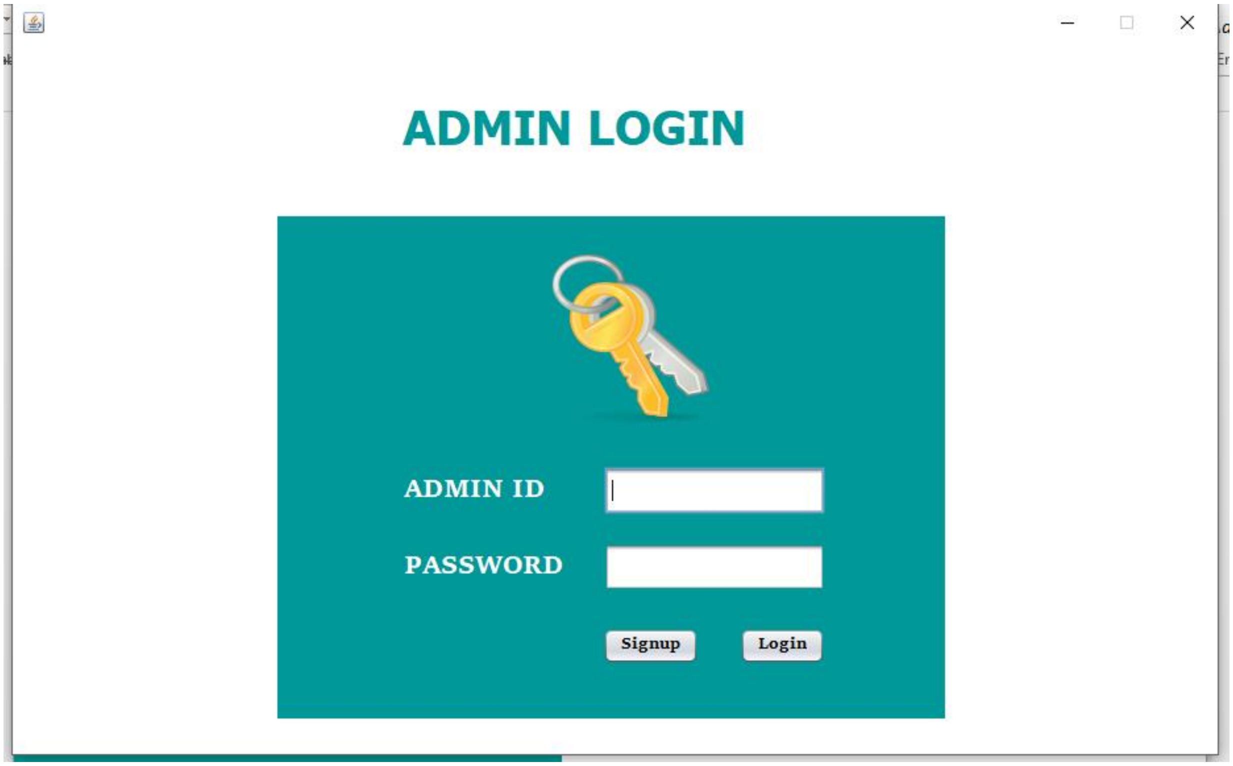


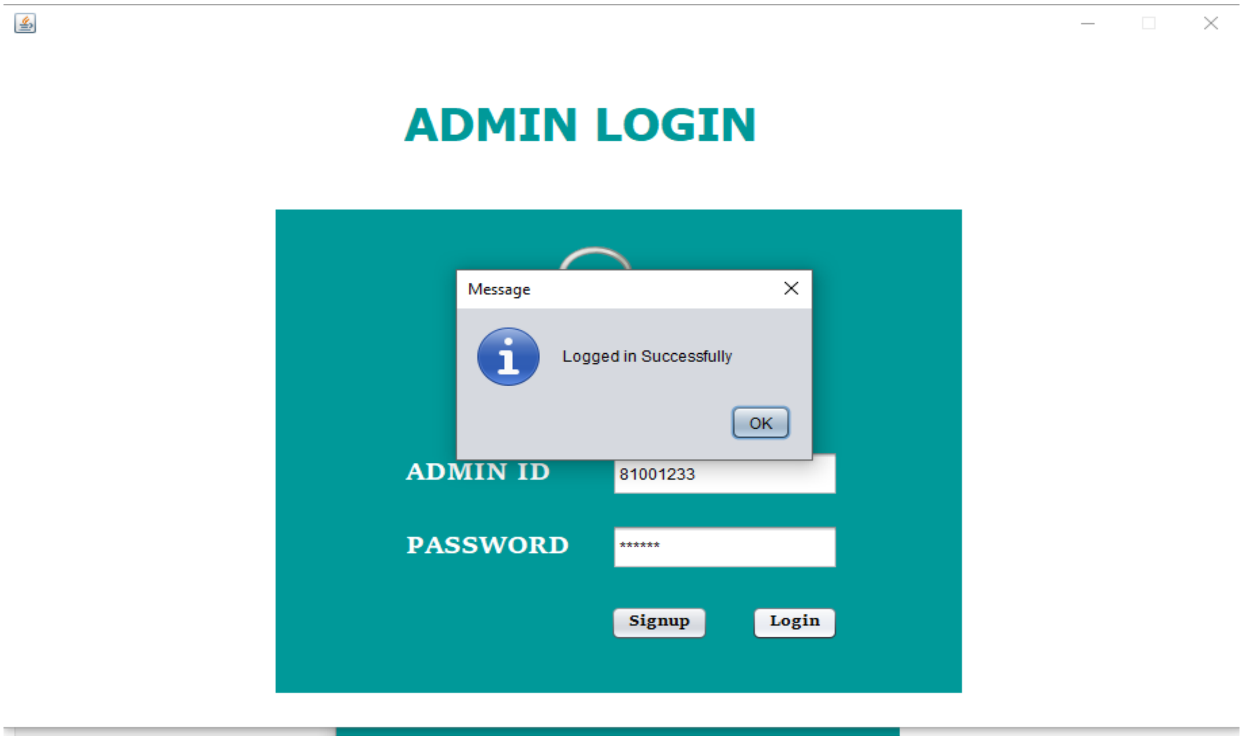
Fig 7.2 Login Frame

Voter id, name and password are the voter login attributes. Once logged in the system the voter can vote in the system.



