



## Online Secured Voting System

Project submitted to the Department of Computer Science and Engineering in the partial fulfillment of the requirement for the Degree of B.Sc.(Hons.) in CSE program

Submitted by

Jannatul Ferdous(Ananta)

Reg. ID: 17502003861

Session: 2017-18

Supervised by

Maheli Ahmed

Lecturer, Department of Computer Science and Engineering



Department of Computer Science and Engineering

College Of Technology

August 2023

# Online Secured Voting System

Submitted by

Jannatul Ferdous(Ananta)

Reg. ID: 17502003861

Supervised by

Maheli Ahmed

Submitted to the Department of Computer Science and Engineering of College  
of Technology in the partial fulfillment of the requirement for the Degree of  
B.Sc.(Hons.) in CSE

Project Evaluation Committee:

1.Supervisor .....

Maheli Ahmed

Lecturer, Department of Computer Science and Engineering

2. Member .....

3. Member .....

4. Member .....

5. Member .....

## **Project Approval**

Student Name: Jannatul Ferdous(Ananta)

Student Id: 17502003861

Thesis Title: Online Secured Voting System

We the undersigned, recommend that the project completed by the student listed above, in the partial fulfillment of the requirement for the Degree of B.Sc.(Hons.) in CSE, be accepted by the Department of Computer Science and Engineering, College Of Technology for deposit.

## **Supervisor Approval**

.....

Maheli Ahmed

## **Departmental Approval**

.....

Md. Nazmul Ahsan

Department Head, Department of Computer Science and Engineering

College Of Technology

Narayanganj, Dhaka.

## **Abstract**

Our paper deals with online voting system that facilitates user(voter), candidate and administrator (who will be in charge and will verify all the user and information) to participate in online voting. our online voting system is highly secured, and it has a simple and interactive user interface. The proposed online portal is secured and have unique security feature such as unique id generation that adds another layer of security (except login id and password) and gives admin the ability to verify the user information and to decide whether he is eligible to vote or not. It also creates and manages voting and an election detail as all the users must login by user name and password and click on candidates to register vote. Our system is also equipped with a chat bot that works as a support or guide to the voters, this helps the users in the voting process.

**Keywords:** HTML, CSS, Java Script, PHP, MYSQL, phpMyAdmin, XAMPP

# Acknowledgment

In this very special moment, first and foremost I would like to express my heartiest gratitude to the almighty God for allowing me to accomplish this B.Sc.(Hons.) study successfully. I am grateful to my respectable supervisor Maheli Ahmed, who has given me suggestions, inspiration and guidance during this research work.

I would like to thank our honorable examiners of the examination committee for their valuable comments and suggestions that helped to improve manuscript.

I am thankful to my family members for their unconditional support and encouragement. I wish to say thanks to all the teachers of Department of Computer Science and Engineering of College Of Technology.

Jannatul Ferdous (Ananta)

August, 2023

## Table of Contents

### Chapter 1

#### Introduction

1.1	Introduction .....	9
1.2	Motivation.....	9
1.3	Scope of work .....	9
1.4	Objective of the Project.....	9-10
1.5	Organization of the Project .....	10
1.6	Summary.....	10

### Chapter 2

#### Literature Review

2.1	What is Voting? .....	11
2.2	Types of Voting .....	11
2.3	How Voting is Conducted? .....	12
2.4	E-Voting System .....	13-14
2.5	Summary.....	14

### Chapter 3

#### Electronic Voting System in Current World

3.1	Introduction .....	15
3.2	Real Life Example.....	15-16
3.3	Analysis.....	16
3.4	Fact Finding .....	16-17
3.5	Attacks on Electronic Voting .....	17--18
3.6	Securing Online Voting System .....	18-20
3.6.1	Accuracy .....	18
3.6.2	Verifiability.....	18
3.6.3	Democracy.....	19
3.6.4	Privacy .....	19

3.6.5	Convenience .....	19
3.6.6	Consistency .....	19
3.6.7	Cryptographic Verification .....	19-20
3.7	Security Mechanism Can Be Maintained.....	20
3.8	How SSL Works on the internet.....	20-21
3.9	Summary.....	21

## Chapter 4

### Proposed Online EVM System with Enhanced Security

4.1	Introduction .....	22
4.2	Overview of EVM System .....	22
4.3	ER Diagram .....	23
4.4	Context Diagram .....	23
4.5	Context Diagram .....	24
4.6	Data Flow Diagram(1).....	24
4.7	Data Flow Diagram(2).....	25
4.8	Flow Chart.....	26
4.9	Algorithm .....	27
4.9.1	Definitive Standards.....	27
4.9.2	AES Rounds and Round keys .....	27-28
4.9.3	Example and Implementation .....	28
4.10	Encryption .....	28-31
4.11	Decryption .....	31-32
4.12	Summary.....	32

## Chapter 5

### Implementation

5.1	Platform Overview.....	33
5.2	System Requirement .....	33
5.3	Overview of Implemented System .....	33
5.4	Implementation of AES Algorithm in the System.....	33-35
5.5	System Code .....	35-42
5.6	Summary.....	5-2

## **Chapter 6**

### **Comparison Analysis**

6.1	Traditional Voting System V/S Online Secured Voting System .....	43
6.2	Summary .....	43
<b>Reference</b>	.....	44

## **Chapter 7**

### **Appendix**

7.1	Appendix A.....	45
7.2	Appendix B.....	46-47
7.3	Appendix C.....	48
7.4	Appendix D.....	49

## **Chapter 8**

### **Conclusion And Future work**

8.1	Conclusion .....	50
8.2	Future Modification .....	50



# Chapter 1 Introduction

## 1.1 Introduction

“ONLINE SECURED VOTING SYSTEM” is an online voting technique. In this system people who have citizenship of Bangladesh and whose age is above 18 years of age and any gender can give his\her vote going to any physical polling station. In the polling station the voting system is online. This vote doesn't store in that polling station but they are store in database. There is a database which is maintained in which all the names of voters with complete information are stored. In “ONLINE SECURED VOTING SYSTEM” a voter can use his\her voting right online without any difficulty. He\She has to be registered first for him/her to vote. Anyone can register within the admin observation. After registration, the voter is assigned a Voter ID with which he/she can use to log into the system. If invalid/wrong details are submitted, then the citizen is not registered to vote.

## 1.2 Motivation

In every election of Bangladesh violence are occurred in pooling station. Ballet box and ballet paper hijacking, vote fraud happens few or more all the time. After counting vote sometimes, the losing candidate avoid the election by making transparency of voting system. Online voting is an electronic way of choosing leaders via an online based dedicated application. The advantage of online voting over the common “Secured voting”. Since the votes aren't store In the local polling station so the security can be ensured from centrally.

## 1.3 Scope of Work

It is focused on studying the existing system of voting and to make sure that the peoples vote is counts, for fairness in the elective positions. This is also will produce:

- Less effort and less labor intensive, as the primary cost and focus primary on creating, managing, and running a secure web voting portal.
- Increasing number of voters as individuals will find it easier and more convenient to vote, especially those abroad by making a polling station in there

## 1.4 Objective of the Project

- At a times voter can give vote to a nominee. For that reason, prevention of vote fraud can be possible.
- Vote will be stored in a server in encrypted way. So, vote cannot be seen to others. It gives security to voter.

- Vote will be counted automatically. For that reason, it will not have any fault in the counting process of the result. It will give result in very short time and accurate result.
- The whole processing is in online so the additional cost for laborer, equipment and man power reduce.

## **1.5 Organization of the Project**

Chapter 1 consists of knowledge about what is online voting system and motivation about the system. Using online EVM system there is much scope like, less labor intensive, as the primary cost and focus primary on creating, managing, and running a secure web voting portal. The objective of this project is also included in chapter 1.

Chapter 2 consists of voting system. There are many types of voting. It will increase the knowledge about voting system. The way in which the voting system is conducted. There is also description about E-voting System.

Chapter 3 consists of the information about the EVM system of the current world. There is also an example of real-life system. The analysis about how an existing system is working. There is fact finding of the system, like feasibility, cost, and security.

Chapter 4 consists of overview of proposed EVM system. The technique of our work. ER diagram, DFD, algorithm, interfaces of nominee, voter, admin. The procedure of how our system will work and provide security for the system.

Chapter 5 description about the platform of our system, also the devices and server that we need to execute operation, Then, we discuss about that when a voter cast a vote the vote will be encrypted (using encryption algorithm) during transmission time the vote will be a cipher so that attacker cannot understand it. The cipher will be store in to the database then decrypt it to count result.

Chapter 6 shows the comparison between traditional voting system and ONLINE SECURED VOTING SYSTEM. It shows the efficiency and secured side of ONLINE SECURED SYSTEM.

Chapter 7 is the overview of our Whole Online Secured Voting System and also about Future Modification.

## **1.6 Summary**

This Chapter consists about our motivation like- Online voting is an electronic way of choosing leaders via an online based dedicated application. The advantage of online voting over the common voting system is “Secured voting”. This chapter also describes about scope of work like- Less effort and less labor intensive, as the primary cost and focus primary on creating, managing, and running a secure web voting portal. In this chapter the objective of our project is also described, Like- At a time a voter can give vote to a nominee. For that reason, prevention of vote fraud can be possible, Vote will be stored in a server in encrypted way. So, vote cannot be seen to others. It gives security to voter, etc. Also consists the organization of this project.

# Chapter 2 Literature

## Review

### 2.1 What is Voting?

A voting system or electoral system consists of the set of rules which must be followed for a vote to be considered valid, and how votes are counted and aggregated to yield a final result. It is a method by which voters make a choice between candidates, often in an election or on a policy referendum. Common voting systems are majority rule, proportional representation or plurality voting with a number of variations and methods such as first-past-the-post or preferential voting. The study of formally defined voting systems is called social choice theory or voting theory, a subfield of political science, economics, or mathematics. Those who are unfamiliar with voting theory are often surprised to learn that voting systems other than majority rule exist, or that disagreements exist over what it means to be supported by a majority. Depending on the meaning chosen, the common "majority rule" systems can produce results that the majority does not support. If every election had only two choices, the winner would be determined using majority rule alone. However, when there are more than two options, there may not be a single option that is most liked or most disliked by a majority. A simple choice does not allow voters to express the ordering or the intensity of their feeling. Different voting systems may give very different results, particularly in cases where there is no clear majority preference <sup>[1][2]</sup>

### 2.2 Types of Voting

- a) **Paper-Based Voting:** The voter gets a blank ballot and use a pen or a marker to indicate he want to vote for which candidate. Hand-counted ballots is a time and labor consuming process, but it is easy to manufacture paper ballots and the ballots can be retained for verifying, this type is still the most common way to vote. <sup>[2][3]</sup>
- b) **Lever Voting Machine:** Lever machine is peculiar equipment, and each lever is assigned for a corresponding candidate. The voter pulls the lever to poll for his favorite candidate. This kind of voting machine can count up the ballots automatically. Because its interface is not user-friendly enough, giving some training to voters is necessary. <sup>[2][3]</sup>
- c) **Direct Recording Electronic Voting Machine:** This type, which is abbreviated to DRE, integrates with keyboard; touch screen, or buttons for the voter press to poll.

