

SIMPLISTIC ONLINE VOTING SYSTEM

A PROJECT REPORT

Submitted by

GANESH M 812618205008

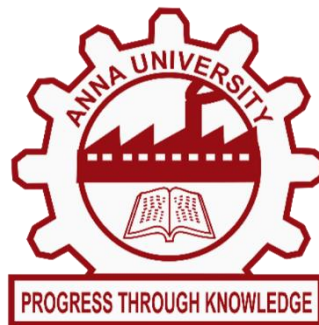
SANTHOSH I 812618205016

VIJAYAKUMAR M 812618205023

*in partial fulfillment for the award of the degree
of*

**BACHELOR OF TECHNOLOGY
IN
INFORMATION TECHNOLOGY**

**M.A.M COLLEGE OF ENGINEERING
SIRUGANUR, TRICHY**



ANNA UNIVERSITY : CHENNAI 600 025

JUNE 2022

ANNA UNIVERSITY : CHENNAI 600 025

BONAFIDE CERTIFICATE

Certified that this project report “**SIMPLISTIC ONLINE VOTING SYSTEM**” is the bonafide work of **GANESH M – 812618205008, SANTHOSH I – 812618205016, VIJAYAKUMAR M - 812618205023**” who carried out the project work under my supervision.

SIGNATURE

Dr.G.KALPANADEV, M.E., Ph.D

HEAD OF THE DEPARTMENT

Professor,

Department of IT,

M.A.M College of Engineering,

Siruganur, Tiruchirappalli-621 105.

SIGNATURE

Mrs.K.UDHAYA SURIYA, M.E.

SUPERVISOR

Assistant Professor,

Department of IT,

M.A.M College of Engineering,

Siruganur, Tiruchirappalli-621 105.

Submitted for the project Viva-Voce Examination held on

INTERNAL EXAMINER

EXTERNAL EXAMINER

ACKNOWLEDGEMENT

We greatly express our sincere gratitude and profound thanks to our Honourable Chairman **Mr.M.ABDUL MAJEDU**, Secretary **Dr.M.A.MOHAMMED NIZAM**, Director **Dr.V.SHANMUGANATHAN**, M.A.M College of Engineering for rendering their full support and encouragement towards the truthful completion of this project.

We express our deep sense of gratitude and profound thanks to our Principal **Dr.S.RAVIMARAN, M.E., Ph.D.**, who gave this great opportunity to complete the project efficiently.

We are highly indebted to **Dr.G.KALPANADEV, M.E., Ph.D.**, Head of the Department of INFORMATION TECHNOLOGY for her support and guidance during the entire course of our project. I express my heartfelt thanks for her assistance and valuable suggestion.

We thank our Guide **Mrs.K.UDHAYA SURIYA, M.E.**, for moral support during the span of our project. Also, we like to thank our staff members for their valuable ideas and resourceful guidance.

Finally, we thank our parents and all our friends who provided some valuable insight throughout this work and without whose effort the project would not have come true.

Simplistic Online Voting System

ABSTRACT

In view of traditional voting environment, voting process is quite troublesome because of disinclination of voters to visit booth. Huge transformation in computer technology has implored us to propagate an online voting system which is much more accessible, favourable and adequate. A new way of voting cracks the limitation of traditional voting and focuses on the security and performability of the voting, so that it can reach to “Each and Every” voter. The online voting system provides a convenient, easy and efficient way to vote eliminating the shortcomings of traditional approach. The proposed project is to build an E-Voting system which is basically an online voting system through which people can cast their vote through internet. To achieve the required security OTP (one time password) and Fingerprint verification approach is used, which is most common on the web to tell the difference between a human using a web service and an automated bot thus making the website more secure against spam- bot attacks. So that fraudulent can be eliminated using this technique. Multiple voting’s are eliminated by checking particular voter already polled their vote or not. If the voter already polled their vote they will not be allowed to vote again.

TABLE OF CONTENTS

CHAPTER NO	TITLE	PAGE NO
	ABSTRACT	4
	LIST OF TABLES	8
	LIST OF FIGURES	8
1	INTRODUCTION	10
	1.1 FINGERORINT VERFICATION AND ENCODING	11
	1.2 OTP VERIFICATION	13
	1.3 BLOCKCHAIN	15
	1.3.1 BLOCKCHAIN TRANSACTION	17
2	LITERATURE SURVEY	19
3	OBJECTIVES	24
4	SYSTEM ANALYSIS	26
	4.1 EXISTING SYSTEM	26
	4.1.1 PAPER-BASED VOTING	26
	4.1.2 LEVER VOTING MACHINE	26
	4.1.3 PUNCH CARD	27
	4.2 DISADVANTAGES	27
	4.3 PROPOSED SYSTEM	27
	4.4 ADVANTAGES	27

CHAPTER NO	TITLE	PAGE NO
5	ALGORITHMS	28
	5.1 BASE64 ALGORITHMS	28
	5.1.1 BASE64 ENCODING PROCESS	28
	5.2 PROOF OF AUTHORITY (POA) BLOCKCHAIN	29
	5.2.1 DISTRICT NODE	30
	5.2.2 BOOTNODE	30
6	DEVELOPMENT ENVIRONMENT	31
	6.1 HARDWARE REQUIREMENTS	31
	6.2 SOFTWARE REQUIREMENTS	31
7	SOFTWARE ENVIRONMENT	32
	7.1 PHP	32
	7.1.1 INTRODUCTION TO PHP	32
	7.1.2 FEATURES OF PHP	33
	7.1.3 COMMON USES OF PHP	34
	7.1.4 CHARACTERISTICS OF PHP	34
	7.2 CODEIGNITER	35
	7.2.1 INTRODUCTION TO CODEIGNITER	35
	7.2.2 CODEIGNITER FEATURES	35
	7.2.3 CODEIGNITER APPLICATION ARCHITECTURE	36
	7.2.4 DIRECTORY STRUCTURE OF CODEIGNITER	37

CHAPTE NO	TITLE	PAGE NO
8	SYSTEM SPECIFICATION	38
	8.1 HARDWARE SYSTEM CONFIGURATION	38
	8.2 SOFTWARE SYSTEM CONFIGURATION	38
	8.3 MFS100 OPTICAL FINGERPRINT SENSOR	38
9	IMPLEMETATION	39
	9.1 INTRODUCTION	39
	9.2 VOTER MODULE	39
	9.3 ADMIN MODULE	42
	9.3.1 CANDIDATE MODULE	44
	9.3.2 VOTING MODULE	46
	9.3.3 VOTERS MODULE	48
	4.3.4 SETTINGS MODULE	48
10	CONCLUSION	52
	REFERENCE	53

LIST OF TABLES

TABLE NO	TITLE	PAGE NO
1.1	STRUCTURE OF THE BLOCKCHAIN	15
5.1	BASE64 ENCODING/DECODING TABLE	28

LIST OF FIGURES

FIGURE NO	TITLE	PAGE NO
1.1	BASIC FUNCTION OF THE SHA-256 HASH	16
1.2	CREATION OF NEW BLOCK CONTAINING A HASH VALUE AND A VOTE	17
1.3	A SIMPLE REPRESENTATION OF THE BLOCKCHAIN STRUCTURE OF EACH CANDIDATE	18
5.1	VOTING SYSTEM BLOCKCHAIN	30
7.1	CODEIGNITER APP ARCHITECTURE	36
7.2	DIRECTORY STRUCTURE OF CODEIGNITER	37
7.3	MFS100 OPTICAL FINGERPRINT SENSOR	38
9.1	VOTER LOGIN PAGE	39
9.2	OTP VERIFICATION PAGE	40
9.3	FINGERPRINT VERIFICATION PAGE	40

FIGURE NO	TITLE	PAGE NO
9.4	PASSWORD RESET PAGE	41
9.5	VOTING PAGE	42
9.6	VOTING PAGE AFTER VOTED	42
9.7	ADMINISTRATOR LOGIN PAGE	43
9.8	ADMINISTRATOR WELCOME PAGE	43
9.9	CANDIDATES PAGE	44
9.10	ADD CANDIDATE OVERLAY	45
9.11	EDIT CANDIDATE OVERLAY	45
9.12	VOTING MANAGEMENT PAGE	46
9.13	VOTING PAGE BEFORE CONDUCTING VOTING PROCESS	47
9.14	VOTERS PAGE	47
9.15	EDIT VOTER OVERLAY	48
9.16	SETTINGS PAGE	48
9.17	VOTER REGISTRATION PROCESS FLOW DIAGRAM	50
9.18	VOTING PROCESS FLOW DIAGRAM	51

CHAPTER 1

INTRODUCTION

Voting system is the pillar of every democracy in which voters choose their leaders to show their presence for the way that they will be supervised. Voting scheme have grown from counting hands in previous days to system that include papers, punch card, optical scan machine and mechanical lever i.e., to the electronic voting system. This traditional voting system is the time-consuming process therefore maximum of people is not able to vote because of their busy schedule.

The fundamental idea behind secure online voting system to conquer inability of the conventional voting system as it suffers from various drawbacks such as it consumes huge volume of paper work, time, there is no personal role of higher officers, damage of electronic machines due to lack of attention. Secure online voting system is the system through which any voter can vote from anywhere at any time.

Our main goal is to implement a system which will animate maximum number of voters to cast their vote remotely which will reduce time consumption and hence there will be increase in voting. This system is twofold system incorporating website voting system which ensures much more transparency and security.

1.1 FINGERPRINT VERIFICATION AND ENCODING

Biometrics, using unique data about a person's physical characteristics for identification, is more secure and convenient than traditional methods of personal recognition. However, the use of sensitive data also brings some privacy and security concerns. To solve the problems in case a biometric template is compromised, we must make sure the biometric data is safe and secure.

For that Instead of storing the original biometric data in the system database during enrolment, the system stores only its encoded data. Base64 encoding algorithm is used to formats to represent arbitrary binary data as text. Base64 is part of the MIME email protocol, used to encode binary attachments. Base64 is included in the standard libraries of popular programming languages such as Java, C#, Swift, PHP, Python, Rust, JavaScript, and Go. Major database systems such as Oracle and MySQL include base64 functions.

On the Web, we often combine binary resources (images, videos, sounds) with text-only documents (XML, JavaScript, HTML). Before a Web page can be displayed, it is often necessary to retrieve not only the HTML document but also all of the separate binary resources it needs. The round-trips needed to retrieve all of the resources are often a performance bottleneck. Consequently, major websites such as Google, Bing, and Baidu deliver small images within HTML pages using the data URI scheme.

A data URI takes the form “data:<content type>;base64,<base64 data>.” where the text “R0lGODl ...” is a base64 representation of the binary data of a GIF image. Data URIs are supported by all major browsers. We estimate that billions of pages containing base64 data are loaded every day.

Base64 formats encode arbitrary bytes into a stream of characters chosen from a list of 64 ASCII characters. Three arbitrary bytes can be thus encoded using four ASCII characters. Though base64 encoding increases the number of bytes by 33%, this is alleviated by the commonly used text compression included in the HTTP protocol. The size difference, after compression, can be much smaller than 33% and might even be negligible.

Base64 can also be used for security and privacy purposes. Credentials are often stored and transmitted using base64, e.g., in the HTTP Basic authentication method.

Encoding and decoding base64 data is fast. We do not expect base64 decoding to be commonly a bottleneck in Web browsers. Yet it can still be much slower to decode data than to copy it: e.g., memcopy may use as little as 0.03 cycles per byte while a fast base64 decoder might use 1.8 cycles per byte on the same test (and be 60× slower), see Table 6. Because base64 is ubiquitous and used on a massive scale within servers and database systems, there is industry interest in making it run faster.