ADMIN LOGIN

Fig 7.3 Admin Login



ADMIN LOGIN

Message

Logged in Successfully

ADMIN ID 81001233

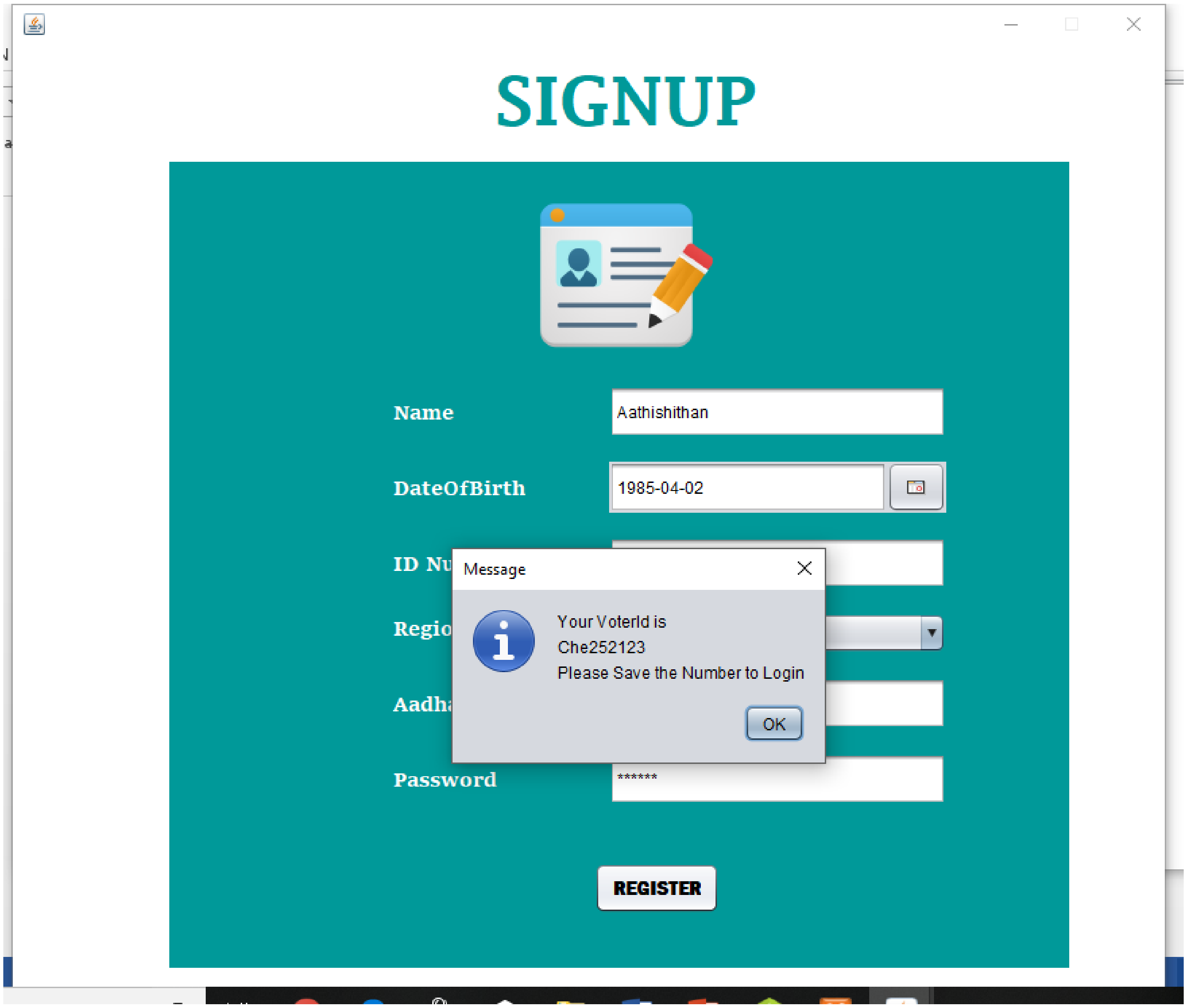
PASSWORD ******

Fig 7.4 Admin Login II

Fig 7.3 and 7.4 shows the admin login pages. If admin id and password matches admin will allow to enter the system. Admin can able to check current status, get the final results and admin can able to see vote analytics.

7.3 SIGNUP

Signup used to register the details and it will provide the voter id automatically. Admin and voter must be signup their details to login the system.