Some of them lay in voting records and counting the votes is very quickly. But the other DRE without keep voting records are doubted about its accuracy. <sup>[2][3]</sup>

- d) **Punch Card:** The voter uses metallic hole-punch to punch a hole on the blank ballot. It can count votes automatically, but if the voter's perforation is incomplete, the result is probably determined wrongfully. <sup>[2][3]</sup>
- e) **Optical Voting Machine:** After each voter fills a circle correspond to their favorite candidate on the blank ballot, this machine selects the darkest mark on each ballot for the vote then computes the total result. This kind of machine counts up ballots rapidly. However, if the voter fills over the circle, it will lead to the error result of optical-scan. <sup>[2][3]</sup>

Recent years, a considerable number of countries has adopted E-voting for their official elections. These countries include; America, Belgium, Japan and Brazil. <sup>[2][3]</sup>

## 2.3 How Voting Is Conducted?

An electoral system specifies the form of the ballot, the set of allowable votes; and the tallying method, an algorithm for determining the outcome. This outcome may be a single winner, as in the case of a presidential election, or may result in multiple winners, such as in the election of a legislative body. The electoral system may also specify how voting power is distributed among the voters, and how voters are divided into subgroups (constituencies) whose votes are counted independently.

The real-world implementation of an election is generally *not* considered part of the voting system. For example, though a voting system specifies the ballot abstractly, it does not specify whether the actual physical ballot takes the form of a piece of paper, a punch card, or a computer display. A voting system also does not specify whether or how votes are kept secret, how to verify that votes are counted accurately, or who is allowed to vote. These are aspects of the broader topic of elections and election systems.

Different voting systems have different forms for allowing the individual to express his or her vote. In ranked ballot or "preference" voting systems, such as Instant-runoff voting, the Borda count, or a Condorcet method, voters order the list of options from most to least preferred. In range voting, voters rate each option separately on a scale. In plurality voting (also known as "first-past-the-post"), voters select only one option, while in approval voting, they can select as many as they want. In voting systems that allow "plumping", like cumulative voting, voters may vote for the same candidate multiple times.

Some voting systems include additional choices on the ballot, such as write-in candidates, none of the above option, or a no confidence in that candidate option. <sup>[2][3]</sup>

## 2.4 E-Voting System<sup>[4]</sup>

**Electronic voting** (also known as **e-voting**) is voting using electronic means to either aid or take care of the chores of casting and counting votes. Depending on the particular implementation, e-voting may encompass a range of Internet services, from basic data transmission to full-function online voting through common connectable household devices. Similarly, the degree of automation may vary from simple chores to a complete solution that includes voter registration & authentication, vote input, local or precinct tallying, vote data encryption and transmission to servers, vote consolidation and tabulation, and election administration. A worthy e-voting system must perform most of these tasks while complying with a set of standards established by regulatory bodies, and must also be capable to deal successfully with strong requirements associated with security, accuracy, integrity, swiftness, privacy, auditability, accessibility, cost effectiveness, scalability and ecological sustainability. Electronic voting technology can include punched cards, optical scan voting systems and specialized voting kiosks (including self-contained direct-recording electronic voting systems, or DRE). It can also involve transmission of ballots and votes via telephones, private computer networks, or the Internet.<sup>[2]</sup>

In general, two main types of e-Voting can be identified:

- e-voting which is physically supervised by representatives of governmental or independent electoral authorities (e.g. electronic voting machines located at polling stations);
- Remote e-voting via the internet (also called i-voting) where the voter votes at home or without going to a polling station.

Much insecurity has been found in commercial voting machines, such as using a default administration password.<sup>[6][7]</sup> Cases have also been reported of machines making unpredictable, inconsistent errors. Key issues with electronic voting are therefore the openness of a system to public examination from outside experts, the creation of an authenticable paper record of votes cast and a chain of custody for records.

Electronic voting technology can speed the counting of ballots, reduce the cost of paying staff to count votes manually and can provide improved accessibility for disabled voters. However, there has been contention, especially in the United States, that electronic voting, especially DRE voting, could facilitate electoral fraud and may not be fully auditable. In addition, electronic voting has been criticized as unnecessary and expensive to introduce. Several countries have cancelled e-voting systems or decided against a large-scale rollout, notably the Netherlands and the United Kingdom.

Electronic voting systems for electorates have been in use since the 1960s, when punched card systems debuted. Their first widespread use was in the USA where 7 counties switched to this method for the 1964 presidential election. The newer optical scan voting systems allow a computer to count a voter's mark on a ballot. DRE voting machines which collect and tabulate votes in a single machine are used by all voters in all elections in Brazil and India, and also on a large scale

in Venezuela and the United States. They have been used on a large scale in the Netherlands but have been decommissioned after public concerns.

Internet voting systems have gained popularity and have been used for government elections and referendums in the United Kingdom (although not presently), Estonia and Switzerland as well as municipal elections in Canada and party primary elections in the United States and France

There are also hybrid systems that include an electronic ballot marking device (usually a touch screen system similar to a DRE) or other assistive technology to print a voter verified paper audit trail, and then use a separate machine for electronic tabulation

## **2.5 Summary**

Chapter 2 consists of voting system. There are many types of voting like- Paper-Based Voting, Optical Voting Machine etc. It will increase the knowledge about voting system. The way in which the voting system is conducted. There is also description about E-voting System.

# Chapter 3

## Electronic Voting System in Current World

### 3.1 Introduction

In 1985, there was an implementation of a computerized election database by the Superior Electoral Court, while the electronic voting machine as conceived today was only developed in 1995 and first used in municipal elections the following year. But it was in 1989, in Brusque (SC), where Judge Carlos Prudencio held the first voting experience with micro-computers.<sup>[2]</sup>

Arizona made transitional moves towards online voting. Each registered Democrat received a personal identification number in the mail. These citizens had the option to either cast ballots at a designated location or over the internet from the comfort of their own home. Voters voting over the internet were required to insert their PIN and answer two personal questions. Once all the information is verified, they have the voting options.<sup>[2]</sup>

Estonia has made notable advances in Internet Voting technology. In Estonia, each voter has a national ID card that they use to identify each citizen. The ID card is the security Estonia put in to ensure reliability in votes. Security officials said that they have not detected any unusual activity or tampering of the votes.

It is difficult to say whether online voting successfully increases voter turnout due to the digital divide. A study conducted on “remote electronic voting and turnout in the Estonian 2007 parliamentary elections” showed that rather than eliminating inequalities, e-voting might have enhanced the digital divide between higher and lower socioeconomic classes. People who lived greater distances from polling areas voted at higher levels with this service now available. The 2007 Estonian elections yielded a higher voter turnout from those who lived in higher income regions and who received formal education.

Political parties that have more support from the less fortunate who are unfamiliar with the Internet may suffer in the elections due to e-voting, which tends to increase voting in the upper/middle class. It is unsure as to whether narrowing the digital divide would promote equal voting opportunities for people across various social, economic and ethnic backgrounds. In the long run, this is contingent not only on internet accessibility, which is already widely available in Estonia, but also depends on people’s level of familiarity with the Internet.

### 3.2 Real Life Example

**Electronic Voting Machines** ("EVM") are being used in Indian General and State Elections to implement electronic voting in part from 1999 elections and in total since 2004 elections. The EVMs reduce the time in both casting a vote and declaring the results compared to the old paper ballot system. There were earlier claims regarding EVMs' tamperability and security which have

not been proved. After rulings of Delhi High Court, Supreme Court and demands from various political parties, Election Commission decided to introduce EVMs with Voter-verified paper audit trail (VVPAT) system. The Voter-verified paper audit trail (VVPAT) system was introduced in 8 of 543 parliamentary constituencies as a pilot project in Indian general election, 2014.<sup>[3]</sup>

### **3.3 Analysis**

As soon as the last voter has voted, the Polling Officer in-charge of the Control Unit will press the 'Close' Button. Thereafter, the EVM will not accept any votes. Further, after the close of poll, the Balloting Unit is disconnected from the Control Unit and kept separately. Votes can be recorded only through the Balloting Unit. Again the Presiding officer, at the close of the poll, will hand over to each polling agent present an account of votes recorded. At the time of counting of votes, the total will be tallied with this account and if there is any discrepancy, this will be pointed out by the Counting Agents. During the counting of votes, the results are displayed by pressing the 'Result' button. There are two safeguards to prevent the 'Result' button from being pressed before the counting of votes officially begins, (a) This button cannot be pressed till the 'Close' button is pressed by the Polling Officer in-charge at the end of the voting process in the polling booth and (b) This button is hidden and sealed; this can be broken only at the counting center in the presence of designated office

### **3.4 Fact Finding**

A candidate can know how many people from a polling station voted for him. This is a significant issue particularly if lop-sided votes for/against a candidate are cast in individual polling stations and the winning candidate might show favoritism or hold grudge on specific areas. The Election Commission of India has stated that the manufacturers of the EVMs have developed a 'Totaliser' unit which can connect several balloting units and would display only the overall results from an Assembly or a Lok Sabha constituency instead of votes from individual polling stations. The control units do not electronically transmit their results back the Election Commission, even though a simple and unconditionally secure protocol for doing this exists. The Indian EVMs are purposely designed as stand-alone units to prevent any intrusion during electronic transmission of results. Instead, the EVMs are collected in counting booths and tallied on the assigned counting day(s) in the presence of polling agents of the candidates. An international conference on the Indian EVMs and its tamper ability of the said machines was held under the chairmanship of Subramanian Swamy, President of the Janata Party and former Union Cabinet Minister for Law, Commerce and Justice at Chennai on 13 February 2010. The conclusion was that the Election Commission of India was shirking its responsibility on the transparency in the working of the EVMs. In April 2010, an independent security analysis was released by a research team led by Hari Prasad, Rop Gonggrijp, and J. Alex Halderman. The study included video demonstrations of two attacks that the researchers carried out on a real EVM, as well as descriptions of several other potential vulnerabilities. In order to mitigate these threats, the researchers suggest moving to a



voting system that provides greater transparency, such as paper ballots, precinct count optical scan, or a voter verified paper audit trail, since, in any of these systems, skeptical voters could, in principle, observe the physical counting process to gain confidence that the outcome is fair. But Election Commission of India points out that for such tampering of the EVMs, one needs physical access to EVMs, and pretty high tech skills are required. Given that EVMs are stored under strict security which can be monitored by candidates or their agents all the time, it's impossible to gain physical access to the machines. Plus, to impact the results of an election, hundreds to thousands of machines will be needed to tamper with, which is almost impossible given the hi-tech and time consuming nature of the tampering process.