1.2 OTP VERIFICATION

One-Time Password is a password system where passwords can only be used once and the user has to be authenticated with a new password key each time. This guarantee the safety even if an attacker is tapping password in network or a user loses it. Besides, OTP features anonymity, portability, and extensivity, and enables to keep the information from being leaked. The type of OTP generate device is smart card, USB, fingerprint recognition and so on. Our propose Online Banking Authentication System use Mobile OTP, one of the OTP generate device which has same security as the existing OTP and with the convenience of mobile features, and the used of semi-permanent. This reduction in acquisition costs as well as easy to download the brother deployment, if the introduction of financial. In addition, user does not require a separate cost except for the initial download costs.

An OTP is a generated password which only valid once. The user is given a device that can generate an OTP using an algorithm and cryptographic keys. On the server side, an authentication server can check the validity of the password by sharing the same algorithm and keys.

Several software or devices can be used to generate the OTP, for example personal digital assistants, mobile phones, dedicated hardware tokens as it the most secure smart cards is devices among all the OTP generator provide tamper-resistant two-factor authentication: a PIN to unlock the OTP generator

(something you know), and the OTP smart card itself (something you have). Figure 1 illustrates the three steps that required to generate an OTP: the collection of some external data, such as the time for synchronous OTP or a challenge for an asynchronous OTP, a ciphering algorithm with secret keys shared by the device and the authentication server, and finally a formatting step that sets the size of the OTP to typically six to eight digits.

Until recently, OTP solutions were based on proprietary and often patented time-based or event-based algorithms. In 2005, OATH-HOTP [6] was defined as an open standard by major actors in the industry. This open standard allows multisource of the OTP generating devices and authentication servers from different vendors. The HOTP algorithm is based on a secret key and a counter shared by the device and the server, and uses standard algorithms such as SHA-1 and HMAC.

OTP has carried more advantages over PKI as it does not require the deployment of smart card readers, drivers and PC software. However in terms of features, OTP only provides identification and authentication, whereas PKI provides addition encryption and signature. OTP being a password-based authentication is also vulnerable to man-in-the-middle attacks, such as phishing scams. Since there is no mutual authentication of the PC and the internet service provider server, an attacker can intercept an OTP using a mock-up site, and impersonate the user to the real internet web site.

1.3 BLOCKCHAIN

Blockchain was first introduced by Satoshi Nakamoto (a pseudonym), who proposed a peer-to-peer payment system that allows cash transactions through the Internet without relying on trust or the need for a financial institution. Blockchain is secure by design, and an example of a system with a high byzantine failure tolerance.

Bitcoin is considered the first application of the Blockchain concept to create a currency that could be exchanged over the Internet relying only on cryptography to secure the transactions. Blockchain is an ordered data structure that contains blocks of transactions. Each block in the chain is linked to the previous block in the chain. The first block in the chain is referred to as the foundation of the stack. Each new block created gets layered on top of the previous block to form a stack called a Blockchain.

Field	Description	Size
Block Size	The size of the whole block.	4 bytes
Block Header	Encrypted almost unique Hash.	80 bytes
Transaction Counter	The number of transactions that follow.	1 to 9 bytes
Transaction	Contains the transaction saved in the block.	Depends on the transaction size.

Table 1.1 Structure of the Blockchain

Each block in the stack is identified by a hash placed on the header. This hash is generated using the Secure Hash Algorithm (SHA-256) to generate an almost idiosyncratic fixed-size 256-bit hash. The widely used algorithm was designed by the National Security Agency (NSA) in 2001 and was used as the protocol to secure all federal communications. The SHA-256 will take any size plaintext as an input, and encrypt it to a 256-byte binary value. The SHA-256 is always a 256-bit binary value, and it is a strictly one-way function. The figure 2 below shows the basic logic of the SHA-256 encryption.



Fig 1.1 Basic Function of the SHA-256 Hash

Each header contains information that links a block to its previous block in the chain, which creates a chain linked to the very first block ever created, which is referred to as the foundation. The primary identifier of each block is the encrypted hash in its header. A digital fingerprint that was made combining two types of information: the information concerning the new block created, as well as the previous block in the chain.

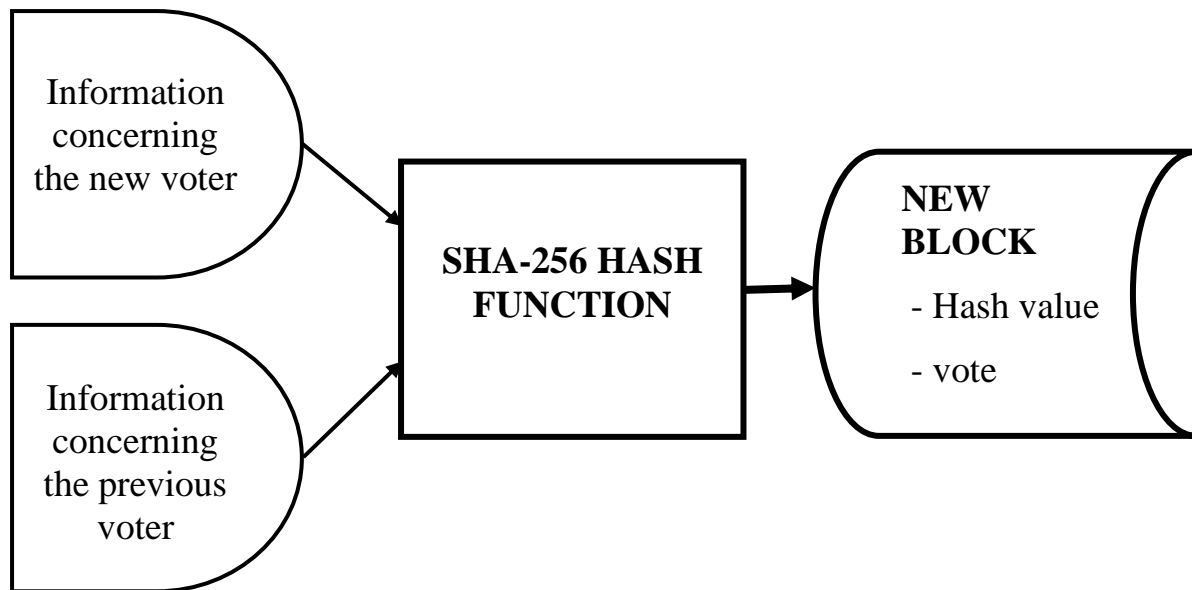


Fig 1.2 Creation of new Block containing a Hash Value and a Vote

As soon as a block is created, it is sent over the Blockchain. The system will keep an eye on incoming blocks continuously update the chain when new blocks arrive.

1.3.1 BLOCKCHAIN TRANSACTION

The first transaction added to the block will be a special transaction that represents the candidate. When this transaction is created it will include the candidate's name and will serve as the foundation block, with every vote for that specific candidate placed on top of it. Unlike the other transactions, the foundation will not count as a vote, and it will only contain the name of the candidate. Our e-Voting system will allow a protest vote, where the voter may return a blank vote to demonstrate dissatisfaction with all candidates or a refusal

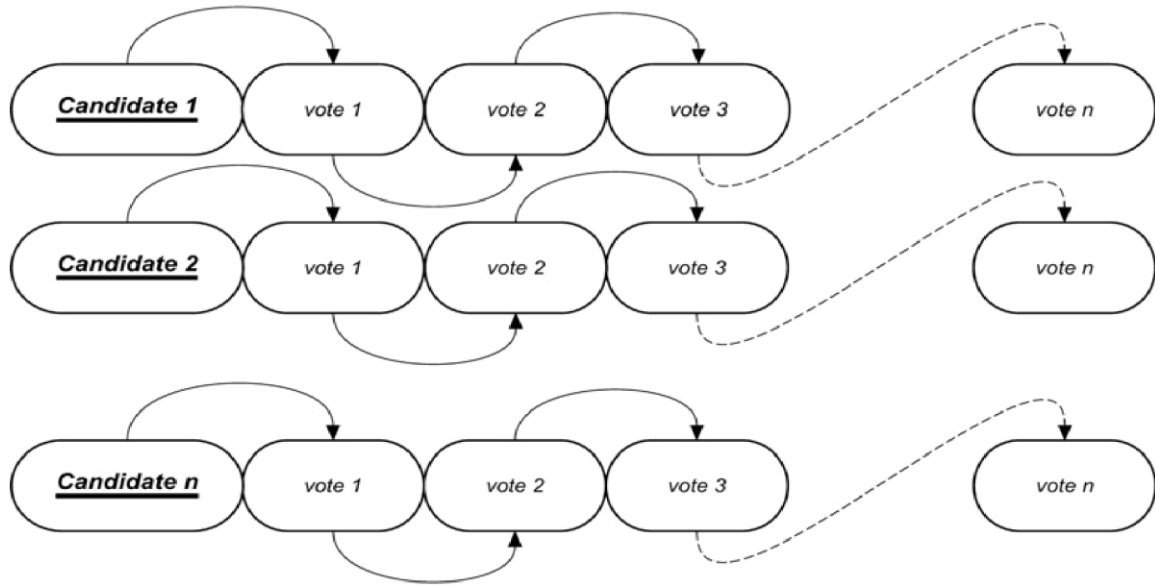


Fig 1.3 A Simple Representation of the Blockchain Structure of each Candidate

of the current political system and/or election. Every time a person votes the transaction gets will be recorded and the Blockchain will be updated.

To ensure that the system is secure, the block will contain the previous voter's information. If any of the blocks were compromised, then it would be easy to find out since all blocks are connected to each other. The Blockchain is decentralized and cannot be corrupted; no single point of failure exists. The Blockchain is where the actual voting takes place. The user's vote gets sent to one of the nodes on the system, and the node then adds the vote to the Blockchain. The voting system will have a node in each district to ensure the system is decentralized.

This system proposes a new e-voting system based on the identified voting requirements and blockchain as a service. We explain the setup of the blockchain, define the smart contract for e-voting that will be deployed on the blockchain and show how the proposed system satisfies the envisioned voting requirements.

CHAPTER 2

LITERATURE SURVEY

2.1 LITERATURE SURVEY 1

TITLE:

Performance Improvement using Pseudorandom One Time Password
(OTP) in Online Voting System.

AUTHOR:

Preeti Ahlawat, Rainu Nandal.

ABSTRACT:

In today's world of growing advanced mobile technologies, the traditional voting method can be changed to a newer and effective approach termed as mobile voting. The Mobile voting system provides a convenient, easy and efficient way to vote eliminating the shortcomings of traditional approach. In this paper we propose to build an E-Voting system which is basically an online voting system through which people can cast their vote through their smart phones or by using an e-voting website. To achieve the required security, we are using OTP (one time password) approach, which is most commonly on the web to tell the difference between a human using a web service and an automated bot thus making the website more secure against spam- bot attacks. If the results of the matching algorithm are three-point match then checks whether this person own

voter ID after that it will check with AADHAAR ID, If he has the right to vote then a voting form is presented to him, and the third level of authentication is carried out by using One Time Password (OTP) principle. The OTP principle emphasizes that each time the user tries to log on, the algorithm produces pseudorandom output thus improving the security. The result shows that the proposed algorithm capable of finding over 90% of the faces in database and allows their voter to vote in approximately 58 seconds. choices regarding exact issues, pieces of rule, citizen initiatives, constitutional amendments, recalls and/or to select their government and political representatives. To allow the use of this right, almost all voting systems around the world contain the following steps: Voter identification and authentication, voting and recording of votes cast, vote counting, publication of election results. Voter identification is required during of the electoral process:

1. first for voter registration in direction to establish the right to vote and then, at voting time, to allow a citizen to use their right to vote by authenticating if the person satisfies all the requirements needed to vote (authentication).
2. Security is important of the e-voting process. Therefore, the necessity of designing a secure e-voting system is very important. Generally, mechanisms that ensure the security and privacy of an election can be time consuming, expensive for election administrators, and inconvenient for voters.

2.2 LITERATURE SURVEY 2

TITLE:

Blockchain-Based E-Voting System.

AUTHOR:

Friðrik Þ. Hjálmarsson, Gunnlaugur Mohammad Hamdaqa, Gísli
Hjálmtýsson.