SIGNUP

Name: Aathishithan

DateOfBirth: 1985-04-02

Message

Your VoterId is
Che252123
Please Save the Number to Login

Password: ******

Fig 7.5 Signup Frame

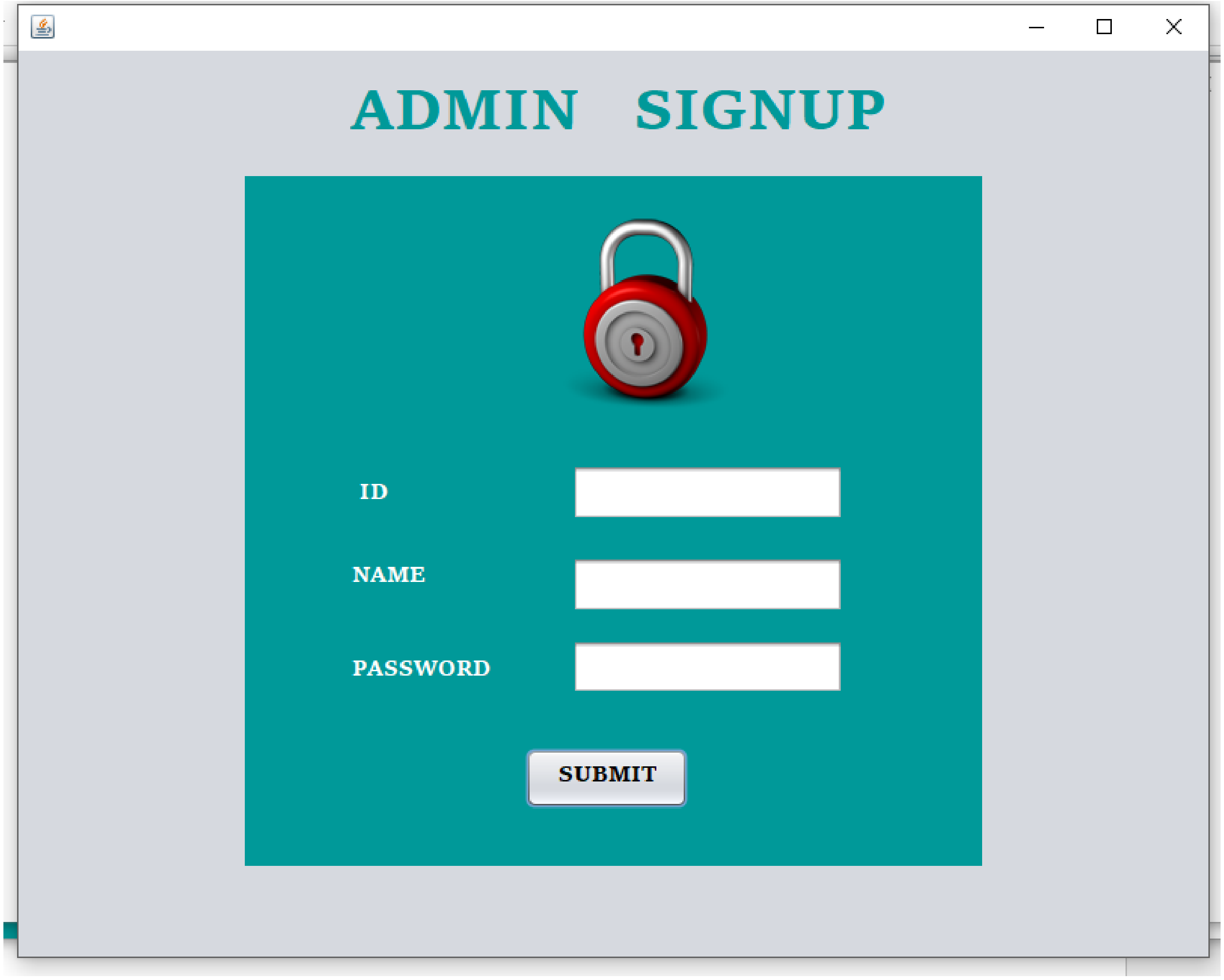
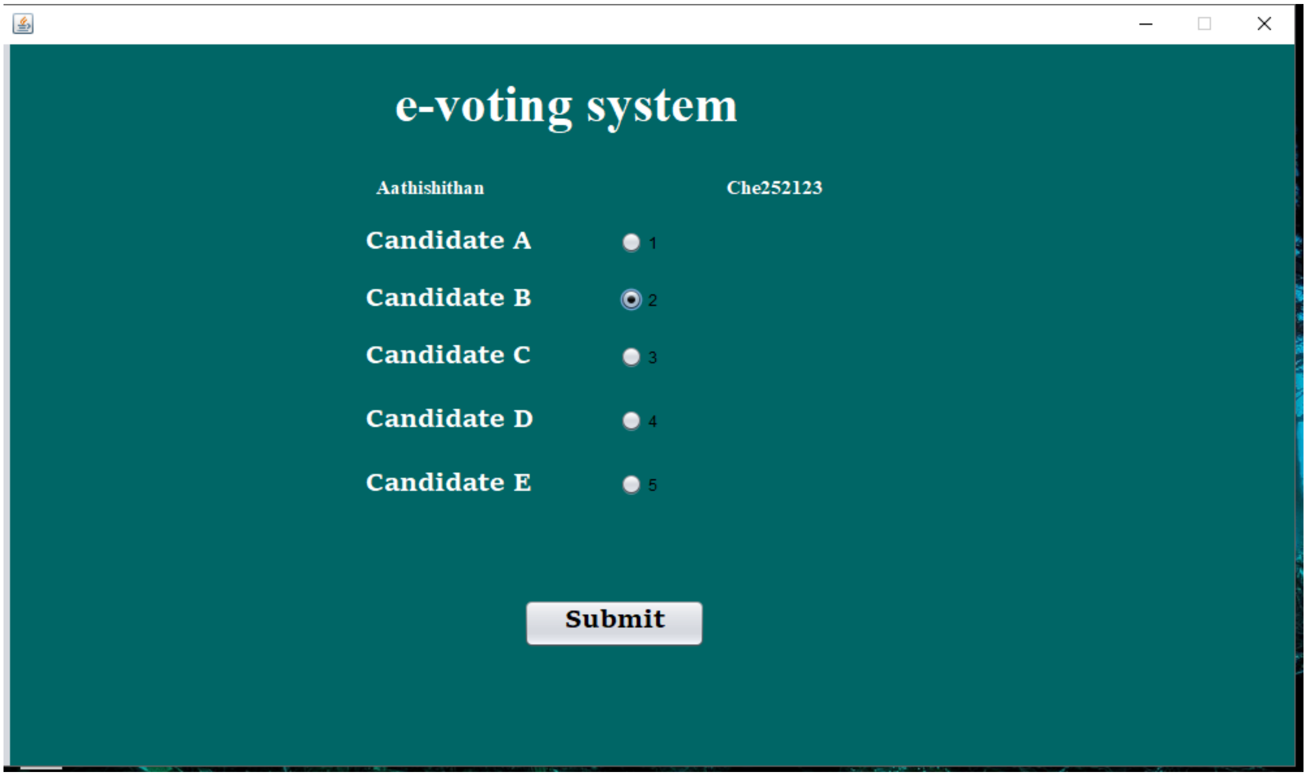