On 25 July 2011, responding to a PIL (Writ Petition (Civil) No. 312 of 2011), Supreme Court of India asked EC to consider request to modify EVMs and respond within 3 months. The petitioner Rajendra Satyanarayan Gilda had alleged that EC has failed to take any decision despite his repeated representation. The petitioner suggested that the EVMs should be modified to give a slip printed with the symbol of the party in whose favor the voter cast his ballot.

On 17 January 2012, Delhi High Court in its ruling on Dr. Subramanian Swamy's Writ Petition (Writ Petition (Civil) No. 11879 of 2009) challenging the use of EVMs in the present form said that EVMs are not "tamper-proof". Further, it said that it is "difficult" to issue any directions to the EC in this regard. However, the court added that the EC should itself hold wider consultations with the executive, political parties and other stake holders on the matter.

Swamy appealed against Delhi High Court's refusal to order a VVPAT system in Supreme Court. On 27 September 2012, Election Commission's advocate Ashok Desai submitted to a Supreme Court bench of Justice P Sathasivam and Justice Ranjan Gogoi that field trial for VVPAT system is in progress and that a status report will be submitted by early January 2013. Desai said that on pressing of each vote, a paper receipt will be printed, which will be visible to the voters inside a glass but cannot be taken out of the machine. To this, Dr Swamy replied that the new system was acceptable to him. The Supreme Court posted the matter for further hearing to 22 January 2013.

Another similar writ petition filed by the Asom Gana Parishad is still pending before the Gauhati High Court. On 8 October 2013, Supreme Court of India delivered its verdict on Subramanian Swamy PIL, that Election Commission of India will use VVPATs along with EVMs in a phased manner and the full completion should be achieved by 2019.<sup>[3]</sup>

### 3.5 Attacks on Electronic Voting

a) **Denial-Of-Service (Dos) Attack** is an attempt to make a machine or network resource unavailable to its intended users, such as to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet. Denial of service is typically accomplished by flooding the targeted machine or resource with superfluous requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled.

- b) **Trojan Horse, or Trojan,** is any malicious computer program which is used to hack into a computer by misleading users of its true intent. The term is derived from the Ancient Greek story of the wooden horse that was used to help Greek troops invade the city of Troy by stealth Insider attack on voting system Insider attacks are particularly insidious threats to electoral integrity. Traitors that misuse the trust that is placed in them often have system access that facilitates malicious acts themselves and their subsequent cover-up efforts.
- c) **Spoofing Attack:** It is a situation in which one person or program successfully masquerades as another by falsifying data, thereby gaining an illegitimate advantage. They are thus vulnerable to spoofing attacks when extra precautions are not taken by applications to verify the identity of the sending or receiving host. IP spoofing and ARP spoofing in particular may be used to leverage man-in-the-middle attacks against hosts on a computer network. Spoofing attacks which take advantage of TCP/IP suite protocols may be mitigated with the use of firewalls capable of deep packet inspection or by taking measures to verify the identity of the sender or recipient of a message.
- d) **Bad Verify Attack:** The Ghost Click attack defeats the verification app, but applying it on a large scale would lead to a suspiciously high number of replacement votes. We also experimented with a stealthier but more complicated style of attack that targets the verification app directly.
- e) **Worm:** A worm is a type of virus that does not change any existing program or file to spread itself. Instead, it makes copies of itself within an infected computer and spreads to become active on other systems. It is intentionally destructive, overwriting portions of the files with random data. This damage is non-repairable, so files may need reinstallation or restoring from a backup.
- f) **Man-In-The-Middle Attack (MITM):** MITM attack is an attack in which data being transmitted between two parties on a network is intercepted, read and modified by a system attacker without the communicating parties knowing that their data has been compromised.<sup>[7]</sup>

## 3.6 Securing Online Voting System

### 3.6.1 Accuracy

A system is accurate if 1). It is not possible for a vote to be altered, 2). It is not possible for a validated vote to be eliminated from the final tally, 3). It is not possible for an invalid vote to be counted in the final tally <sup>[8]</sup>

### 3.6.2 Verifiability

“A system is verifiable if anyone can independently verify that all votes have been counted correctly”. Currently, many experts believe that the best method to verify votes and perform

recounts is with paper ballots. In addition, the voter should be able to verify that their ballot is entered correctly and allow them to adjust their vote if necessary.<sup>[8]</sup>

### **3.6.3 Democracy**

A system is democratic if 1). It permits only eligible voters to vote and 2). It ensures that each eligible voter can vote only once”. This characteristic can be accomplished by incorporating accuracy and verifiability. Currently, many counties require that voters vote in their own precinct so, that they can sign their name in the approved voter list. Some counties have implemented a database that tracks voters.

### **3.6.4 Privacy**

Privacy is one of the most important properties of an information system must satisfy, in which systems the need to share information among different, not trusted entities. “A system is private if 1). Neither election authorities nor anyone else can link any ballot to the voter who cast it and 2). No voter can prove that he or she voted in a particular way”. Privacy is a concern to all users of a voting system.<sup>[6]</sup>

### **3.6.5 Convenience**

“A system is convenient if it allows voters to cast their votes quickly, in one session, and with minimal equipment or special skills”. The introduction of touch screens into the voting process was first used to aid the disabled population. This increased convenience of touch screens could lead to higher voter participation and decreased time at the polls. If the system utilizes technology that society is already comfortable using, voters will perceive the system to be more convenient.<sup>[6]</sup>

### **3.6.6 Consistency**

A system is consistent if it operates efficiently at each location, in each situation, and the functions perform exactly as designed. Each voting machine must be an exact duplicate of the other to ensure consistency and quality control. This also, increases usability as the voting process does not vary between locations, especially important for our mobile society<sup>[6]</sup>.

### **3.6.7 Cryptographic Verification**

The concept of election verifiability through cryptographic solutions has emerged in the academic literature to introduce transparency and trust in electronic voting systems. It allows voters and election observers to verify that votes have been recorded, tallied and declared correctly, in a manner independent from the hardware and software running the election. Three aspects of verifiability are considered: individual, universal, and eligibility. Individual verifiability allows a voter to check that her own vote is included in the election outcome, universal verifiability allows voters or election observers to check that the election outcome corresponds to the votes cast, and

eligibility verifiability allows voters and observers to check that each vote in the election outcome was cast by a uniquely registered voter.<sup>[8]</sup>

### 3.7 Security Mechanism Can Be Maintained

For Example, if we take Man-In-The-Middle Attack, to prevent this attack we have to use Secure Socket Layer (SSL). In the world of electronic commerce, security is a highly essential feature to have in anyway system. A socket is a term for a communications port between computers over any interconnection medium using any computer-to-computer protocol. SSL is a protocol that is used for sending secure encrypted data over the internet. SSL layer is present between TCP/IP protocol and the application layer as shown. SSL protocol can protect users from “man in the middle attacks. The SSL protocol is based on the public key cryptography which has a public and private key pair, the public key can be revealed to everyone but the private key is only known to the recipient of the message being sent. The message is encrypted with the public key and decrypted with the private key. SSL security medium is based on cryptography. Cryptography is the conversion of data into a secret code for transmission over a public network. The plain text is converted into a coded equivalent called cipher text via an encryption algorithm. The cipher text is decrypted at the receiving end and turned back into plaintext. AES is the most commonly used internet encryption algorithm. The Secure Socket Layer protocol has been succeeded by the Transport Layer Security(TLS) protocol, which has similar features to its predecessor SSL. Most internet browser software support TLS<sup>[1]</sup>

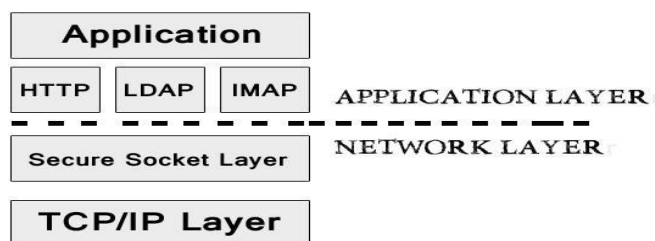


Figure 3.1 : SSL Running Above TCP/IP

### 3.8 How SSL Works on the Internet

SSL makes use of the symmetric key encryption system from AES for encrypting information going through the network; asymmetric key encryption is form of encryption which utilizes a Secret single key for encrypting data and decrypting data. A major problem of symmetric key encryption is the case of how the key would be sent to a legitimate user without being compromised. In order for the key to be exchanged for the secure data transmission to take place,

the web browser would have to commence an SSL session with the web server. The web server would respond to the secure session request by sending its SSL digital certificate, which would include its public key, issuer name, certificate issue and expiry date etc. The browser checks the certificate to ensure that it is valid and it's signed from a known certificate authority, the most common certificate authority is VeriSign. If the certificate is not authentic or unrecognized, the web browser issues a warning message to the user. If, the certificate is valid and authentic, the web browser creates a unique session key that would be used to encryption all data transmission going through the network, during the session. The web browser would encrypt the session key with the public key of the webserver stored in the SSL certificate and send it back to the web server. The web server would decrypt the encrypted message with its private key. Once these processes are done, a secure transmission would exist between the browser and the server, and all data being transmitted would be encrypted. Apache tomcat web server can be configured to perform SSL connections<sup>[11]</sup>

### **3.9 Summary**

In This chapter there is description about Electronic Voting System in Current World working procedure. This chapter consists of Electronic Voting System real life example, attacks on voting system and working procedure of Secure Socket Layer

# Chapter 4

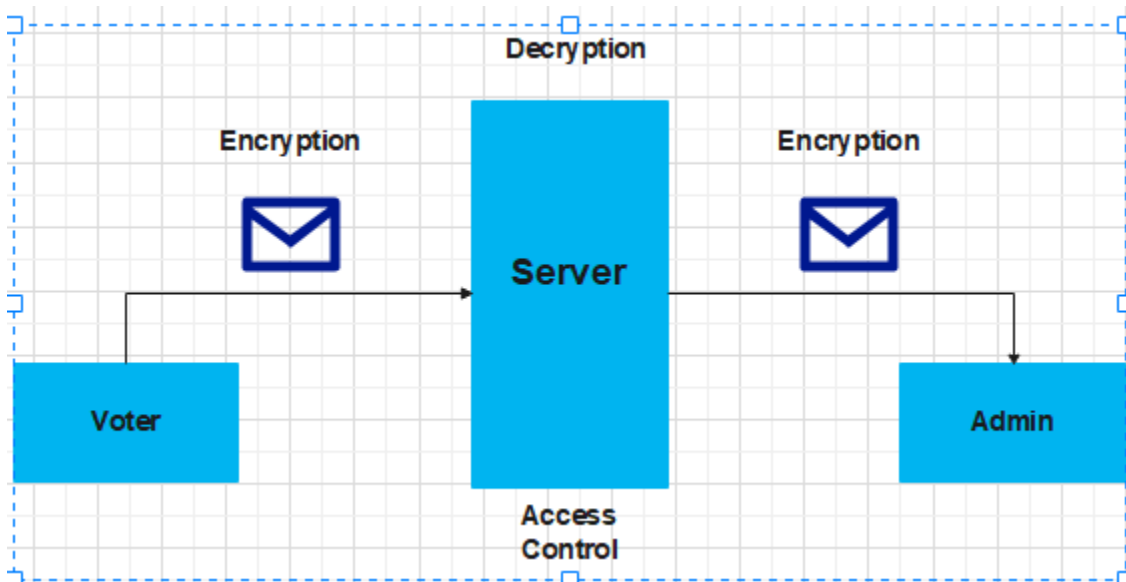
## Proposed Online EVM System with Enhanced Security

### 4.1 Introduction

This system gives security. This system ensures authentication of a voter, confidentiality of votes, integrity of a vote. This system encrypt vote, make it a cypher then store it in a database. It secures the vote from the attack of an attacker and also generates an error free counted vote result.