ABSTRACT:

Building a secure electronic voting system that offers the fairness and privacy of current voting schemes, while providing the transparency and flexibility offered by electronic systems has been a challenge for a long time. In this work-in-progress paper, we evaluate an application of blockchain as a service to implement distributed electronic voting systems. The paper proposes a novel electronic voting system based on blockchain that addresses some of the limitations in existing systems and evaluates some of the popular blockchain frameworks for the purpose of constructing a blockchain-based e-voting system. In particular, we evaluate the potential of distributed ledger technologies through the description of a case study; namely, the process of an election, and the implementation of a blockchain based application, which improves the security and decreases the cost of hosting a nationwide election.

2.3 LITERATURE SURVEY 3

TITLE:

Fingerprint Voting System Using Arduino.

AUTHOR:

A.Piratheepan, S.Sasikaran, P.Thanushkanth, S.Tharsika, M.Nathiya,
C.Sivakaran, N.Thiruchchelvan and K.Thiruthanigesan.

ABSTRACT:

Fingerprint Voting System was implemented with the Arduino technology. In this System a voter can poll his vote easily. In this database server all voter's information was stored to register in this system, the voter should fill a registration form with the help of a user id and password. This information will be checked by the database server. Because all the information about the voter would be already there is anything wrong, the system will not allow the voter to poll his or her vote. This system is helpful to the voter's decreases the time of voting process also. It is more Secured way. Fingerprint is an important identity of the user. Fingerprint Voting System is user-friendly. It has simple architecture, responses very quickly manner, It reduce the polling time, Easy to carrying to polling centre from the polling box, Reduce the staff of voting centre, It provide easy and accurate counting without any troubles.

2.4 LITERATURE SURVEY 4

TITLE:

Faster Base64 Encoding and Decoding Using AVX2 Instructions.

AUTHOR:

WOJCIECH MUŁA and DANIEL LEMIRE.

ABSTRACT:

Web developers use base64 formats to include images, fonts, sounds, and other resources directly inside HTML, JavaScript, JSON, and XML files. We estimate that billions of base64 messages are decoded every day. We are motivated to improve the efficiency of base64 encoding and decoding. Compared to state-of-the-art implementations, we multiply the speeds of both the encoding ($\approx 10\times$) and the decoding ($\approx 7\times$). We achieve these good results by using the single-instruction-multiple-data instructions available on recent Intel processors (AVX2). Our accelerated software abides by the specification and reports errors when encountering characters outside of the base64 set. It is available online as free software under a liberal license.

CHAPTER 3

OBJECTIVES

The most crucial factor for a system like e-VOTE to be successful is to exhibit a Voting Protocol that can prevent opportunities for fraud or for sacrificing the voter's privacy. The Voting Protocol that will be designed and implemented for the e-VOTE system will combine the advantages of existing protocols and techniques, while at the same time it will aim at eliminating most of the identified deficiencies and problems. The related attributes that the e-VOTE system will fully support, and against which it will be extensively tested and validated, are listed below. These attributes can be also considered, according to the literature, as a set of criteria for a "good" electronic voting system that can easily enjoy the trust and confidence of the voters and process organizers. i.) Democracy: The system should be "democratic" in the sense that it will permit only eligible voters to vote (eligibility) and it will ensure that each eligible voter can vote only once (unreusability). ii.) Privacy: The system should ensure that none of the actors involved in the voting process (organizers, administrators, voters etc.) can link any ballot (contextually) to the voter who cast it, and that no voter can prove that he or she voted in a particular way (unintractability). iii.) Integrity: The necessary mechanism should be employed in order to guarantee that no one can duplicate his or someone else's vote (duplicability) and no one can change someone else's vote (unchangeability) iv.) Accuracy: The system

functionality should ensure that no one can falsify or modify the result of the voting by eliminating a valid vote or counting an invalid vote in the final tally.

v.) Verifiability: The system should allow and support anyone to independently verify that all votes have been counted correctly. vi.) Convenience: The system should allow and assist voters to cast their votes quickly, in one session, and with minimal equipment or special skills. vii.) Flexibility: The system should allow a variety of ballot formats and it should be customized to the specific characteristics of the voting processes. viii.) Mobility: The system should not pose any restrictions on the location from which a voter can cast a vote. ix.) Efficiency: The election can be held in a timely manner (i.e., all computations during the election are done in a reasonable amount of time and voters are not required to wait on other voters to complete the process). x.) Scalability: The size of the election should not drastically affect performance. In parallel with the development of the aforementioned e-VOTE functionality and the implementation of the associated voting protocol, the consortium will take into account all relevant European legal and regulatory issues that may pose extra requirements or constraints in terms of the functionality, the equipment, or the security measures. Furthermore, legal issues associated with the use of Internet for electronic voting will be explored, clarified and incorporated into the system.

CHAPTER 4

SYSTEM ANALYSIS

4.1 EXISTING SYSTEM

4.1.1 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 labour 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.

4.1.2 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 favourite 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. 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.

4.1.3 Punch card

The voter uses metallic hole-punch to punch a hole on the blank ballot. It can count votes automatically.

4.2 DISADVANTAGES

- The existing system of election is running manually. The voter has to visit to booths to vote a candidate so there is wastage of time.
- Voter must be present in his/her Constituency to give his/her Vote.
- Vote counting has to be done manually.
- There are Electronic voting machines used which takes more cost.

4.3 PROPOSED SYSTEM

- Proposing the new system of online voting system, where the voting is conducted through internet.
- This proposed system will conduct very simply and easily with also take care of all the security needs.
- In this system voters will have to login with their given user id and password and then complete both OTP and Biometric authentications to vote.

4.4 ADVANTAGES

- Voting is very simple and fast voter can vote within 2 mins.
- Voters no need to visit booths to vote a candidate.

CHAPTER 5

ALGORITHMS

5.1 BASE64 ALGORITHM

Base64 encoding takes the original binary data and operates on it by dividing it into tokens of three bytes. A byte consists of eight bits, so Base64 takes 24bits in total. These 3 bytes are then converted into four printable characters from the ASCII standard.

Base64 Encoding/Decoding Table															
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Q	R	S	T	U	V	W	X	Y	Z	a	b	c	d	e	f
16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v
32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
w	x	y	z	0	1	2	3	4	5	6	7	8	9	+	/
48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63

Table 5.1 Base64 Encoding/Decoding Table

5.1.1 Base64 encoding process

1. Divide the input bytes stream into blocks of 3 bytes.
2. Divide 24 bits of each 3-byte block into 4 groups of 6 bits.
3. Map each group of 6 bits to 1 printable character, based on the 6-bit value using the Base64 character set map.

4. If the last 3-byte block has only 1 byte of input data, pad 2 bytes of zero (`\x0000`). After encoding it as a normal block, override the last 2 characters with 2 equal signs (`==`), so the decoding process knows 2 bytes of zero were padded.
5. If the last 3-byte block has only 2 bytes of input data, pad 1 byte of zero (`\x00`). After encoding it as a normal block, override the last 1 character with 1 equal sign (`=`), so the decoding process knows 1 byte of zero was padded.
6. Carriage return (`\r`) and new line (`\n`) are inserted into the output character stream. They will be ignored by the decoding process.

5.2 PROOF OF AUTHORITY (POA) BLOCKCHAIN

In order to satisfy the privacy and security requirements for e-voting, and to ensure that the election system should not enable coerced voting, voters will have to vote in a supervised environment. In our work, we setup a Go-Ethereum permissioned Proof-of-Authority (POA) blockchain to achieve these goals. POA uses an algorithm that delivers comparatively fast transactions through a consensus mechanism based on identity as a stake.

The structure of the blockchain is illustrated in Figure, and mainly consists of two types of nodes.

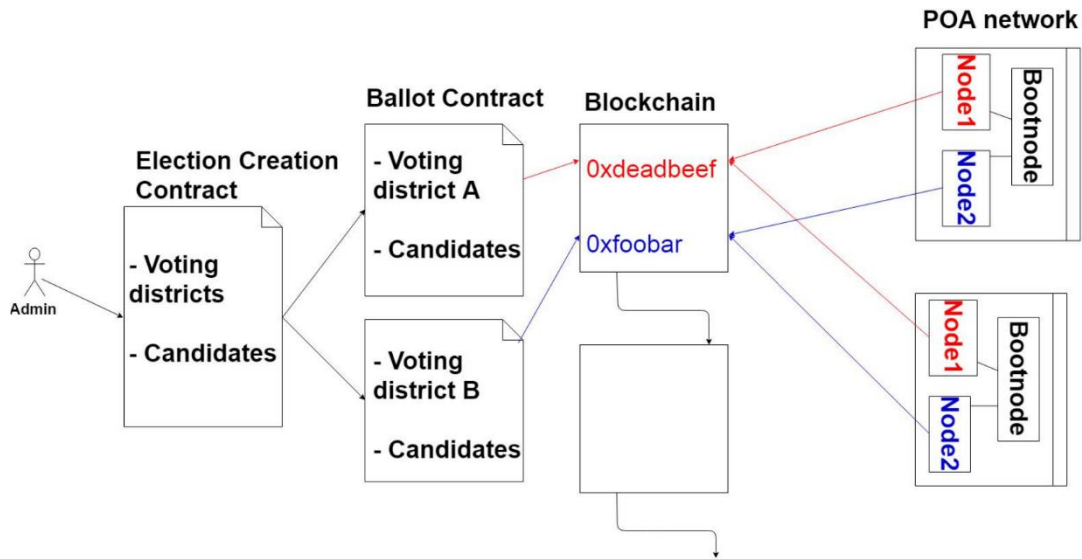


Fig 5.1 Voting system blockchain

5.2.1 District Node

Represent each voting district. Each district node has a software agent that autonomously interacts with the "bootnode" and manages the life cycle of the smart contract on that node. When the election administrator (see smart contract section) creates an election, a ballot smart contract is distributed and deployed onto its corresponding district node.

5.2.2 Bootnode

Each institution, with permissioned access to the network, host a bootnode. A bootnode is a discovery and coordination service that helps the district nodes to discover each other and communicate. The bootnode does not keep any state of the blockchain and is run on a static IP so that district nodes find their peers faster.

CHAPTER 6

DEVELOPMENT ENVIRONMENT

6.1 HARDWARE REQUIREMENTS

Processor	:	Intel Core 2 duo
System Type	:	64 – bit Operating System
RAM	:	4 GB
Hard Disk	:	Minimum 1 GB or Higher
Screen Resolution	:	720P
Input Device	:	Keyboard, Mouse and Fingerprint scanner
Internet Connection	:	5 Mbps Speed

6.2 SOFTWARE REQUIREMENTS

Operating System	:	Windows 10
Programming language	:	PHP
Framework	:	CodeIgniter
IDE	:	Visual Studio code
Version Control	:	Git
Browser	:	Chrome, Firefox

CHAPTER 7

SOFTWARE ENVIRONMENT

7.1 PHP

7.1.1 INTRODUCTION TO PHP

PHP is a general-purpose scripting language geared toward web development. It was originally created by Danish-Canadian programmer Rasmus Lerdorf in 1994. The PHP reference implementation is now produced by The PHP Group. PHP originally stood for Personal Home Page, but it now stands for the recursive initialism PHP: Hypertext Pre-processor.

PHP code is usually processed on a web server by a PHP interpreter implemented as a module, a daemon or as a Common Gateway Interface (CGI) executable. On a web server, the result of the interpreted and executed PHP code which may be any type of data, such as generated HTML or binary image data would form the whole or part of an HTTP response. Various web template systems, web content management systems, and web frameworks exist which can be employed to orchestrate or facilitate the generation of that response. Additionally, PHP can be used for many programming tasks outside the web context, such as standalone graphical applications and robotic drone control. PHP code can also be directly executed from the command line.

The standard PHP interpreter, powered by the Zend Engine, is free software released under the PHP License. PHP has been widely ported and can be deployed on most web servers on a variety of operating systems and platforms.