Fig 7.6 Admin Signup

7.4 VOTING PROCESS

It is the main frame of the system, the voter can vote to the candidates from this frame. The candidate names are shown in this frame the voter can choose any one of the candidate from that list and submit their vote by clicking submit button. The voter name and the voter id of the voter will display in this frame the vote value, voter name and voter id are stored in the local database. The vote value is encrypted by paillier encryption technique. Encryption performed by using the public keys. The encrypted vote value only stored in the local database.



e-voting system

Aathishithan Che252123

Candidate A ○ 1

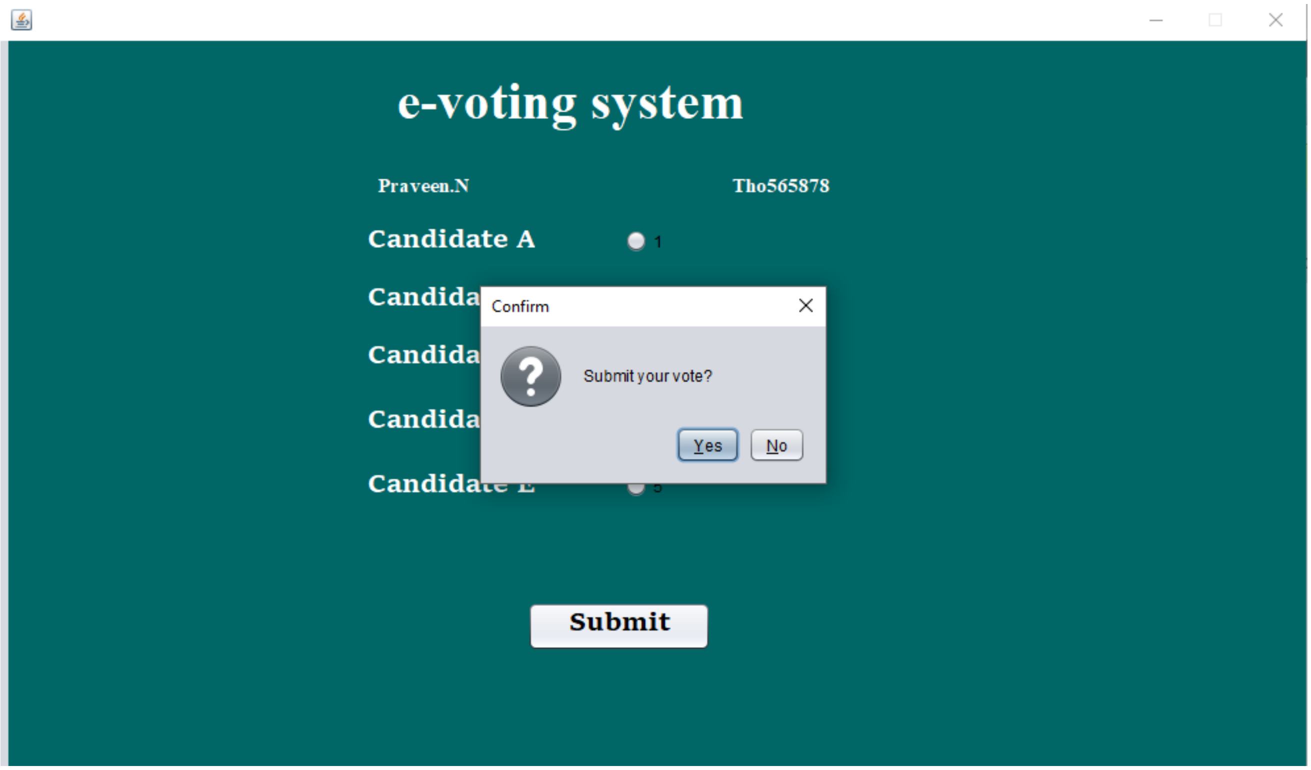
Candidate B ● 2

Candidate C ○ 3

Candidate D ○ 4

Candidate E ○ 5

Fig 7.7 Voting Frame I



e-voting system

Praveen.N Tho565878

Candidate A ○ 1

Candida

Candida

Candida

Candidate E

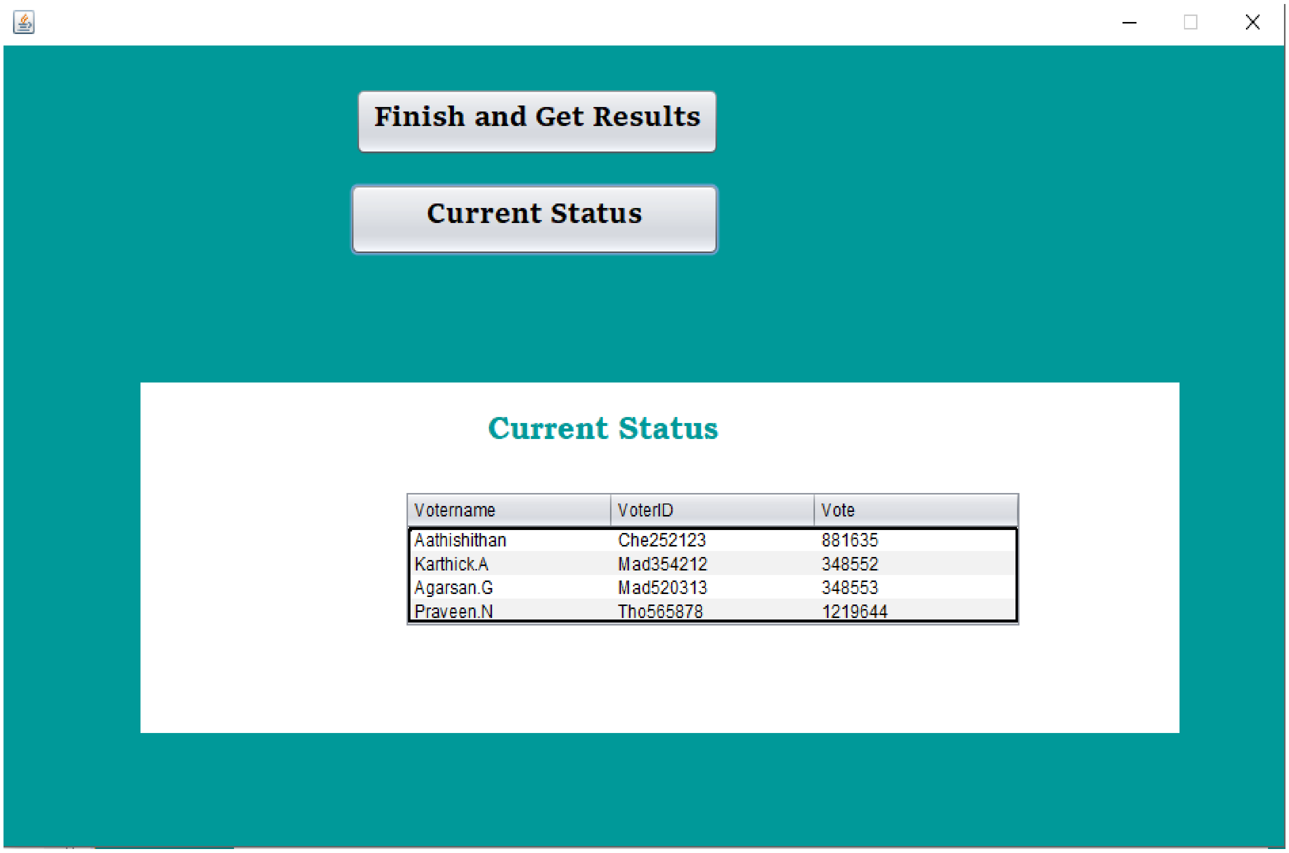
Confirm

Submit your vote?

Fig 7.8 Voting Frame II

7.5 CHECKING CURRENT STATUS

The admin can check the current status of the voting process. The admin must be logged in the system to check the current status of the voting. The table will show the current details of the voting process.