### 4.2 Overview of EVM System

Voter will provide his/her user information. Voter Submit all information. If Voter gives valid data then Voter can log in to see his/her profile. Voter will give vote. Vote will pass in an encrypted way. Vote stored in a server in a decrypted way. Admin will get it in an encrypted way and then decrypt again.



**Fig 4.2 The Overall system**

Admin enter Admin\_Id. Admin gives Password. Then submit it. Admin can count result, manages voter list and nominee list. Admin manages voter list, nominee list. Admin counts the final result and publish it. Admin enters Nominee\_Id. And name. Then submit it. If admin gives nominee valid data then, admin can handle the nominee profile

### 4.3 ER Diagram

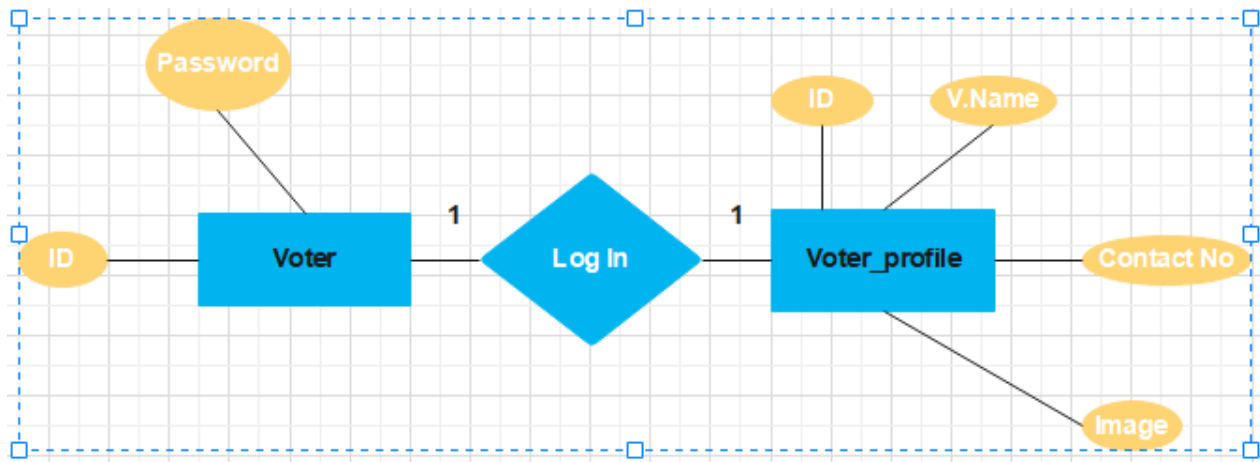


Fig 4.3 ER diagram (From Voter Perspective)

### 4.4 Context Diagram

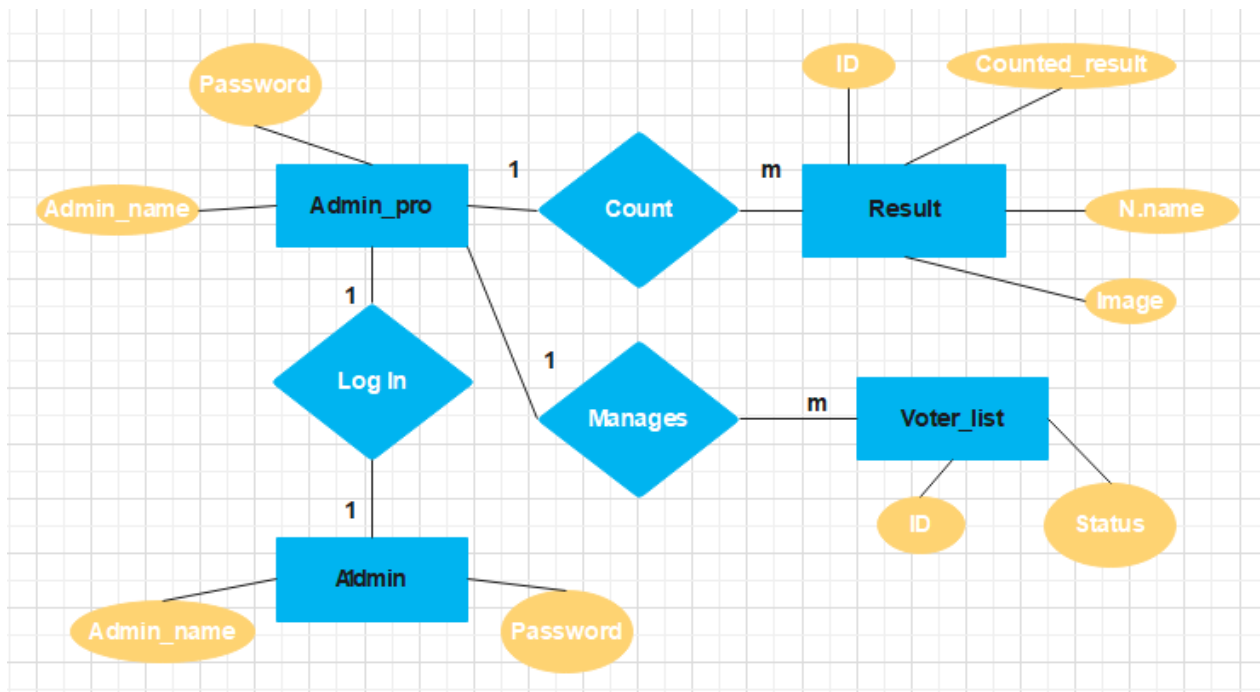


Figure 4.4 ER diagram (From Admin Perspective)

## 4.5 Context Diagram

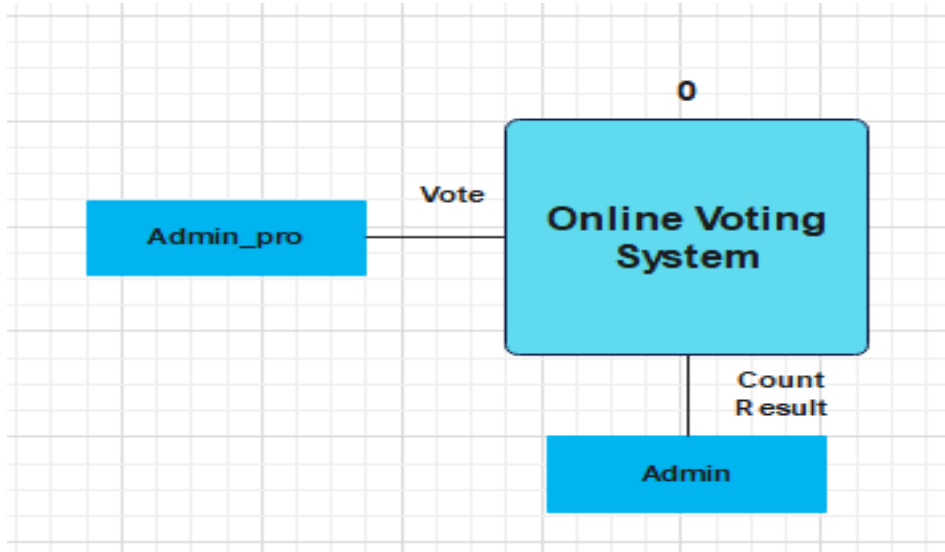
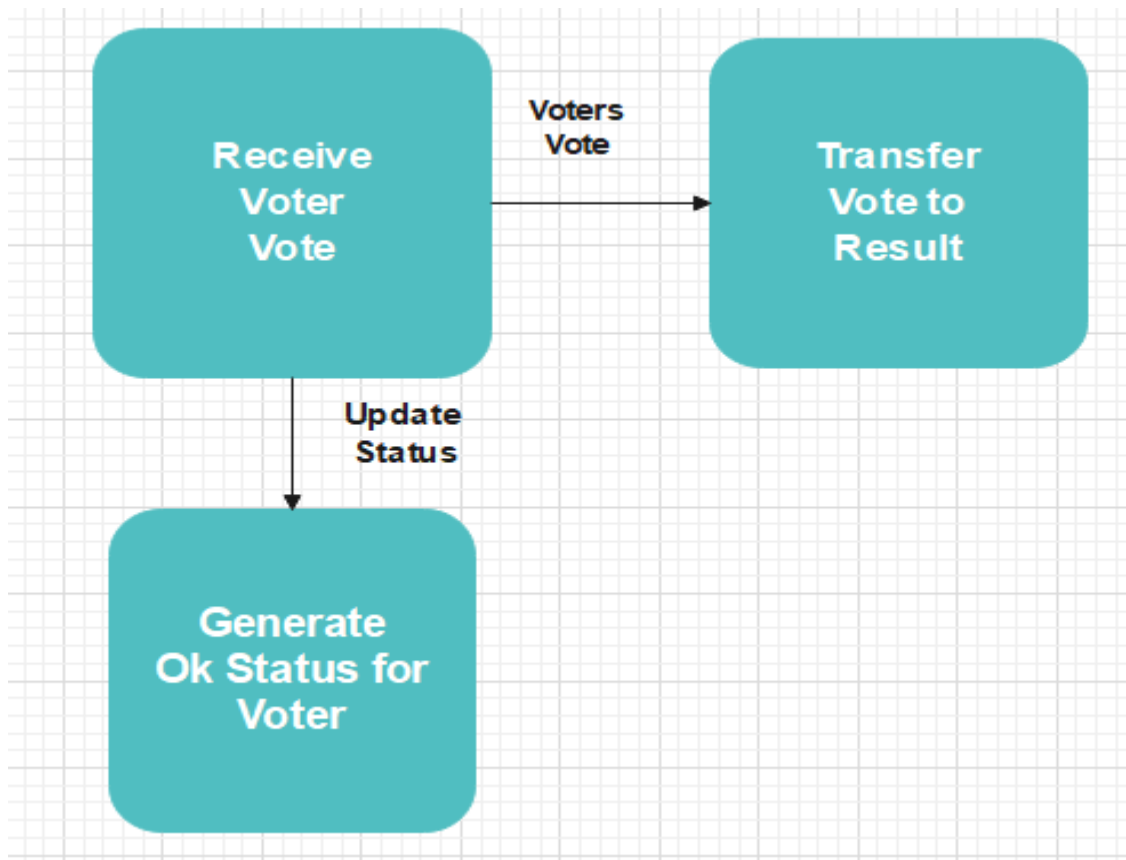