The PHP language evolved without a written formal specification or standard until 2014, with the original implementation acting as the de facto standard which other implementations aimed to follow. Since 2014, work has gone on to create a formal PHP specification.

W3Techs reports that, as of January 2022, "PHP is used by 78.1% of all the websites whose server-side programming language we know."

7.1.2 FEATURES OF PHP

- ✓ PHP is a server-side scripting language that is embedded in HTML. It is used to manage dynamic content, databases, session tracking, even build entire e-commerce sites.
- ✓ It is integrated with a number of popular databases, including MySQL, PostgreSQL, Oracle, Sybase, Informix, and Microsoft SQL Server.
- ✓ PHP is pleasingly zippy in its execution, especially when compiled as an Apache module on the Unix side. The MySQL server, once started, executes even very complex queries with huge result sets in record-setting time.
- ✓ PHP supports a large number of major protocols such as POP3, IMAP, and LDAP. PHP4 added support for Java and distributed object architectures

(COM and CORBA), making n-tier development a possibility for the first time.

- ✓ PHP is forgiving: PHP language tries to be as forgiving as possible.
- ✓ PHP Syntax is C-Like.

7.1.3 COMMON USES OF PHP

- ✓ PHP performs system functions, i.e., from files on a system it can create, open, read, write, and close them.
- ✓ PHP can handle forms, i.e., gather data from files, save data to a file, through email you can send data, return data to the user.
- ✓ You add, delete, modify elements within your database through PHP.
- ✓ Access cookies variables and set cookies.
- ✓ Using PHP, you can restrict users to access some pages of your website.
- ✓ It can encrypt data.

7.1.4 CHARACTERISTICS OF PHP

Five important characteristics make PHP's practical nature possible,

- ✓ Simplicity
- ✓ Efficiency
- ✓ Security
- ✓ Flexibility
- ✓ Familiarity

7.2 CODEIGNITER

7.2.1 INTRODUCTION TO CODEIGNITER

CodeIgniter is a simple, elegant and powerful toolkit with a very small footprint, used by those developers who want to create full-featured Web Applications. CodeIgniter is an open-source PHP Framework. It has a very rich set of functionalities, which will increase the speed of website development work. As there are various sources through which websites can be developed, but CodeIgniter is preferred over the others.

7.2.2 CODEIGNITER FEATURES

Some of the most important features are mentioned below:

- ✓ CodeIgniter is very simple to configure, as it is an open-source framework.
- ✓ As per our own requirement we can do customization very easily.
- ✓ Those who don't want to waste a lot of time in difficult coding, as coding in PHP is easy to use, simple and very quick.
- ✓ It allows us to well organize the code underlying our webpage easily.
- ✓ The folder structure used here is linear therefore very easy to use.
- ✓ It helps in easy hassle-free migration of server hosting from one to another.
- ✓ CodeIgniter make use of the MVC system to simplify the coding, expedient and reusable.
- ✓ It helps to find out the errors in codes and fix the issues in the web applications.

- ✓ It is user-friendly which help developers to create a dynamic, secure and effective web applications in a short time.
- ✓ Programmers can create web applications as with additional features and high-end functionalities by using in-built resource and libraries of the CodeIgniter.
- ✓ Programmers uses CI because of Fast development. It creates both front-end and rear-end of a web-application in secure and fast manner.
- ✓ Its active record implementation feature is outstanding and quick and easy to remember.

7.2.3 CODEIGNITER APPLICATION ARCHITECTURE

The working of CodeIgniter Application is mentioned in a simple flowchart given below, which will help you understand the entire process effortlessly in easy steps. Each and every step in the flow chart is explained in elaboration and point wise for your easy grasping.

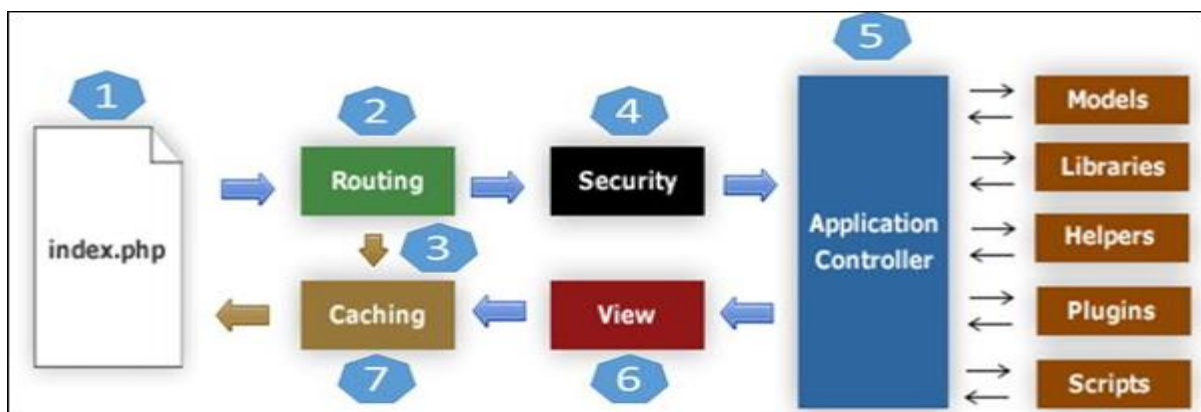


Fig 7.1 CodeIgniter app Architecture

- ✓ As shown in the Flow chart, whenever a request comes to CodeIgniter, it will first go to *index.php* page.
- ✓ In the second step, Routing decides whether to pass the request to step 3 for Caching or to pass the request to step 4 for Security check.
- ✓ If the requested page is already in Caching, then Routing will sanction the request to step 3 and the response will go back to the user.
- ✓ In case the request page does not exist in the Caching, then Routing, will sanction the requested page to step 4 for Security checks.
- ✓ Before passing the request to Application Controller, the Security of the submitted data is checked. After the Security check is done, the Application Controller loads all the necessary Models, Libraries, Helpers, Plugins and Scripts and pass it onto View.
- ✓ The View will provide the page with available data and pass that on for Caching, to process this page quickly for future requests.

7.2.4 DIRECTORY STRUCTURE OF CODEIGNITER

The Directory structure of the CodeIgniter is given in the Screenshot

Image:

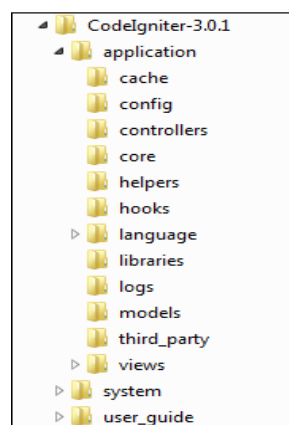


Fig 7.2 Directory structure of CodeIgniter

CHAPTER 8

SYSTEM SPECIFICATION

8.1 HARDWARE SYSTEM CONFIGURATION

- ✓ Any device (mobile, tablet, laptop, computer) with internet connection.
- ✓ Minimum of 2Gb RAM
- ✓ Fingerprint scanner (MFS100).

8.2 SOFTWARE SYSTEM CONFIGURATION

- ✓ Internet browser.

8.3 MFS100 OPTICAL FINGERPRINT SENSOR

MFS100 OPTICAL FINGERPRINT SENSOR - STQC certified single finger scanner. MFS100 is based on optical sensing technology which efficiently recognizes poor quality fingerprints also. MFS100 can be used for authentication, identification and verification functions that let your fingerprint act like digital passwords that cannot be lost, forgotten or stolen. Hard optical sensor is resistant to scratches, impact, vibration and electrostatic shock.



Fig 8.1 MFS100 optical fingerprint sensor

CHAPTER 9

IMPLEMENTATION

9.1 INTRODUCTION

The proposed online voting system contains two main modules,

- a) Voter module
- b) Admin module

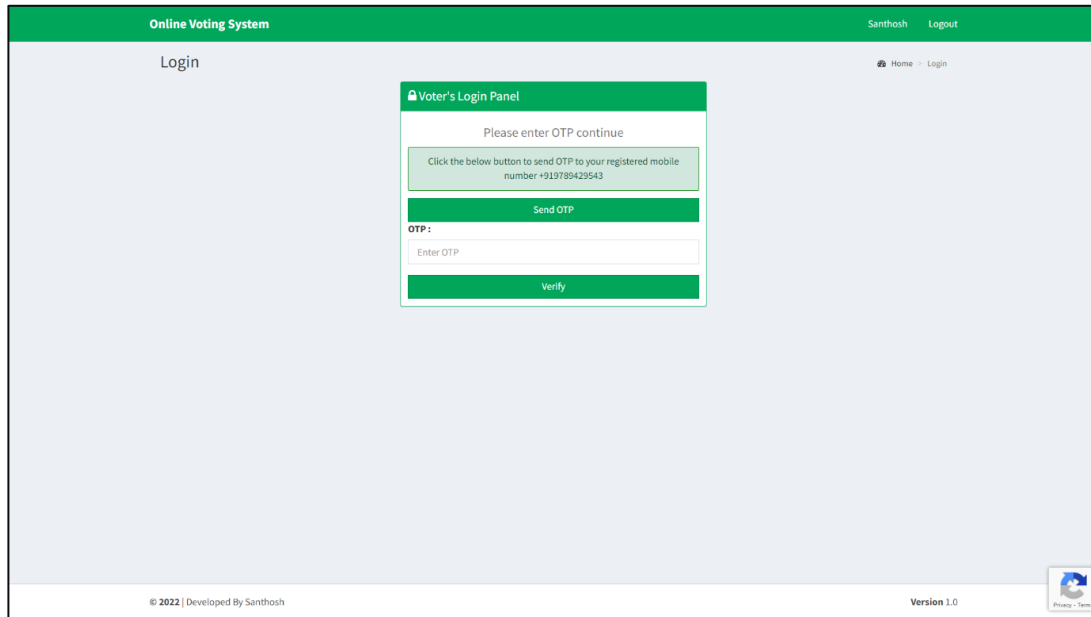
9.2 VOTER MODULE

This module is the module where voters can vote for candidates. This module has access to all the users of the system. In this module first voter have to login with his/her user id and password. After login a six-digit OTP is sent to the voters register mobile number. That OTP is verified by the voter. Next step is to verify the registered fingerprint. After all the steps, voter can choose his/her candidate and vote.

The screenshot displays the 'Voter's Login Panel' within the 'Online Voting System'. The panel is centered on a light blue background. It features a green header bar with the text 'Voter's Login Panel' and a lock icon. Below the header, the text 'Please login to continue' is displayed. The login form includes two input fields: 'Username : Enter Username' and 'Password : Enter Password'. A green 'Login' button with a right-pointing arrow is positioned at the bottom of the form. The overall page layout includes a green top navigation bar with 'Online Voting System' on the left and 'Welcome' on the right. The word 'Login' is visible in the top left of the main content area, and 'Home > Login' is in the top right. The footer contains the copyright notice '© 2022 | Developed By Santhosh' on the left and 'Version 1.0' on the right.