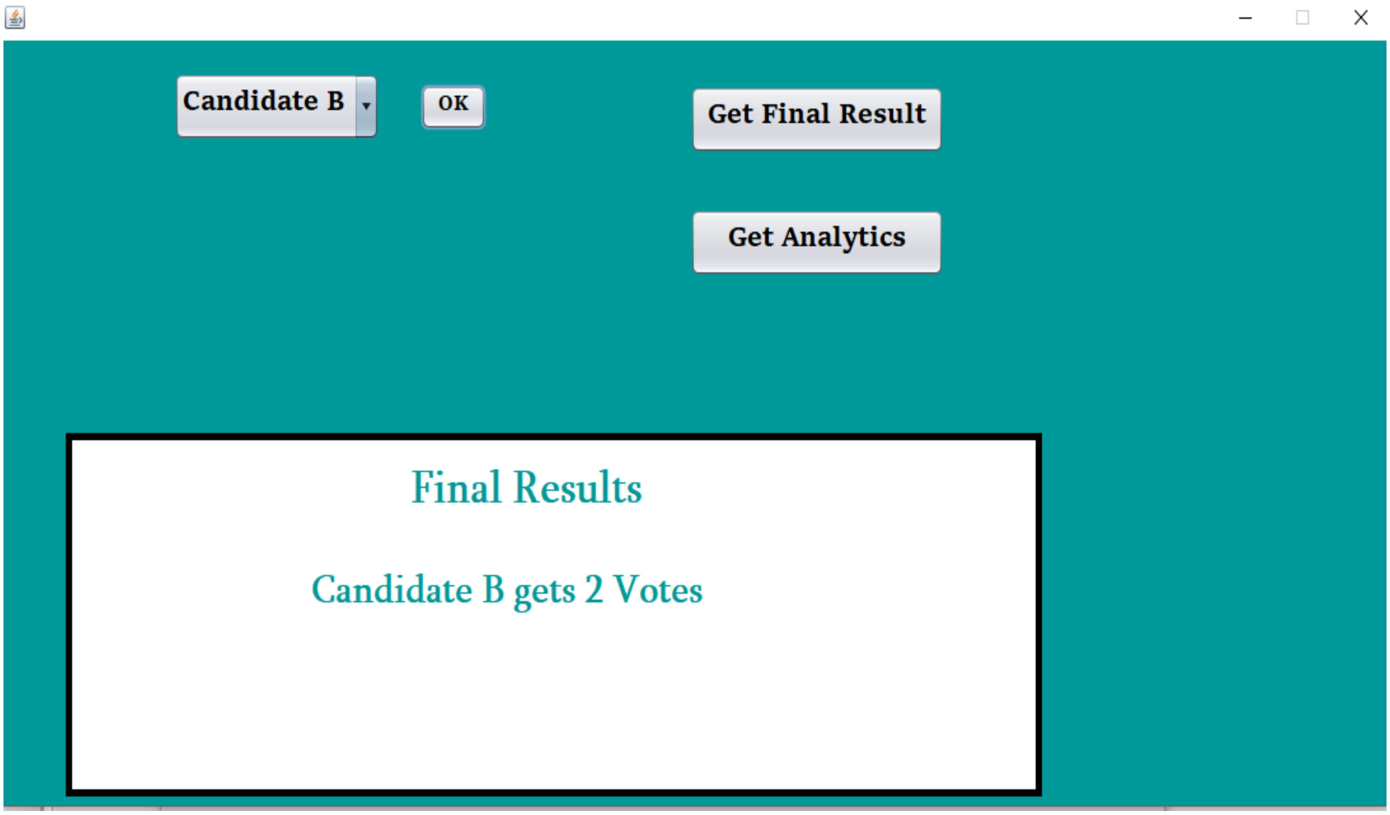
Current Status

Votername	VoterID	Vote
Aathishithan	Che252123	881635
Karthick.A	Mad354212	348552
Agarsan.G	Mad520313	348553
Praveen.N	Tho565878	1219644

Fig 7.9 Current status

7.6 RESULTS

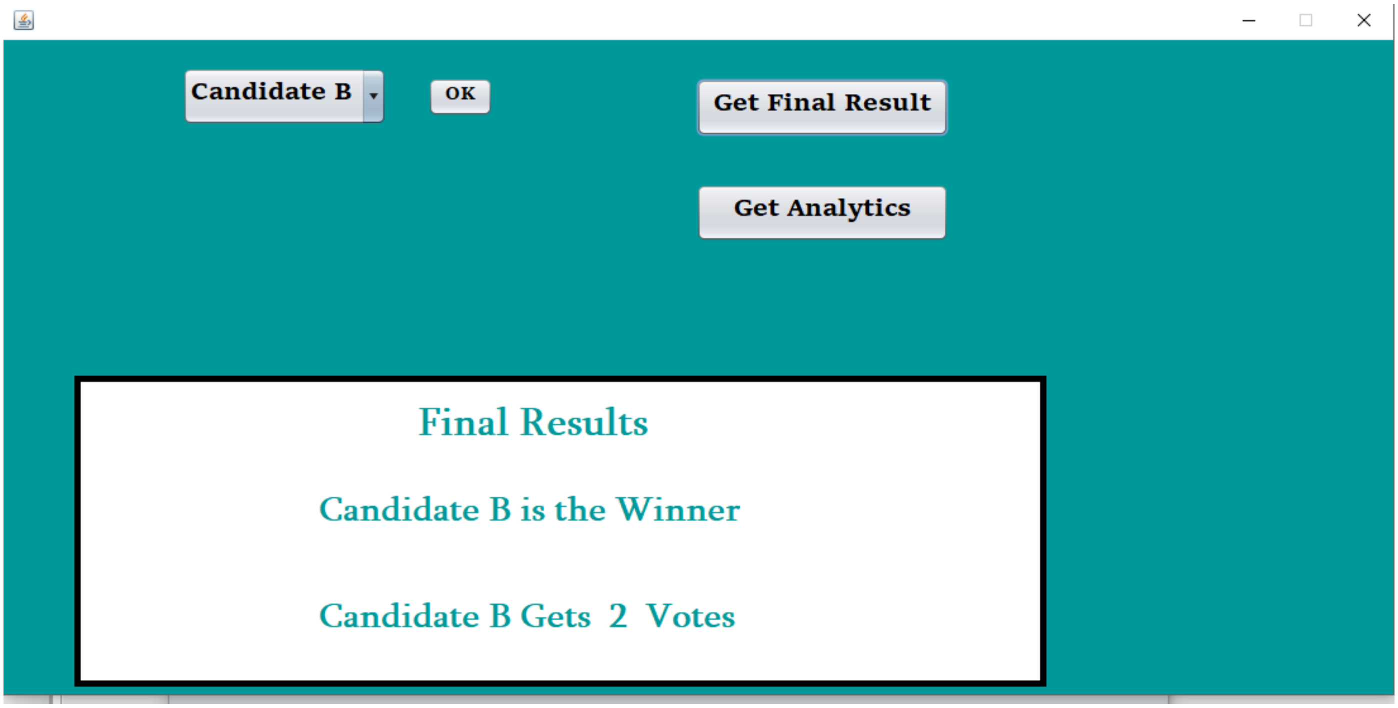
Once all voters complete the process then admin finish the election and admin can get the results of the election. The encrypted vote values are decrypted by paillier decryption technique using the private keys. The results will be display in pie charts and admin can able to see the all candidates vote counts and their percentages. The following fig explains the system briefly.