Figure 4.5: Context Diagram

## 4.6 Data Flow Diagram (1)





## 4.7 Data Flow Diagram (2)

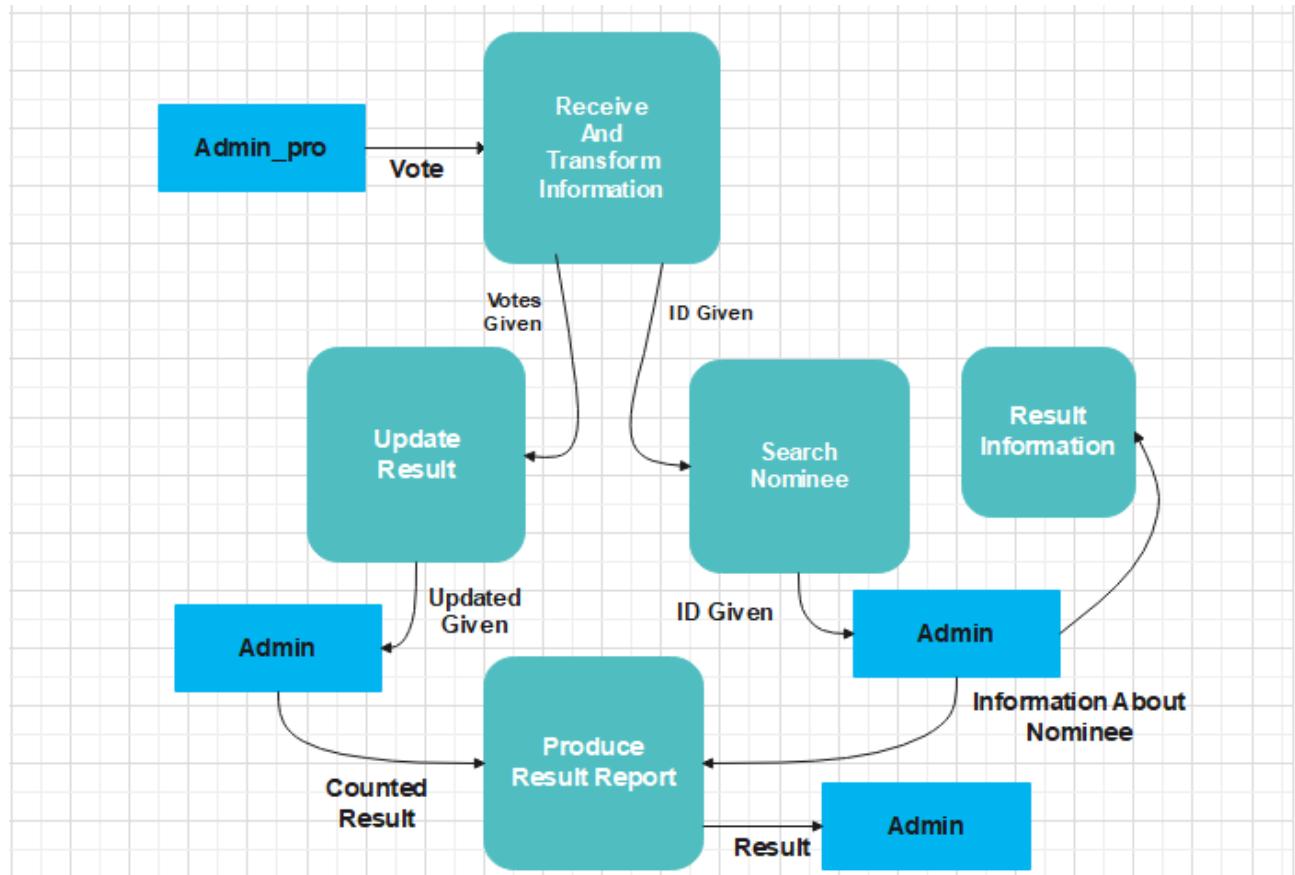


Figure 4.6 & 4.7: 0 and 1 Level DFD

## 4.8 Flow Chart

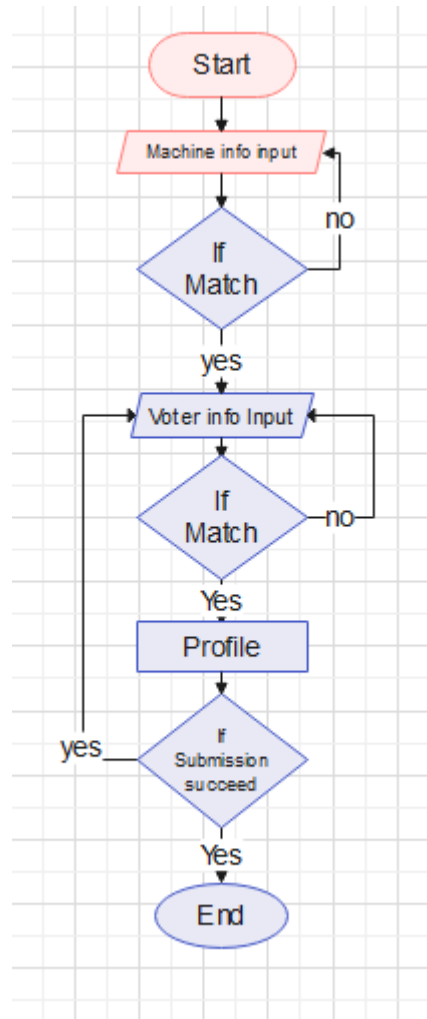


Figure 4.8: Flow Chart

## 4.9 Algorithm<sup>[4]</sup>

The Advanced Encryption Standard (AES), also known by its original name Rijndael is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001.

AES is a variant of the Rijndael block cipher<sup>[5]</sup> developed by two Belgian cryptographers, Joan Daemen and Vincent Rijmen, who submitted a proposal to NIST during the AES selection process. Rijndael is a family of ciphers with different key and block sizes. For AES, NIST selected three members of the Rijndael family, each with a block size of 128 bits, but three different key lengths: 128, 192 and 256 bits.

AES has been adopted by the U.S. government. It supersedes the Data Encryption Standard (DES) which was published in 1977. The algorithm described by AES is a symmetric-key algorithm, meaning the same key is used for both encrypting and decrypting the data.

In the United States, AES was announced by the NIST as U.S. FIPS PUB 197 (FIPS 197) on November 26, 2001. This announcement followed a five-year standardization process in which fifteen competing designs were presented and evaluated, before the Rijndael cipher was selected as the most suitable.

AES is included in the ISO/IEC 18033-3 standard. AES became effective as a U.S. federal government standard on May 26, 2002, after approval by the U.S. Secretary of Commerce. AES is available in many different encryption packages, and is the first (and only) publicly accessible cipher approved by the U.S. National Security Agency (NSA) for top secret information when used in an NSA approved cryptographic module.

Points to remember

- AES is a block cipher.
- The key size can be 128/192/256 bits.
- Encrypts data in blocks of 128 bits each.

That means it takes 128 bits as input and outputs 128 bits of encrypted cipher text as output. AES relies on substitution-permutation network principle which means it is performed using a series of linked operations which involves replacing and shuffling of the input data.

### 4.9.1 Definitive Standards

The Advanced Encryption Standard (AES) is defined in each of:

- FIPS PUB 197: Advanced Encryption Standard (AES)
- ISO/IEC 18033-3: Block ciphers

### 4.9.2 AES Rounds and Round keys<sup>[17]</sup>

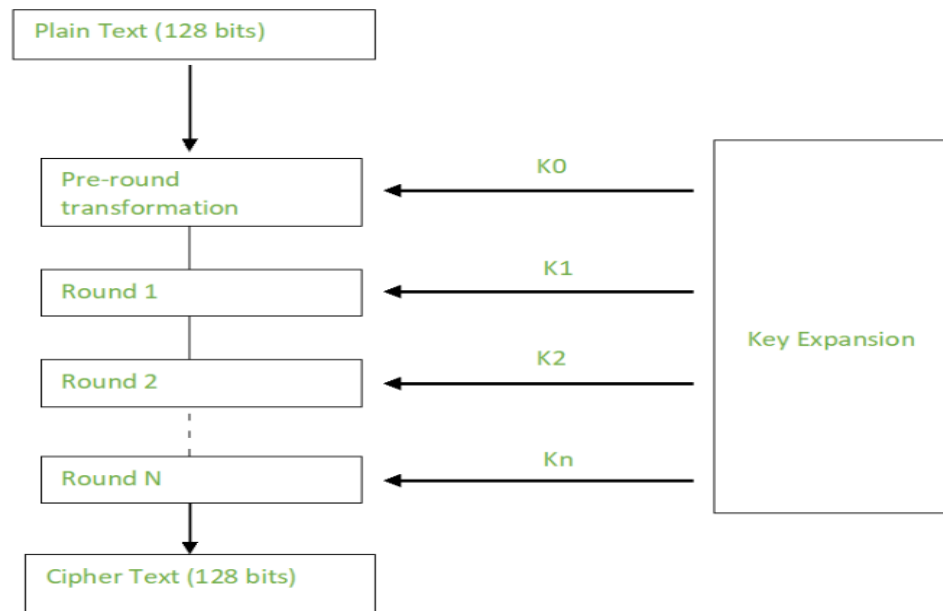
AES performs operations on bytes of data rather than in bits. Since the block size is 128 bits, the cipher processes 128 bits (or 16 bytes) of the input data at a time.

The number of rounds depends on the key length as follows :

- 128 bit key – 10 rounds
- 192 bit key – 12 rounds
- 256 bit key – 14 rounds

### Creation of Round keys :

A Key Schedule algorithm is used to calculate all the round keys from the key. So the initial key is used to create many different round keys which will be used in the corresponding round of the encryption.



### 4.9.3 Example and implementation<sup>[17]</sup>

The implementation of AES involves doing a set of simple operations repeatedly. Each repetition is called a "round". Depending on the size of the key (128, 192 or 256 bit), the input (block of 16 bytes) goes through 10, 12 or 14 rounds. In applying the 2 Big Ideas - Diffusion and Confusion, AES makes sure that each bit in the 16 byte block depends on every bit in the same block from 2 rounds previously. That's quite the achievement, so let's speak about the operations in detail.