Fig 9.1 Voter login page

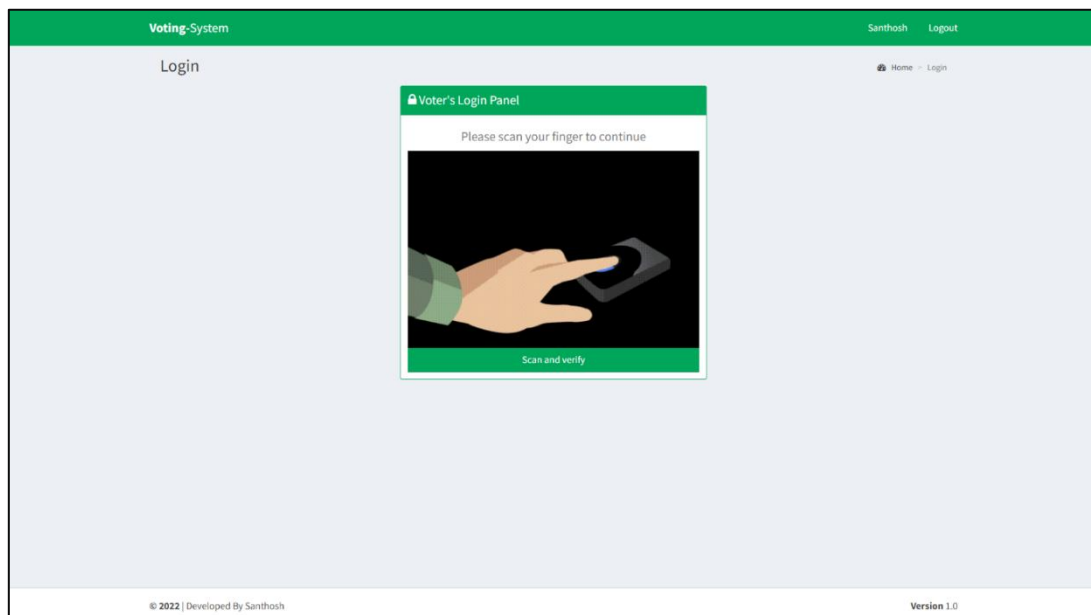
Each voter has a unique voter id and password. Using them they can login the page in the fig 4.1.



The screenshot shows a web application titled "Online Voting System". The header is green with "Santhosh" and "Logout" on the right. The main content area has a light blue background. On the left, there's a "Login" link. In the center, a modal titled "Voter's Login Panel" is displayed. Inside the modal, it says "Please enter OTP continue" and "Click the below button to send OTP to your registered mobile number +919789429543". There is a green "Send OTP" button. Below that, it says "OTP:" followed by an input field labeled "Enter OTP" and a green "Verify" button. The footer contains "© 2022 | Developed By Santhosh" on the left, "Version 1.0" on the right, and a "Privacy - Terms" link with a circular icon on the far right.

Fig 9.2 OTP verification page

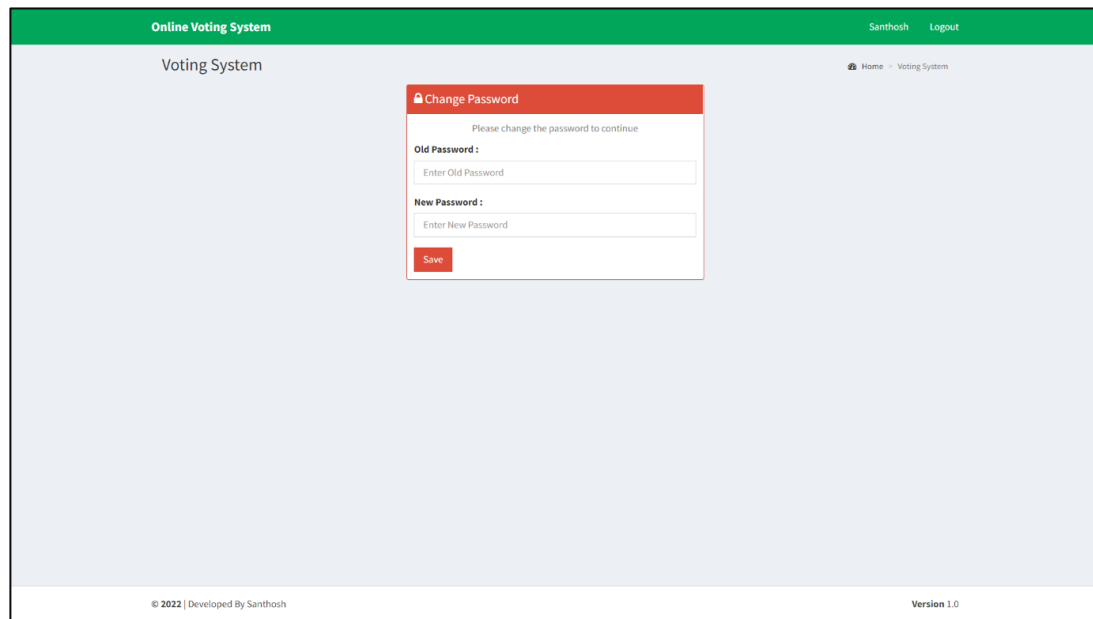
Voters have to authenticate their registered mobile number by clicking the send OTP button and verify the OTP received in their registered mobile number.



The screenshot shows a web application titled "Voting-System". The header is green with "Santhosh" and "Logout" on the right. The main content area has a light blue background. On the left, there's a "Login" link. In the center, a modal titled "Voter's Login Panel" is displayed. Inside the modal, it says "Please scan your finger to continue" above an illustration of a hand scanning a fingerprint. Below the illustration is a green "Scan and verify" button. The footer contains "© 2022 | Developed By Santhosh" on the left, "Version 1.0" on the right, and a "Privacy - Terms" link with a circular icon on the far right.

Fig 9.3 Fingerprint verification page

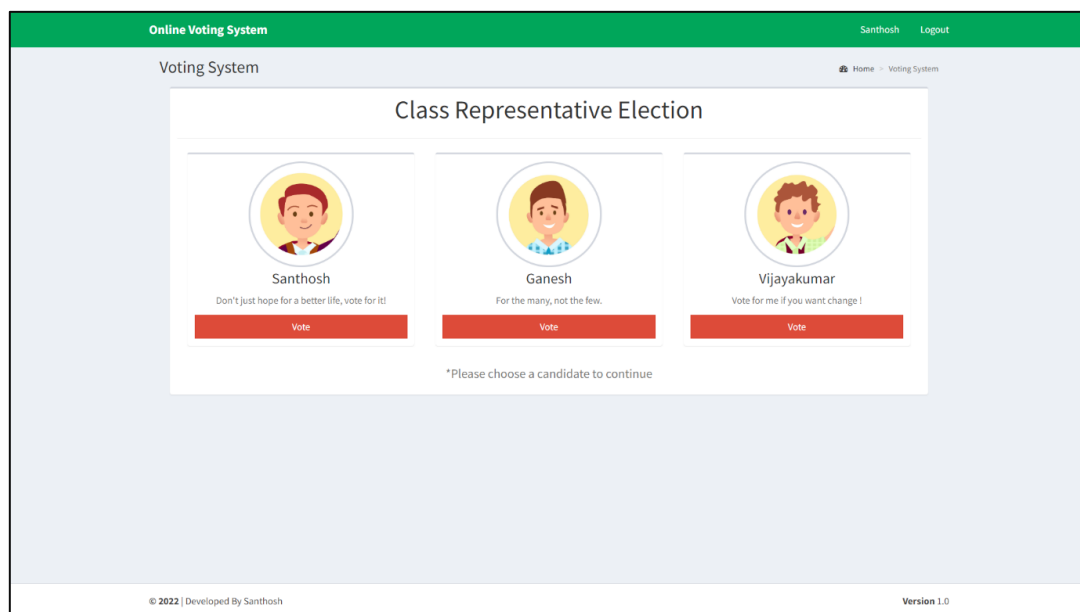
Voters have to verify their fingerprint they gave during the voter registration process for proceeding to the voting page.



The screenshot shows the 'Online Voting System' interface. At the top, there is a green header bar with 'Online Voting System' on the left and 'Santhosh Logout' on the right. Below the header, the page title 'Voting System' is displayed. A central modal window titled 'Change Password' is open, containing the text 'Please change the password to continue'. It has two input fields: 'Old Password' with the placeholder 'Enter Old Password' and 'New Password' with the placeholder 'Enter New Password'. A red 'Save' button is at the bottom of the modal. The footer of the page shows '© 2022 | Developed By Santhosh' on the left and 'Version 1.0' on the right.

Fig 9.4 Password reset page

When a registered voter logged in for the first time they will be asked for reset their password because, when the user id created by administrator the user id and password are to be the same.



The screenshot shows the 'Online Voting System' interface. At the top, there is a green header bar with 'Online Voting System' on the left and 'Santhosh Logout' on the right. Below the header, the page title 'Voting System' is displayed. A central modal window titled 'Class Representative Election' is open. It contains three candidate cards. Each card has a circular profile picture, the candidate's name, a slogan, and a red 'Vote' button. The candidates are Santhosh (slogan: 'Don't just hope for a better life, vote for it!'), Ganesh (slogan: 'For the many, not the few.'), and Vijayakumar (slogan: 'Vote for me if you want change!'). Below the cards, there is a note: '*Please choose a candidate to continue'. The footer of the page shows '© 2022 | Developed By Santhosh' on the left and 'Version 1.0' on the right.

Fig 9.5 Voting page

After all the authentication processes are completed the voter will be presented with the voting page where they can select to which candidate they vote for.

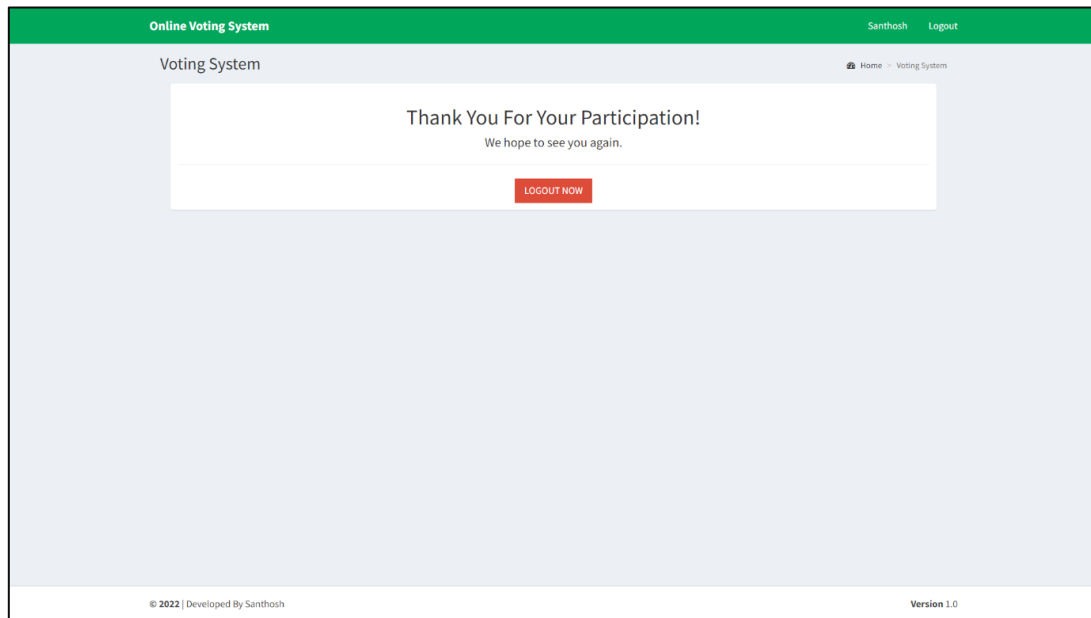


Fig 9.6 Voting page after voted

Once a voter casted their vote they can't visit the voting page again and vote again. Alternatively they will be redirected to this thank you page.