Final Results

Candidate B gets 2 Votes

Fig 7.10 Result Frame



Final Results

Candidate B is the Winner

Candidate B Gets 2 Votes

Fig 7.11 Result Frame II

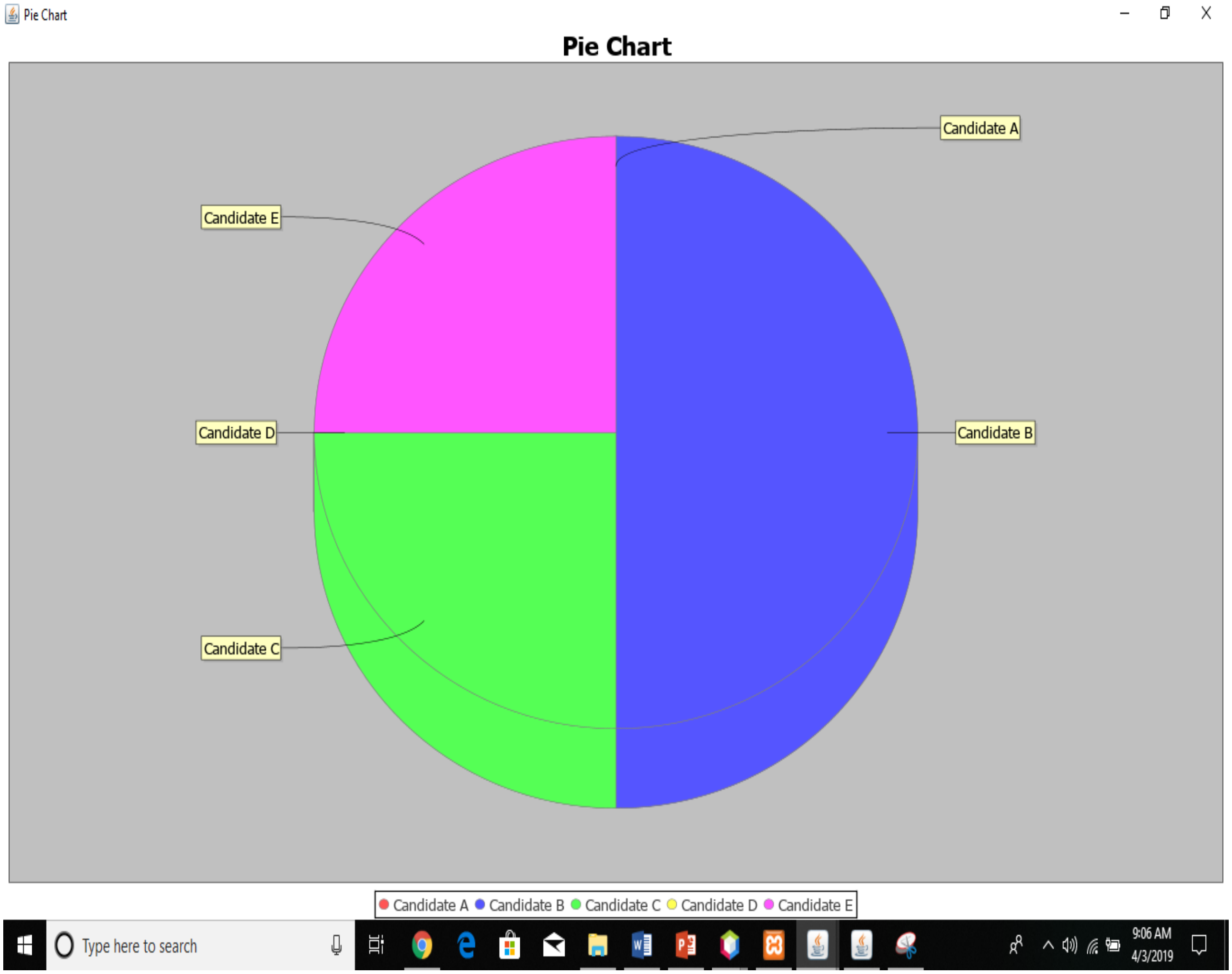


Fig 7.12 Result Pie Chart

CHAPTER 8

CONCLUSION AND FUTURE ENHANCEMENT

8.1 CONCLUSION

The committee believes that e-voting systems offer potential for voting and election management that is an improvement over what has thus far been available. However, the realization of this potential requires a commitment to this path by the nation, the states, and local jurisdictions that is not yet evident. From facilitating or enabling alternative forms of voting (e.g., absentee voting, early voting) to increasing the comprehensibility of ballots and reducing opportunities for fraud and enhancing the accuracy of vote counts, electronic voting systems of all kinds offer possibilities for greater enfranchisement of the population at large. Because electronic voting systems cannot simply replace the voting systems already deployed and in use, a commitment to this path will require innovative and dynamic methods to develop, implement, and improve comprehensive electronic voting solutions rather than just individual components.

Further, this commitment must be understood as an ongoing effort that includes support for a new national research process, with research laboratories at the national, regional, or state levels; the implementation of research and development efforts to resolve the security and usability issues associated with existing and new election technologies; a lasting commitment to open and dynamic standards, testing, and certification efforts for election technologies; and ongoing efforts to educate election officials, poll workers, voters, and the general public about these new election technologies.

8.2 FUTURE ENHANCEMENT

In future, the proposed system can be extended to end to end verification which means End-to-end auditable or end-to-end voter verifiable (E2E) systems are voting systems with stringent integrity properties and strong tamper resistance. E2E systems often employ cryptographic methods to craft receipts that allow voters to verify that their votes were counted as cast, without revealing which candidates were voted for. As such, these systems are sometimes referred to as receipt-based systems. This would make the system transparent and makes more trustability on the e-voting system. Another enhancement to the system is increase the security by using fingerprint scanner. It will enhance the system to more secure. These are the future work of our e-voting system.