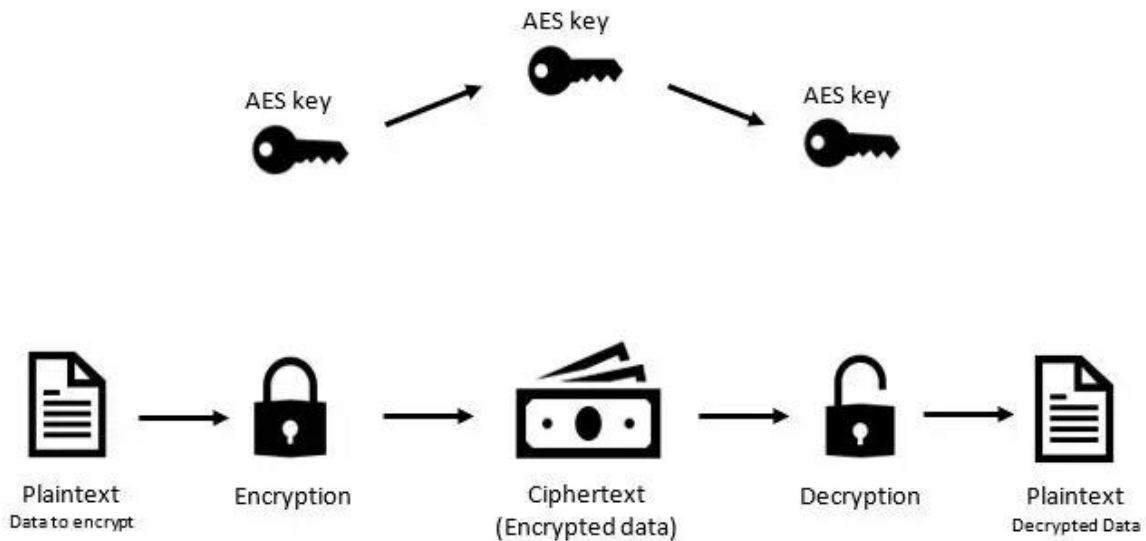
Each round consists of 4 steps:

1. applying a key - `addRoundKey()`

2. substituting bytes - `subBytes()`
3. shifting rows - `shiftRows()`
4. mixing columns - `mixColumns()`

Decryption involves the inverse of these steps, in reverse order:

1. inverse-mixing columns - `invMixColumns()`
2. inverse-shifting rows - `invShiftRows()`
3. inverse-substituting bytes - `invSubBytes()`
4. applying a key - `addRoundKey()`



**Figure 4.9: Using AES algorithm Encryption And Decryption Technique**

#### 4.10 Encryption

AES considers each block as a 16 byte (4 byte x 4 byte = 128 ) grid in a column major arrangement.

[ b0 | b4 | b8 | b12 |

| **b1** | **b5** | **b9** | **b13** |

| **b2** | **b6** | **b10** | **b14** |

| **b3** | **b7** | **b11** | **b15** ]

Each round comprises of 4 steps :

- SubBytes
- ShiftRows
- MixColumns
- Add Round Key

The last round doesn't have the MixColumns round.

The SubBytes does the substitution and ShiftRows and MixColumns performs the permutation in the algorithm.

### **SubBytes :**

This step implements the substitution.

In this step each byte is substituted by another byte. Its performed using a lookup table also called the S-box. This substitution is done in a way that a byte is never substituted by itself and also not substituted by another byte which is a compliment of the current byte. The result of this step is a 16 byte (4 x 4 ) matrix like before.

The next two steps implement the permutation.

### **ShiftRows :**

This step is just as it sounds. Each row is shifted a particular number of times.

- The first row is not shifted
- The second row is shifted once to the left.
- The third row is shifted twice to the left.
- The fourth row is shifted thrice to the left.

(A left circular shift is performed.)

[ **b0** | **b1** | **b2** | **b3** ]      [ **b0** | **b1** | **b2** | **b3** ]

$|b4| |b5| |b6| |b7| \rightarrow |b5| |b6| |b7| |b4|$   
 $|b8| |b9| |b10| |b11| \rightarrow |b10| |b11| |b8| |b9|$   
 $[b12|b13|b14|b15] \rightarrow [b15|b12|b13|b14]$

### MixColumns :

This step is basically a matrix multiplication. Each column is multiplied with a specific matrix and thus the position of each byte in the column is changed as a result.

**This step is skipped in the last round.**

$[c0] = [2 \ 3 \ 1 \ 1] [b0]$   
 $|c1| = |1 \ 2 \ 3 \ 1| |b1|$   
 $|c2| = |1 \ 1 \ 2 \ 3| |b2|$   
 $[c3] = [3 \ 1 \ 1 \ 2] [b3]$

## 4.11 Decryption

The stages in the rounds can be easily undone as these stages have an opposite to it which when performed reverts the changes. Each 128 blocks goes through the 10, 12 or 14 rounds depending on the key size.

The stages of each round in decryption is as follows :

- Add round key
- Inverse MixColumns
- ShiftRows
- Inverse SubByte

The decryption process is the encryption process done in reverse so i will explain the steps with notable differences.

### Inverse MixColumns :

This step is similar to the MixColumns step in encryption, but differs in the matrix used to carry out the operation.

$[b0] = [14 \ 11 \ 13 \ 9] [c0]$   
 $|b1| = |9 \ 14 \ 11 \ 13| |c1|$

| b2 |      | 13 9 14 11 | | c2 |  
[ b3 ]      [ 11 13 9 14 ] [ c3 ]

#### **4.12 Summery**

AES instruction set is now integrated into the CPU (offers throughput of several GB/s) to improve the speed and security of applications that use AES for encryption and decryption. Even though it's been 20 years since its introduction we have failed to break the AES algorithm as it is infeasible even with the current technology. Till date the only vulnerability remains in the implementation of the algorithm.



# Chapter 5 Implementation

## 5.1 Platform Overview

This system is a web based system, that can run in cross platform operating system. Beside this it runs on android system with a web browser for casting vote. We have used SQL as a database application and PHP.

## 5.2 System Requirement

For this system we need a server to host the system<sup>[14]</sup>, a database to store votes, admin information, nominee information, voter information. We will use a machine (Pc, mobile etc) for casting vote in Browser website.

## 5.3 Overview of Implemented System

This system will use the database of Election Commission. On the moment of voting the voter gives her/ his information that can authenticate her/him. After that pass the authentication she/he will has been taken to an interface that shows her/his basic information including her/ his image and here she/he finds a button to cast her/his vote. On the Admin view the admin show the result of vote, registration of voter and candidates.

## 5.4 Implementation of AES Algorithm in the System

Basically this system is emphasis on the vote security. So this example code shows the technique of a vote which is encrypted during its transmission time and stored in a database in encrypted way. Then the encrypted vote is decrypted.

**For Encryption** <sup>[4] [16]</sup>:

```
<!-- For Encryption -->
```

```
<?php
```

```
require_once("admin/inc/config.php");
```

```
$key='aaaabbbbcccc';
```

```
function encryptthis($data, $key) {
```

```
$encryption_key = base64_decode($key);
```

```
$iv = openssl_random_pseudo_bytes(openssl_cipher_iv_length('aes-256-cbc'));
```

```

$encrypted = openssl_encrypt($data, 'aes-256-cbc', $encryption_key, 0, $iv);

return base64_encode($encrypted . '::' . $iv);

}

?>

```

### **For Decryption:**

```

//<!-- For decryption -->

<?php

require_once("admin/inc/config.php");

$key='aaaabbbbcccc';

function decryptthis($data, $key) {

    $encryption_key = base64_decode($key);

    list($encrypted_data, $iv) = array_pad(explode(':', base64_decode($data), 2),2,null);

    return openssl_decrypt($encrypted_data, 'aes-256-cbc', $encryption_key, 0, $iv);

}

?>

<?php

include_once("./cryptofunction.php");

include_once("./admin/inc/config.php");

if(isset($_POST['sign_up_btn']))

{

    $su_username=mysqli_real_escape_string($conn, $_POST['su_username']);

```

```

$su_contact_number=mysqli_real_escape_string

($conn,$_POST['su_contact_number']);

$su_password=mysqli_real_escape_string($conn,$_POST['su_password']);

$su_password=encryptthis($su_password, $key);

$su_retype_password=mysqli_real_escape_string

($conn,$_POST['su_retype_password']);

$su_retype_password=encryptthis($su_retype_password, $key);

$user_role = "Voter";

mysqli_query($conn, "INSERT INTO users(username ,contact_no ,password,

user_role )VALUES

('". $su_username ."','". $su_contact_number ."','". $su_password ."', '". $user_role ."')") or

die(mysqli_error($conn));

?>

```

## 5.5 System code

### Log in Page:

```

<!DOCTYPE html>
<html>
    <head>
        <title>Voting System</title>
        <link rel="stylesheet" href="/assets/css/bootstrap.min.css">
        <link rel="stylesheet" href="/assets/css/login.css">
    </head>
    <body>
        <div class="container h-100">
            <div class="d-flex justify-content-center h-100">

```

```

<div class="user_card">
<div class="d-flex justify-content-center">
<div class="brand_logo_container">

</div>
</div>
<?php
if(isset($_GET['sign-up']))
{
?>
<div class="d-flex justify-content-center form_container">
<form method="post">
<div class="input-group mb-3">
<div class="input-group-append">
<span class="input-group-text"><i class="fas fa-user"></i></span>
</div>
<input type="text" name="su_username" class="form-control input_user"
placeholder="username" required />
</div>
<div class="input-group mb-2">
<div class="input-group-append">
<span class="input-group-text"><i class="fas fa-key"></i></span>
</div>
<input type="text" name="su_contact_number" class="form-control input_pass"
placeholder="contact #". required />
</div>
<div class="input-group mb-2">
<div class="input-group-append">
<span class="input-group-text"><i class="fas fa-key"></i></span>
</div>
<input type="password" name="su_password" class="form-control input_pass"
placeholder="password". required />
</div>
<div class="input-group mb-2">
<div class="input-group-append">
<span class="input-group-text"><i class="fas fa-key"></i></span>
</div>
<input type="password" name="su_retype_password" class="form-control input_pass"
placeholder="retype password". required />
</div>
<div class="d-flex justify-content-center mt-3 login_container">
<button type="submit" name="sign_up_btn" class="btn login_btn">Sign up</button>
</div>
</form>