9.3 ADMIN MODULE

This module is only accessible for who owns the system or the administrator of the system. Using this module administrator can conduct voting, add or remove voters, candidates and administrators, view the results of the voting. Administrator module has 4 sub-modules,

- a) Candidate module
- b) Voting module

c) Voter module

d) Settings module

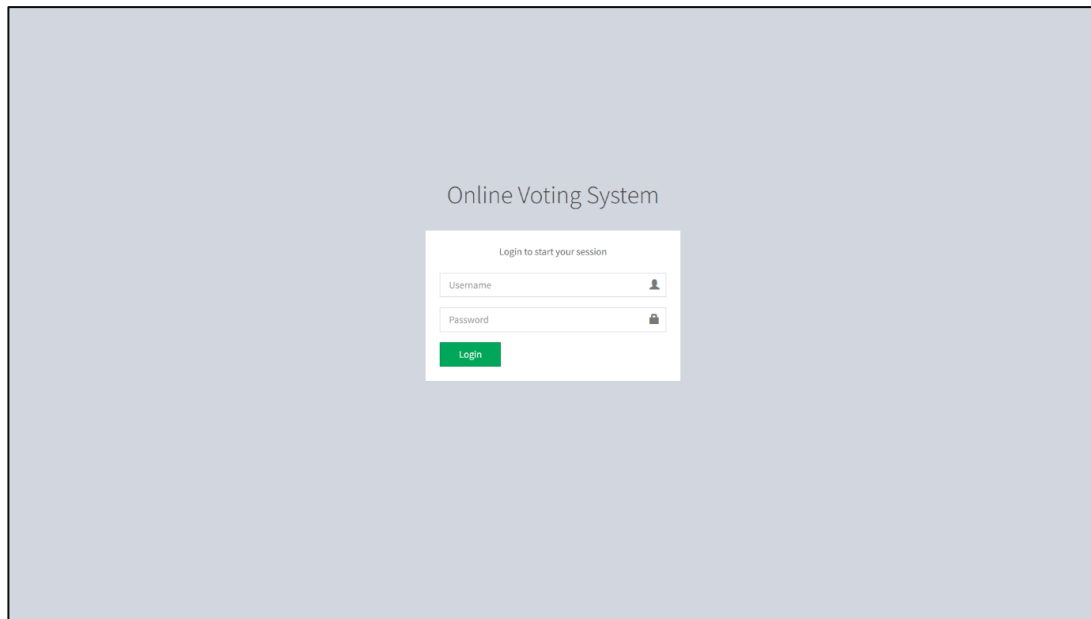


Fig 9.7 Administrator login page

The page shown in the fig 4.7 is responsible for system administrator login. Only administrators can login in this page.

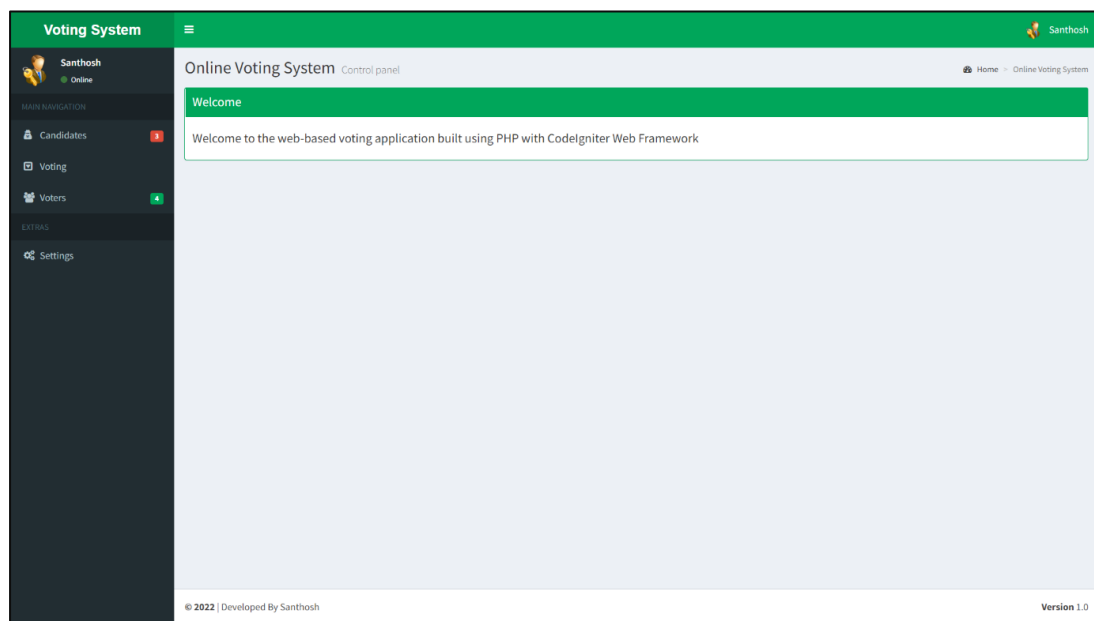


Fig 9.8 Administrator welcome page

When an administrator logged in they will be presented with this welcome page of the administrator module.

9.3.1 Candidate module

This module is responsible for add or remove candidates who participates in the election. Also, the details of the already added candidates can be edited here. Candidates who participate in the current live voting can't be removed or their details can't be edited.

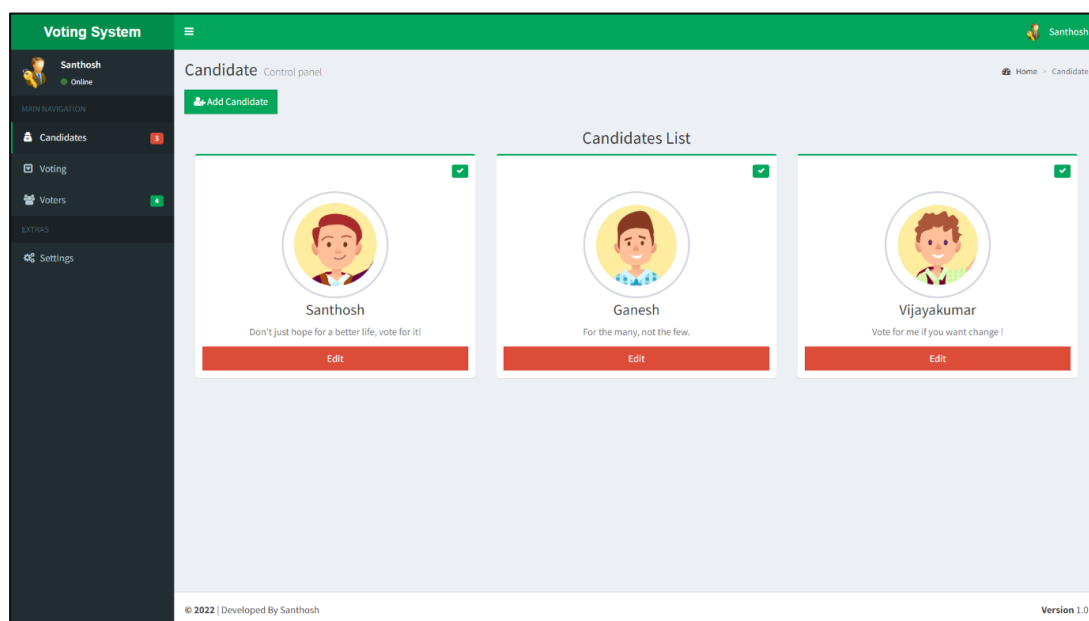


Fig 9.9 Candidates page

This page shows all the candidates registered for the election. And differentiate them by who are participated in the current voting process or not by showing a green tick in the upper right corner of their profile.

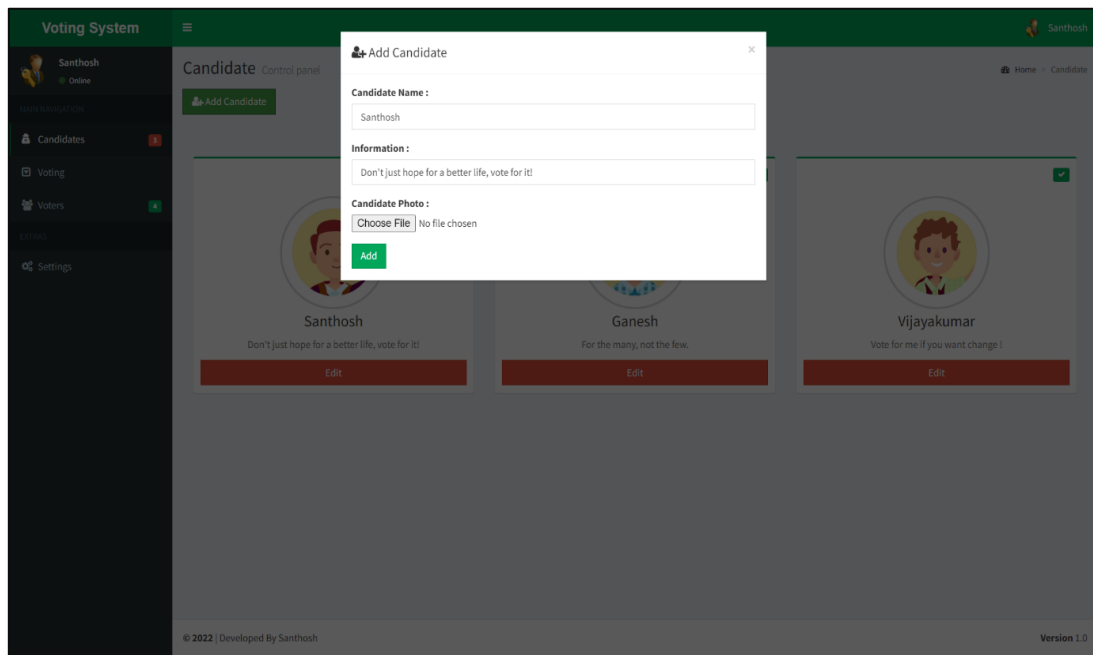


Fig 9.10 Add candidate overlay

Whenever the add candidate button clicked this overlay will popup and asks for the new candidate's information for registration.

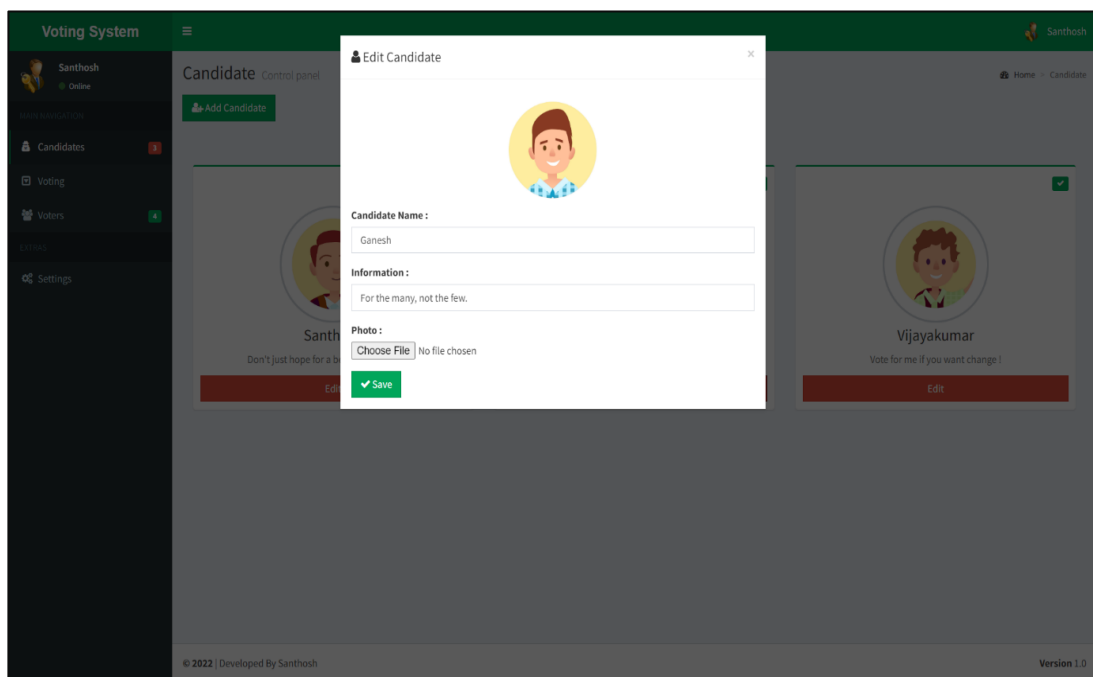


Fig 9.11 Edit candidate overlay

Each candidate's profile has an edit button whenever the button is clicked an overlay will popup and shows the candidate's information for editing.

9.3.2 Voting module

In this module new voting can be added. Topic of the already added voting can be changed. And this module is also responsible for viewing the results of the voting.