APPENDIX A
SOURCE CODE

PAILLIER ENCRYPTION AND DECRYPTION

```
import java.util.*;

import java.math.BigInteger;

import java.util.Random;

class PaillierEncryptionn{

        private static BigInteger p,q;  //two prime numbers

        private static BigInteger n,g; //publickeys

        private static BigInteger temp;

        private static BigInteger m;

        private static BigInteger value1,value2;

        private static BigInteger c,r;

        private static BigInteger lamda,mu; //privatekeys

public static void publickey(){

        Random rand = new Random();


   p= new BigInteger(14,rand);


   q= new BigInteger(14,rand);
   p=prime(p);
   q=prime(q);
   n=p.multiply(q);

temp=(p.subtract(BigInteger.valueOf(1))).multiply(q.subtract(BigInteger.valueOf(1)));
     if(gcd(n,temp).compareTo(BigInteger.valueOf(1))==0){
        System.out.println(p+" "+q);
       }
       else{
           System.out.println("You need to get different prime numbers");
                   System.exit(1);
          }
         g=new BigInteger(5,rand);
                     System.out.println("publickeys:");
                     System.out.println("n:"+n+" g:"+g);
 }

public static void encryption(){
          Scanner scn=new Scanner(System.in);
          System.out.println("Enter the vote value: ");
    m=scn.nextBigInteger();
          Random rand = new Random();
          value1=compute(g,m);
          r=new BigInteger(5,rand);
          value2=compute(r,n);
          c=(value1.multiply(value2)).mod(n.multiply(n));
          System.out.println(c);
}
public static void privatekey(){
          lamda=lcm(p.subtract(BigInteger.valueOf(1)),q.subtract(BigInteger.valueOf
(1)));
          mu=compute(g,lamda);
          mu=mu.mod(n.multiply(n));
          mu=(mu.subtract(BigInteger.valueOf(1))).divide(n);
          mu=mu.modPow(BigInteger.valueOf(-1),n);
          System.out.println("Privatekeys: ");
          System.out.println("lamda:"+lamda+" mu:"+mu);


}
public static void decryption(){
```

```
          //value1=BigInteger.valueOf(0);

          //value2=BigInteger.valueOf(0);

          value1=compute(c,lamda);

          value1=(value1).mod(n.multiply(n));

          value1=(value1.subtract(BigInteger.valueOf(1))).divide(n);

          value2=(mu).mod(n);

          m=(value1).multiply(value2);

    System.out.println("ANS:"+m);

}


public static BigInteger prime(BigInteger num){

          Random rand = new Random();

          if(num.isProbablePrime(1))

                    return num;

          return prime(num= new BigInteger(5,rand));

}


public static BigInteger gcd(BigInteger num1,BigInteger num2){

          if(num2.compareTo(BigInteger.valueOf(0))==0)

                    return num1;
          return gcd(num2,num1.remainder(num2));


}


public static BigInteger lcm(BigInteger num1,BigInteger num2){

          BigInteger temp1=num1.multiply(num2);

          BigInteger  temp2=gcd(num1,num2);

          BigInteger  ans=temp1.divide(temp2);

          return ans;

}


public static BigInteger compute(BigInteger num1,BigInteger num2){

          Integer number=num2.intValue();

          return (num1.pow(number));

}


public static void main(String args[]){

  publickey();

  privatekey();

  encryption();decryption();}}
```

REFERENCES

[1] Xuechao Yang ; Xun Yi ; Surya Nepal ; Andrei Kelarev ; Fengling Han , "A Secure Verifiable Ranked Choice Online Voting System Based on Homomorphic Encryption," IEEE Access,volume 6.

[2] Radjab Harerimana, Syh-Yuan Tan, Wei-Chuen Yau, "A Java Implementation Of Paillier Homomorphic Encryption Scheme," FIFTH International Conference on Information and Communication Technology, 2017.

[3] Tanyaporn Sridokmai ,Somchai Prakancharoen, "The Homomorphic Other Property of Paillier Cryptosystem," in International Conference on Science and Technology 2015, RMUTT.

[4] Srivatsan Sridharan, "Implementation of Authenticated and Secure Online Voting System",IEEE - 31661

[5] Arnis Parsovs, "Homomorphic Tallying for the Estonian Internet Voting SystemSoftware Technology and Applications", Competence Centre, Estonia, August 3, 2016.

[6] Michael Bachmann "Passwords are dead Alternative authentication methods", 2014 IEEE Joint Intelligence and Security Informatics Conference.

[7] Indranil Ghosh Ray, Yogachandran Rahulamathavan and Muttukrishnan Rajarajan, “A New Lightweight Symmetric Searchable Encryption Scheme for String Identification”, IEEE Transaction on Cloud Computing.

[8] K. E. Lauter, “Practical applications of homomorphic encryption,” in Proc. 2012 ACM Workshop on Cloud Computing Security. ACM, 2012, pp. 57–58.

[9] X. Yang, X. Yi, C. Ryan, R. van Schyndel, F. Han, S. Nepal, and A. Song, “A verifiable ranked choice internet voting system,” in Int. Conf. Web Information Systems Engineering, WISE 2017. Springer, 2017, pp. 490–501.

[10] D. A. Lopez Garcia, “A flexible e-voting scheme for debate tools,” Computers & Security, vol. 56, pp. 50–62, 2016.

[11] V. Mateu, J. M. Miret, and F. Sebe, “A hybrid approach to ´ vector-based homomorphic tallying remote voting,” Int. J. Info. Security, vol. 15, no. 2, pp. 211–221, 2016.

[12] A. O. Santin, R. G. Costa, and C. A. Maziero, “A threeballot-based secure electronic voting system,” IEEE Security & Privacy, vol. 6, no. 3, pp. 14–21, 2008.