```

```

</div>

<div class="mt-4">
<div class="d-flex justify-content-center links">
Already have an account! <a href="index.php" class="ml-2">Sign in</a>
</div>
</div>
<?php

}else {
?>

<div class="d-flex justify-content-center form_container">
<form method="post">
<div class="input-group mb-3">
<div class="input-group-append">
<span class="input-group-text"><i class="fas fa-user"></i></span>
</div>
<input type="text" name="contact_no" class="form-control input_user"
placeholder="Contact_no" required />
</div>
<div class="input-group mb-2">
<div class="input-group-append">
<span class="input-group-text"><i class="fas fa-key"></i></span>
</div>
<input type="password" name="password" class="form-control input_pass" value=""
placeholder="password" required />
</div>
<div class="form-group">
<div class="custom-control custom-checkbox">
<input type="checkbox" class="custom-control-input" id="customControlInline">
<label class="custom-control-label" for="customControlInline">Remember me</label>
</div>
</div>
<div class="d-flex justify-content-center mt-3 login_container">
<button type="submit" name="loginbtn" class="btn login_btn">Login</button>
</div>
</form>
</div>

<div class="mt-4">
<div class="d-flex justify-content-center links">
Don't have an account? <a href="?sign-up=1" class="ml-2">Sign Up</a>
</div>
<div class="d-flex justify-content-center links">

```

```

        <a href="#">Forgot your password?</a>
    </div>
</div>
<?php
}}
?>
</div>
</div>
</div>
<script src="/assets/js/jquery.min.js"></script>
<script src="assets/js/bootstrap.min.js"></script>
</body>
</html>

```

### Election Page:

```

<div class="row my-3 text-white" >
<div class="col-4">
<h3>Add New Candidate</h3>
<form method="POST" enctype="multipart/form-data">

<div class="form-group">
<select class="form-control" name="election_id" required>
<option value="">Select Election</option>
<?php
$fetchingElections = mysqli_query($conn, "SELECT * FROM elections") OR
die(mysqli_error($conn));
$isAdminAdded = mysqli_num_rows($fetchingElections);
if($isAdminAdded > 0)
{
while($row = mysqli_fetch_assoc($fetchingElections))
{
$election_id = $row['id'];
$election_name = $row['election_topic'];
$allowed_candidates = $row['no_of_candidates'];
$fetchingcandidate = mysqli_query($conn, "SELECT * FROM candidate_details WHERE
election_id = " . $election_id . " ") or die(mysqli_error($conn));
$added_candidates = mysqli_num_rows($fetchingcandidate);
?>
<option value="<?php echo $election_id; ?>"><?php echo $election_name; ?></option>
<?php
}
}else{
?>
<option value="">Please add election first</option>
<?php

```

```

}
?>
</select>
</div>
<div class="form-group">
<input type="text" name="candidate_name" placeholder="Candidate Name"
class="form-control" required />
</div>
<div class="form-group">
<input type="file" name="candidate_photo" class="form-control" required />
</div>
<div class="form-group">
<input type="text" name="candidate_details" placeholder="Candidate Details"
class="form-control" required />
</div>
<input type="submit" value="Add Candidate" name="addCandidateBtn" class="btn btn-
success"/>
</form>
</div>

```

### Candidates Details:

```

<div class="col-8 text-white" >
<h3>Candidate Details</h3>
<table class="table">
<thead>
<tr class="done">
<th scope="col">S.No</th>
<th scope="col">Photo</th>
<th scope="col">Name</th>
<th scope="col">Details</th>
<th scope="col">Election</th>
<th scope="col">Action</th>
</tr>
</thead>
<tbody>
<?php
$fetchingData = mysqli_query($conn, "SELECT * FROM candidate_details") or
die(mysqli_error($conn));
$isAnyCandidateAdded = mysqli_num_rows($fetchingData);
if($isAnyCandidateAdded > 0){
$sno = 1;
while($row = mysqli_fetch_assoc($fetchingData)){
$selection_id = $row['election_id'];
$fetchingElectionName = mysqli_query($conn, "SELECT * FROM elections WHERE id = '" .
$selection_id . "'" ) or die(mysqli_error($conn));

```

```

$exectfetchingelectionNameQuery = mysqli_fetch_assoc($fetchingElectionName);
$selection_name = $exectfetchingelectionNameQuery['election_topic'];
$candidate_photo = $row['candidate_photo']; ?>
<tr>
<td><?php echo $sno++; ?></td>
<td> </td>
<td><?php echo $row['candidate_name']; ?></td>
<td><?php echo $row['candidate_details']; ?></td>
<td><?php echo $selection_name; ?></td>
<td>
<a href="#" class="btn btn-sm btn-warning">Edit</a>
<a href="#" class="btn btn-sm btn-danger">Delete</a>
</td>
</tr>
<?php
}}
else{
?>
<tr>
<td colspan="7">No any candidate is added yet</td>
</tr>
<?php
}
?>
</tbody>
</table>
</div>
</div>
Voter Panel:
?>
<div class="row my-3">
<div class="col-12">
<h3>Voters Panel</h3>
<?php
$fetchingActiveElections = mysqli_query($conn, "SELECT * FROM elections WHERE status =
'active'") or
die(mysqli_error($conn));
$totalActiveElections = mysqli_num_rows($fetchingActiveElections);
if($totalActiveElections > 0){
while($data = mysqli_fetch_assoc($fetchingActiveElections)){
$selection_id = $data['id'];
$selection_topic = $data['election_topic'];
?>
<table class="table">
<thead>

```



```

<tr>
<th colspan="4" class="bg-green text-white"> <h5> ELECTION TOPIC: <?php echo
strtoupper($election_topic); ?></h5> </th>
</tr>
<tr>
<th>Photo</th>
<th>Candidate Details</th>
<th>$ of Voters</th>
<th>Action</th>
</tr>
</thead>
</table>
<?php }
}else{
echo "No any active election.";
}?>

```

### Result Page:

```

<div class="row my-3">
<div class="col-12">
<h3>Elction Results</h3>
<?php
$fetchingActiveElections = mysqli_query($conn, "SELECT * FROM elections WHERE id = '".
$election_id ."'") or
die(mysqli_error($conn));
$totalActiveElections = mysqli_num_rows($fetchingActiveElections);
if($totalActiveElections > 0)
{
while($data = mysqli_fetch_assoc($fetchingActiveElections))
{
$election_id = $data['id'];
$election_topic = $data['election_topic'];
?>
<table class="table">
<thead>
<tr>
<th colspan="4" class="bg-green text-white"> <h5> ELECTION TOPIC: <?php echo
strtoupper($election_topic); ?></h5> </th>
</tr>
<tr>
<th>Photo</th>
<th>Candidate Details</th>
<th>$ of Voters</th>

```

```

</tr>
</thead>
<tbody>
<?php
$fetchingCandidates = mysqli_query($conn, "SELECT * FROM candidate_details WHERE
election_id = '" . $selection_id . "'") or die(mysqli_error($conn));
while($candidateData = mysqli_fetch_assoc($fetchingCandidates))
{
$candidate_id = $candidateData['id'];
$candidate_photo = $candidateData['candidate_photo'];
//fetching
$fetchingVotes = mysqli_query($conn, "SELECT * FROM votings WHERE candidate_id =
'" . $candidate_id . "' ") or die(mysqli_error($conn));
$totalVotes = mysqli_num_rows($fetchingVotes);
?>
<tr>
<td></td>
<td><?php echo "<b>" . $candidateData['candidate_name'] . "</b> <br />" .
$candidateData['candidate_details']; ?></td>
<td><?php echo $totalVotes; ?></td>
</tr>
<?php
}
?>
</tbody>
</table>
<?php
?>
<!-- </table> -->
</div>
</div>

```

## 5.6 Summary

In this chapter we describe about the platform of our system, also the devices and server that we need to execute operation. Then we discuss about that when a voter cast a vote , the vote will be encrypted (using encryption algorithm), during transmission time the vote will be a cipher so that attacker cannot understand it. The cipher will be stored in to the database then decrypt it to count the result.

# Chapter 6 Comparison Analysis

## 6.1 Traditional Voting System V/S Online Secured Voting System

Online secured voting system is a hassle free and less time consuming voting system. Here we will show comparison between traditional and Online Secured Voting System.

### 6.1.1 Table that shows comparison between traditional and Online Secured Voting System.

Features	Traditional Voting System	Online Secured Voting System
Fraud Prevention	Not Possible	Possible
Encryption and Decryption of a vote.	No.	Yes.
Voter Authentication	No.	Yes.
Confidentiality	No.	Yes
Data Integrity	Does not ensure.	Ensures.
Calculation of votes	Cannot be trusted	Can be Trusted
Hassle free	No	Yes
Time Efficient	No	Yes
Trusted And Secured System	No	Yes.

## 6.2 Summary

This chapter shows the comparison between traditional voting system and ONLINE SECURED VOTING SYSTEM. It shows the efficiency and secured side of ONLINE SECURED SYSTEM. Online Secured Voting System is more trusted and Hassle free. Votes Count is also error free. Voter can cast their vote very easily through this system.

## References

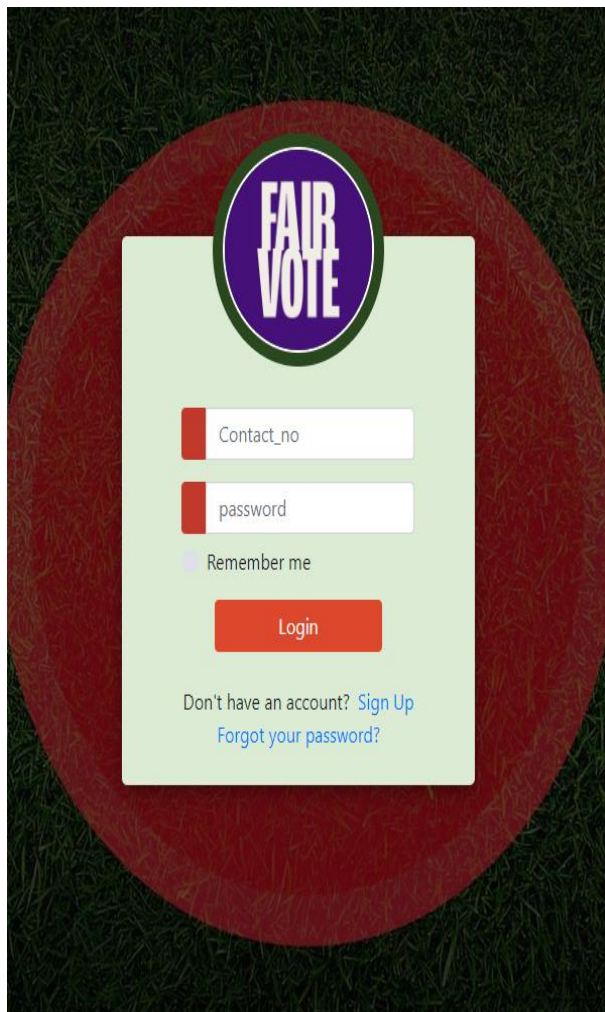
- [1] William Stallings, Cryptography and network security
- [2] [en.wikipedia.org/wiki/Voting\\_system](https://en.wikipedia.org/wiki/Voting_system)
- [3] [en.wikipedia.org/wiki/Electronic\\_voting\\_in\\_India](https://en.wikipedia.org/wiki/Electronic_voting_in_India)
- [4] [simple.wikipedia.org/wiki/AES\\_\(algorithm\)](https://simple.wikipedia.org/wiki/AES_(algorithm))
- [5] Data Communication and Networking, Fourth Edition by Behrouz A. Forouzan
- [6] Handbook of Applied Cryptography, by A.Menezes, P. van Oorschot and S. Vanstone, CRC press, 1996
- [7] <https://developer.android.com/reference/android/webkit/WebView.html>
- [8] [https://en.wikipedia.org/wiki/Attack\\_\(computing\)](https://en.wikipedia.org/wiki/Attack_(computing))
- [9] <https://www.electionsonline.com/online-voting-system/>
- [10] <https://www.w3schools.com/w3js/default.asp>
- [11] <http://php.net/docs.php>
- [12] <http://stackoverflow.com/questions/17717506/how-to-upload-images-into-mysql-database-using-php-code>
- [13] <https://www.tutorialspoint.com/nodejs/index.htm>
- [14] <https://www.apachefriends.org/docs/hosting-xampp-on-1and1.html>
- [15] <http://www.tendacn.com/en/faq/2165.html>
- [16] [https://a1websitepro.com/\(Maximus\)](https://a1websitepro.com/(Maximus))
- [17] <https://www.geeksforgeeks.org/>