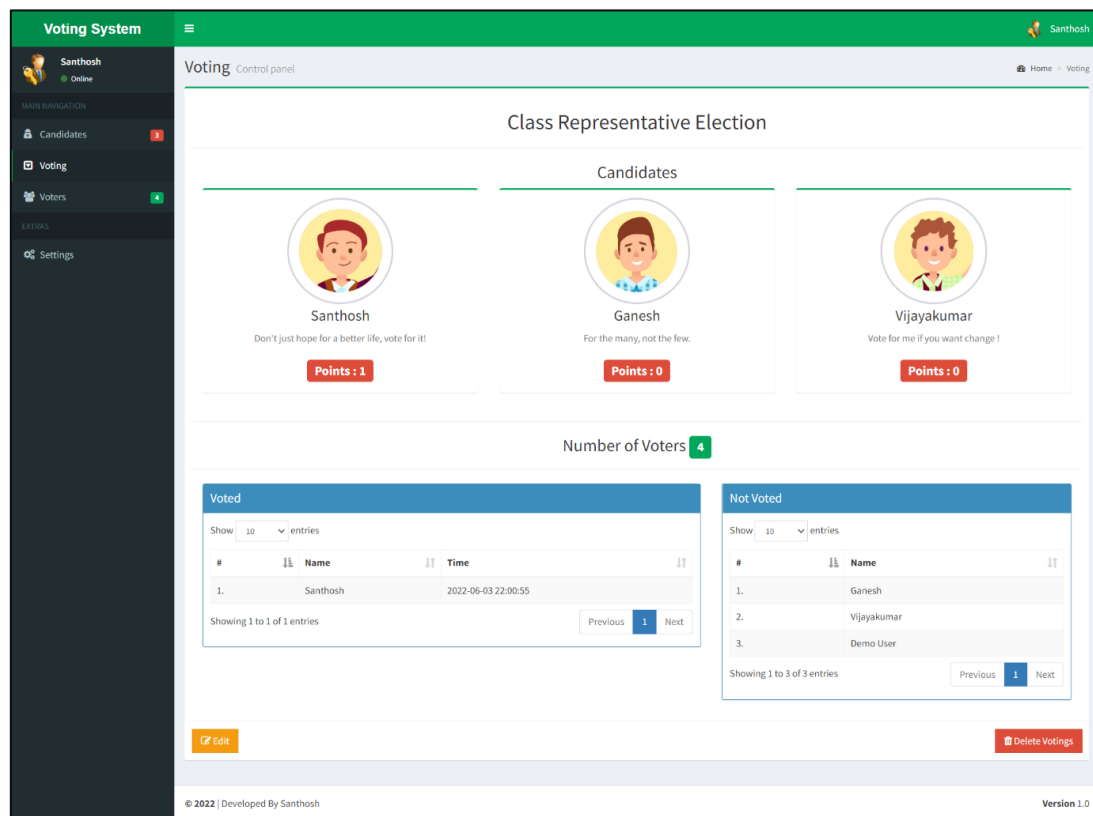


Fig 9.12 Voting management page

The voting process is started from this page by the administrator. Election name and candidates who are participating are chosen from here. And also, all the current live voting details are displayed here like how much vote each candidate got, who are voted and not.

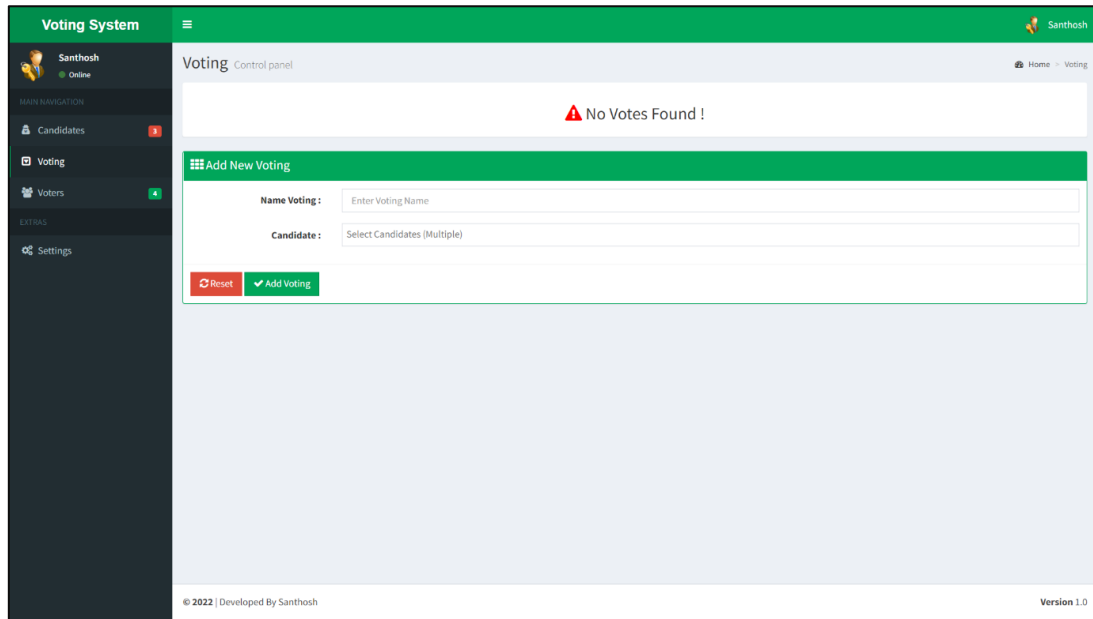


Fig 9.13 Voting page before conducting voting process

Before conducting any voting or after ended the current voting this page will be displayed and asks for details of new voting to conducted.

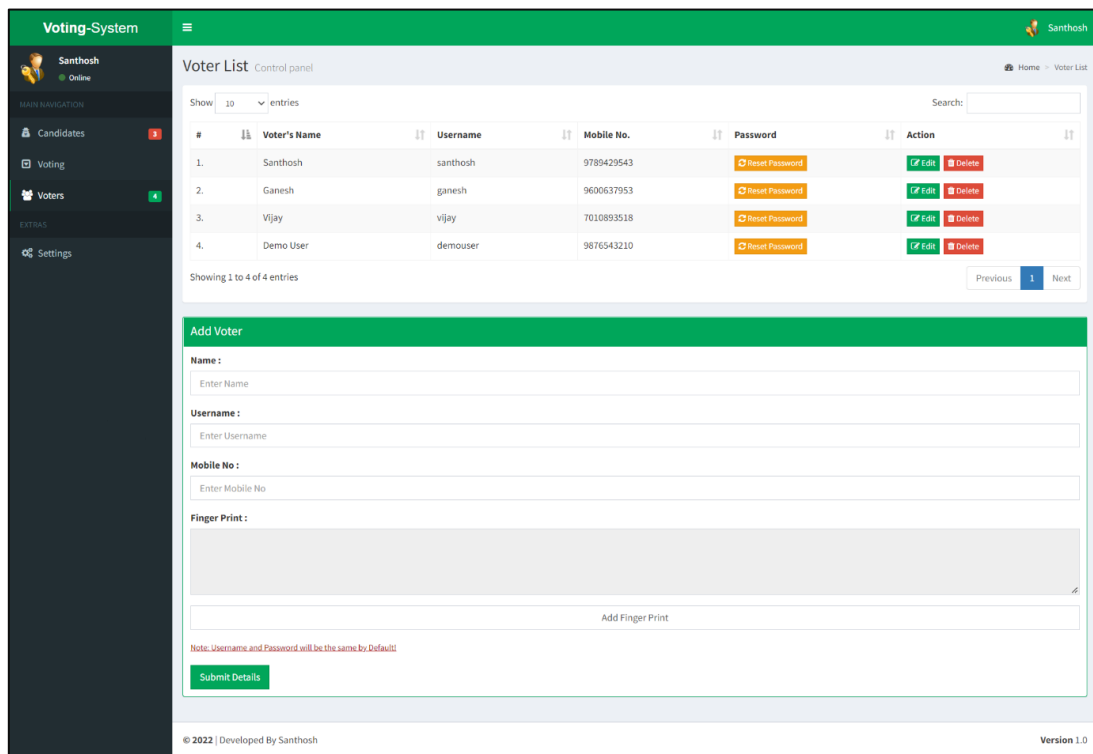


Fig 9.14 Voters page

9.3.3 Voters module

This module is responsible for viewing all the details of the voters. Add or remove voter. Edit voter's registered detailed and reset their password if they want.

This page displays all the details of the voters who are registered in this system. And also this page is responsible for registering new voters to the system.

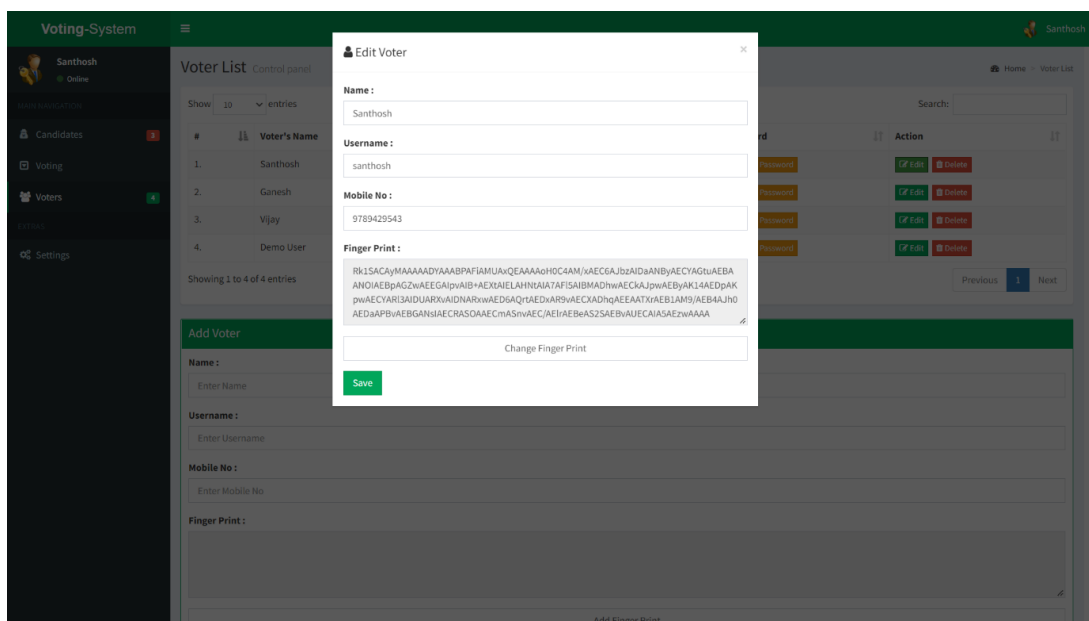


Fig 9.15 Edit voter overlay

Each voter has an edit button. Whenever the button is clicked an overlay will popup and shows the voter's information for editing.

4.3.4 Settings module

This module is responsible for viewing all the details of the administrators and for edit them. It is also responsible for reset the entire application.