## Chapter 7

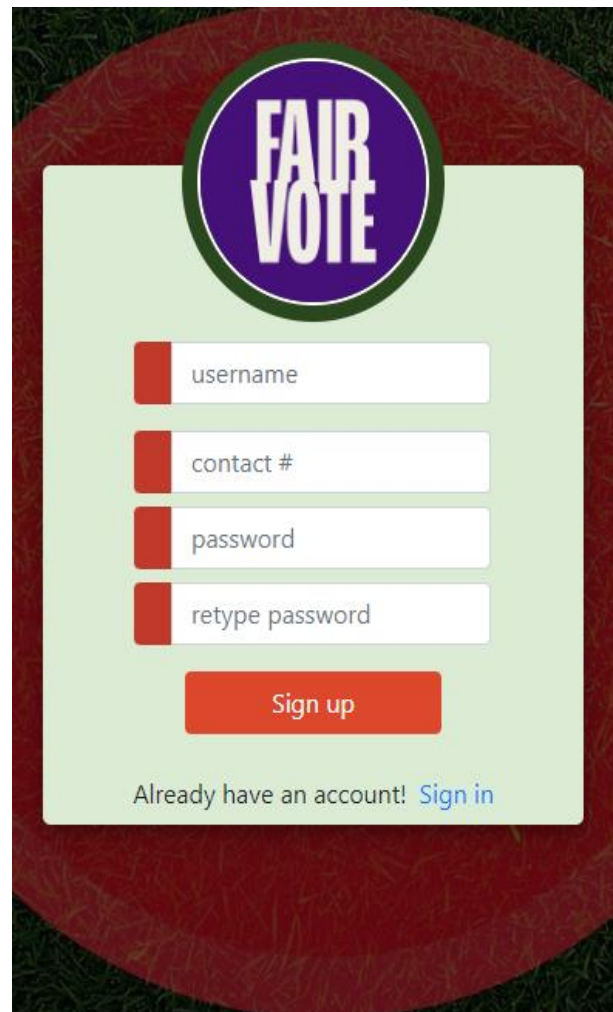
# Appendices

### Appendix A

Screenshot of Login & Signup page.....



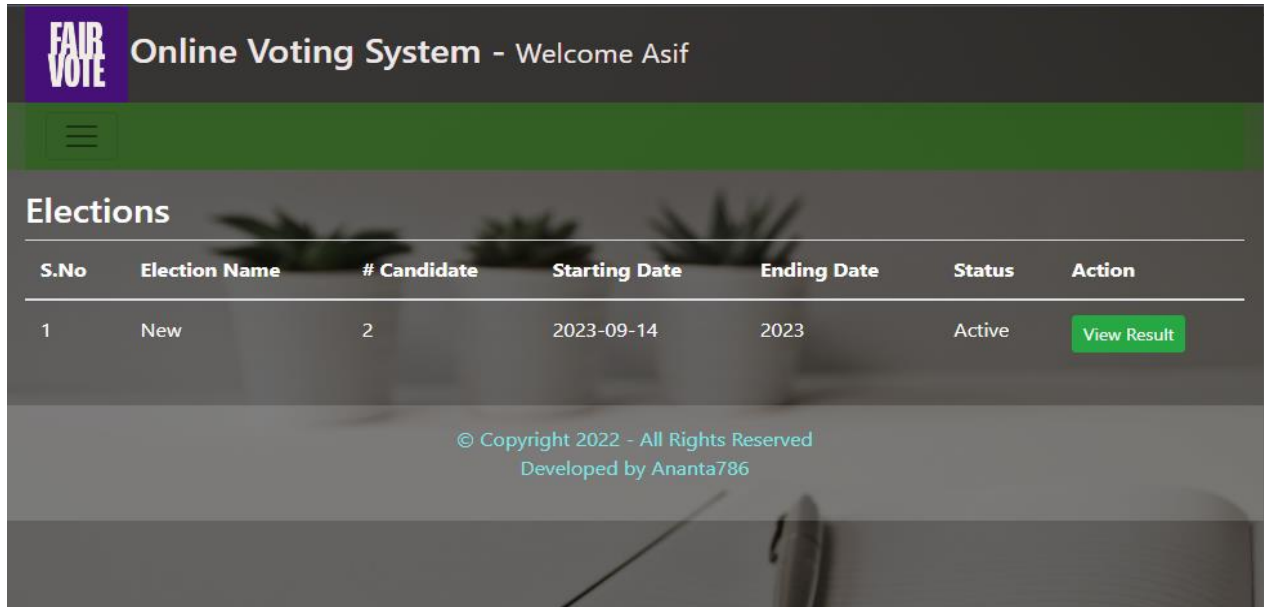
The screenshot shows the login interface for the FAIR VOTE system. It features a purple circular logo with the text "FAIR VOTE" at the top. Below the logo, there are two input fields: "Contact\_no" and "password". A "Remember me" checkbox is located below the password field. A red "Login" button is positioned below the checkbox. At the bottom, there is a link "Don't have an account? Sign Up" and a link "Forgot your password?".



The screenshot shows the signup interface for the FAIR VOTE system. It features a purple circular logo with the text "FAIR VOTE" at the top. Below the logo, there are four input fields: "username", "contact #", "password", and "retype password". A red "Sign up" button is positioned below the "retype password" field. At the bottom, there is a link "Already have an account! Sign in".

## Appendix B

### Screenshot of Admin Panels....



The screenshot shows the 'Online Voting System - Welcome Asif' admin panel. The header includes the 'FAIR VOTE' logo and a hamburger menu icon. The main content area is titled 'Elections' and displays a table with the following data:

S.No	Election Name	# Candidate	Starting Date	Ending Date	Status	Action
1	New	2	2023-09-14	2023	Active	<a href="#">View Result</a>

At the bottom, there is a copyright notice: '© Copyright 2022 - All Rights Reserved Developed by Ananta786'.



The screenshot shows the 'Online Voting System - Welcome Asif' admin panel. The header includes the 'FAIR VOTE' logo and a hamburger menu icon. The main content area is divided into two sections: 'Add New Elction' and 'Upcoming Elections'.

**Add New Elction**

Form fields:

- Election Topic
- NO of Candidate
- Starting\_date
- Ending\_date

[Add Election](#)

**Upcoming Elections**

S.No	Election Name	# Candidate	Starting Date	Ending Date	Status	Action
1	New	2	2023-09-14	2023	Active	<a href="#">Edit</a> <a href="#">Delete</a>

At the bottom, there is a copyright notice: '© Copyright 2022 - All Rights Reserved Developed by Ananta786'.



## Add New Candidate

Select Election



Candidate Name


Choose File

No file chosen

Candidate Details

Add Candidate

## Candidate Details

S.No	Photo	Name	Details	Election	Action
1		asif	voter	New	<a href="#">Edit</a> <a href="#">Delete</a>

## Appendix C


Screenshot of Voter's Panel: Before & After Vote....

**FAIR VOTE**

Online Voting System - Welcome asif

Voters Panel

ELECTION TOPIC: NEW

Photo	Candidate Details	\$ of Voters	Action
	asif voter	0	<a href="#">Vote</a>

© Copyright 2022 - All Rights Reserved  
Developed by Ananta786

**FAIR VOTE**

Online Voting System - Welcome asif

Voters Panel

ELECTION TOPIC: NEW

Photo	Candidate Details	\$ of Voters	Action
	asif voter	1	

© Copyright 2022 - All Rights Reserved  
Developed by Ananta786



## Appendix D

Screenshot of Result Page:

The screenshot shows the 'FAIR VOTE Online Voting System - Welcome Asif' interface. It features a green header with a menu icon. The main content area is titled 'Elction Results' (sic) and displays 'ELECTION TOPIC: NEW'. Below this is a table with three columns: 'Photo', 'Candidate Details', and '\$ of Voters' (sic). The table contains one row for 'asif voter' with a value of '1'. A circular profile picture of a man is shown next to the name. Below the table is a section titled 'Voting Details' with a table containing six columns: 'S.no', 'Voter Name', 'Contact No', 'Voted To', 'Date', and 'Time'. The table has one row with the following data: S.no: 1, Voter Name: asif, Contact No: 111, Voted To: asif, Date: 2023-09-03, Time: 01:15:33. At the bottom, there is a copyright notice: '© Copyright 2022 - All Rights Reserved Developed by Ananta786'.

**FAIR VOTE Online Voting System - Welcome Asif**

**Elction Results**

ELECTION TOPIC: NEW

Photo	Candidate Details	\$ of Voters
	asif voter	1

**Voting Details**

S.no	Voter Name	Contact No	Voted To	Date	Time
1	asif	111	asif	2023-09-03	01:15:33

© Copyright 2022 - All Rights Reserved  
Developed by Ananta786

# Chapter 8

## Conclusion and Future Work

### 7.1 Conclusion

Online Secured Voting System gives authenticity of voters and security of transmission of vote and also prevents security attack. Using this system a voter can give only one vote to a specific nominee. This system is error free and gives the accurate voting result.

### 7.2 Future Modification.

- Include Biometric authentication system into our system to make it more secure.
- Include Nominee page to interact.
- Adding SMARTCARD (voter id Card) for authenticate.
- Time Counting Mechanic.
- Mobile Application.