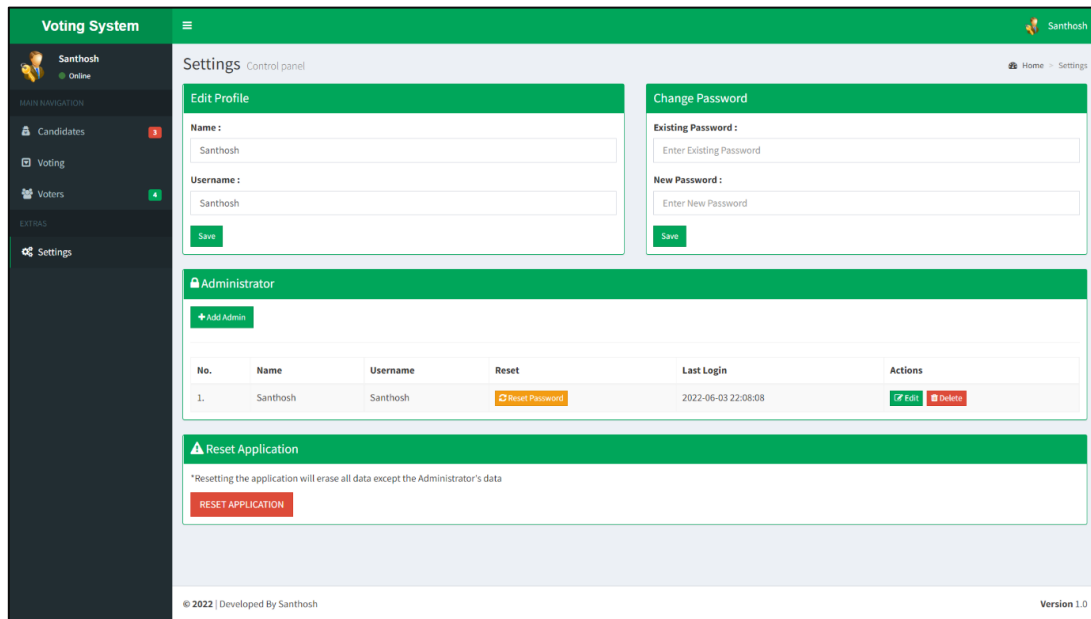


Fig 9.16 Settings page

This page has all the administrator details. It is responsible for adding new administrator, deleting administrator, reset their passwords and edit their details.

This page also has a reset button which will reset the entire application to its original state by deleting all the details including its voter details, candidate detail, election details.

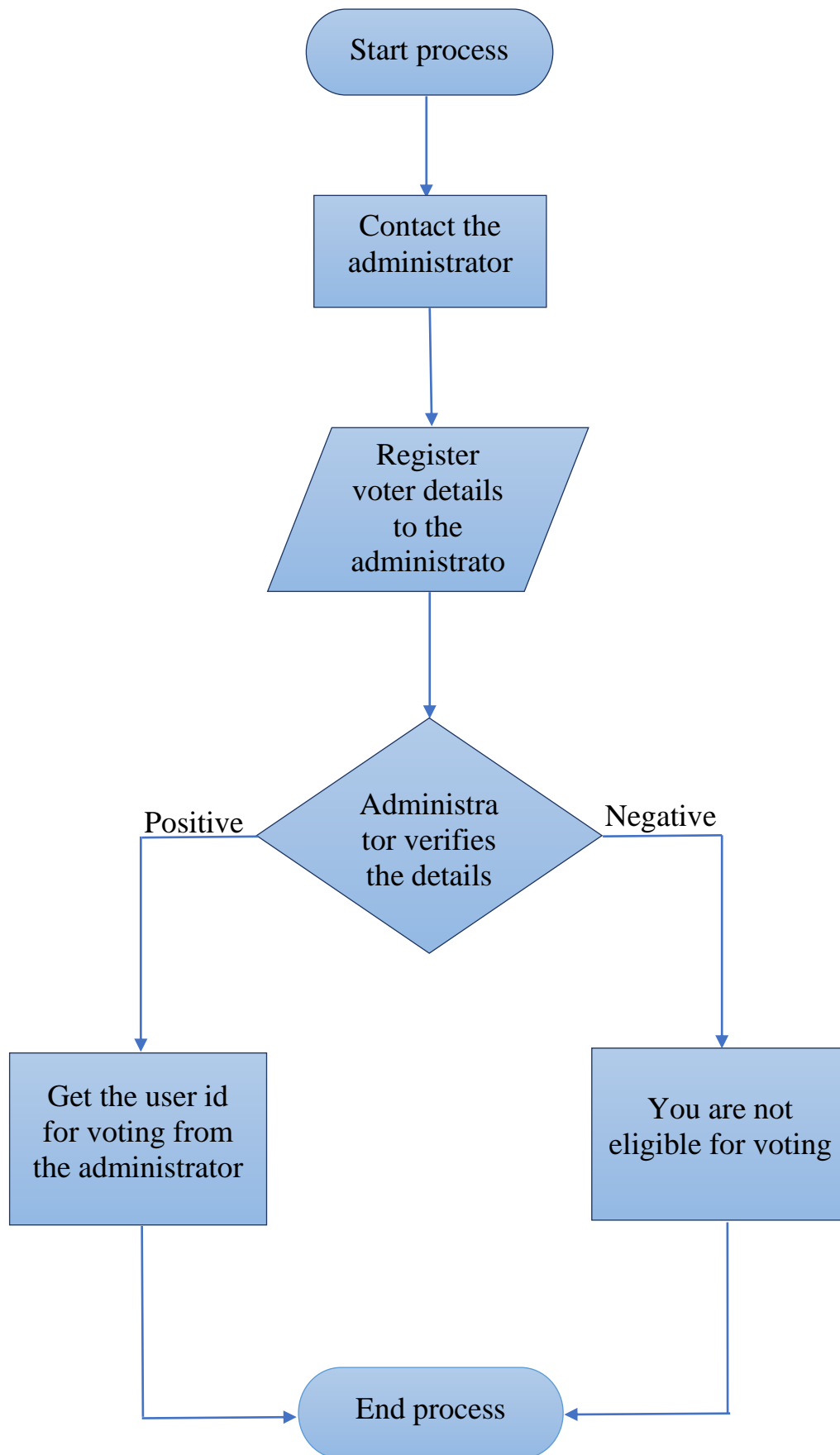


Fig 9.17 Voter registration process flow diagram

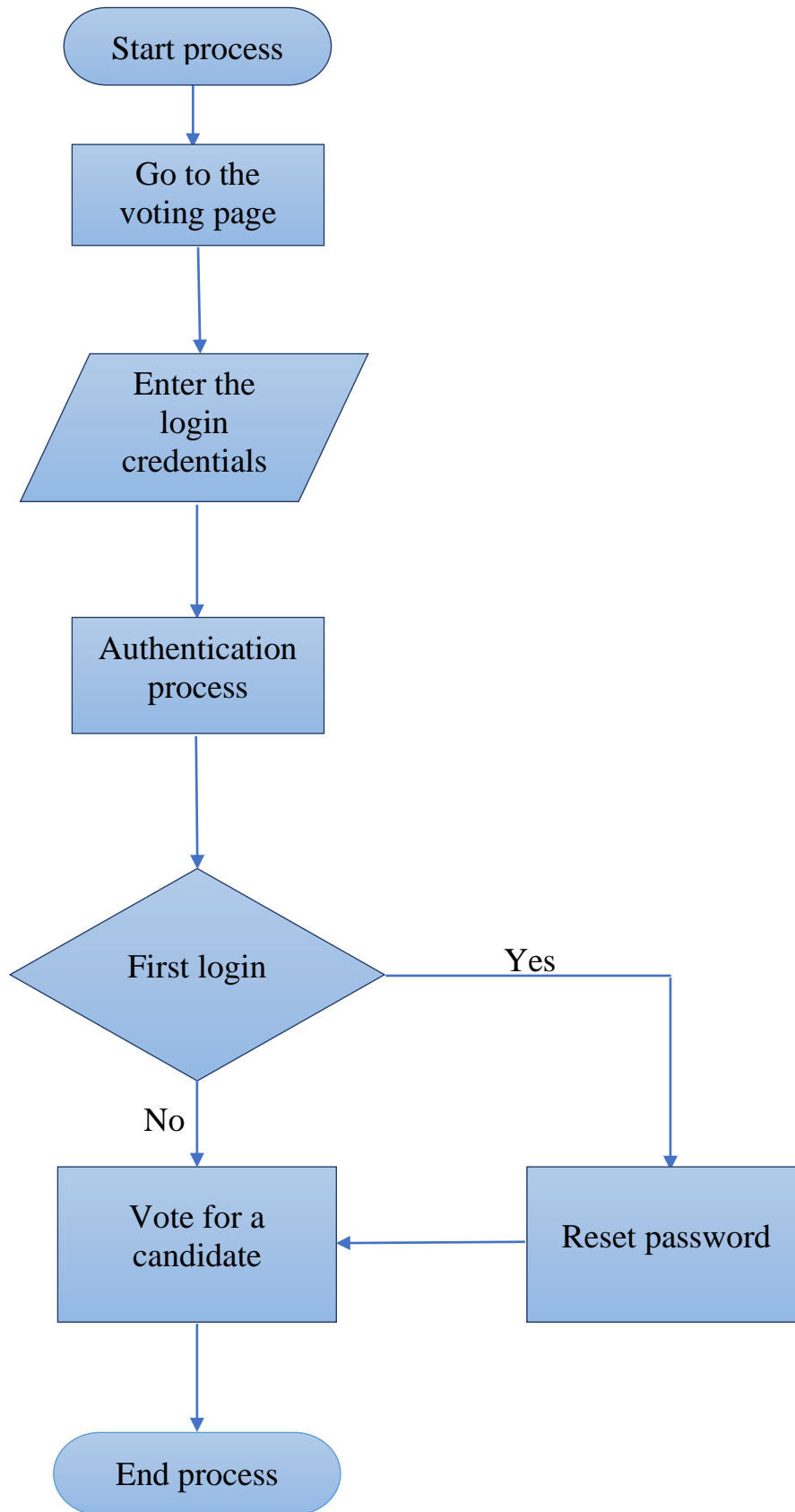


Fig 9.18 Voting process flow diagram

CHAPTER 10

CONCLUSION

This project allows voter to cast his/her voter through internet, therefore voter does not have to go to voting booths to vote they can vote from anywhere. To make our system highly secured we also have enforced the method for fingerprint scanning and OTP verification. It is also based on blockchain technology, which remove all the threats from the communication link. It is a decentralized system, contain hashing and encryption concept for providing the security. Our proposed system ensures that only registered and eligible voter is able to give own votes. Once any voters completed her/his vote, the block will be created. Thus, our model ensures that one voter gives only one vote, no one will allow to give two votes. The system security analysis shows that the system is more robust and secure against existing attacks.

REFERENCE

- [1] Khasawneh, M., M. Malkawi and O. Al-Jarrah, 2014. A Biometric-Secure e-Voting System for Election Process, Proceeding of the 5th International Symposium on Mechatronics and its Applications (ISMA08), Amman, Jordan.
- [2] Virendra Kumar Yadav, SaumyaBatham, Mradul Jain, Shivani Sharma, 2014. An Approach to Electronic Voting System using UIDAI, International Conference on Electronics and Communication Systems.
- [3] Mahendheran, M., V.B. Ajith Rahavan, I. Vasu Devan, T.S. Kiruba Shankar and S. Raja, 2016. Online Polling System to This Digital Era with Thumb Press and Image Capture, Middle-East Journal of Scientific Research, 24(3): 645-649.
- [4] S. Raval, “Decentralized Applications: Harnessing Bitcoin’s Blockchain Technology.” O’Reilly Media, Inc. Sebastopol, California (2016).
- [5] Friðrik Þ. Hjálmarsson, Gunnlaugur K. Hreiðarsson, Mohammad Hamdaqa, Gísli Hjálmtýsson, Blockchain-Based E-Voting System, 2018 IEEE 11th International Conference on Cloud Computing.
- [6] Ahmed Ben Ayed, A Conceptual Secure Blockchain-Based Electronic Voting System, 2015, International Journal of Network Security & Its Applications.
- [7] Ashish Singh, Kakali Chatterjee, SecEVS : Secure Electronic Voting System Using Blockchain Technology, 2018 International Conference on Computing, Power and Communication Technologies (GUCON) Galgotias University, Greater Noida, UP, India. Sep 28-29, 2018.
- [8] Preeti Ahlawat, Rainu Nandal, Performance Improvement using Pseudorandom One Time Password (OTP) in Online Voting System, IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p-ISSN: 2278-8727, Volume 17, Issue 5, Ver. I (Sep. – Oct. 2015), PP 31-38