NITTE MEENAKSHI INSTITUTE OF TECHNOLOGY

(AN AUTONOMOUS INSTITUTION, AFFILIATED WITH VISVESVARAYA TECHNOLOGICAL UNIVERSITY, BELGAUM, APPROVED BY AICTE & GOVT. OF KARNATAKA

MAJOR PROJECT REPORT

on

E-Voting System using Blockchain and Homomorphic Encryption

Submitted in partial fulfilment of the requirement for the award of Degree of

Bachelor of Engineering

in

Computer Science and Engineering

Submitted by:

Prateek G	1NT18CS117
Sheetal S Harshini	1NT18CS149
Shreya A Hegde	1NT18CS153
V Venkata Sree Harsha	1NT18CS181

Under the Guidance of

Mr. P Ramesh Naidu
Assistant Professor, Dept. of CS&E, NMIT

Department of Computer Science and Engineering
(Accredited by NBA Tier-1)

2021-22

NITTE MEENAKSHI INSTITUTE OF TECHNOLOGY

(AN AUTONOMOUS INSTITUTION, AFFILIATED WITH VISVESVARAYA TECHNOLOGICAL UNIVERSITY, BELGAUM , APPROVED BY AICTE & GOVT. OF KARNATAKA)

Department of Computer Science and Engineering

(Accredited by NBA Tier-1)

CERTIFICATE

This is to certify that the final Report on **E-Voting System using Blockchain and Homomorphic Encryption** is an authentic work carried out by **Prateek G (1NT18CS117)**, **Sheetal S Harshini (1NT18CS149), Shreya A Hegde (1NT18CS153)** and **V Venkata Sree Harsha (1NT18CS181)** bonafide students of **Nitte Meenakshi Institute of Technology**, Bangalore in partial fulfilment for the award of the degree of ***Bachelor of Engineering*** in COMPUTER SCIENCE AND ENGINEERING of Visvesvaraya Technological University, Belagavi during the academic year ***2021-2022.*** It is certified that all corrections and suggestions indicated during the internal assessment have been incorporated into the report.

Internal Guide	**Signature of the HOD**	**Signature of Principal**
Mr P Ramesh Naidu Assistant Professor, Dept. CSE, NMIT Bangalore	Dr. Sarojadevi H Professor, Head, Dept. CSE, NMIT Bangalore	Dr. H. C. Nagaraj Principal, NMIT, Bangalore

Signature of Examiners

1.
2.

DECLARATION

We hereby declare that

(i) The project work is our original work

(ii) This Project work has not been submitted for the award of any degree or examination at any other university/college/Institute.

(iii) This Project Work does not contain other persons’ data, pictures, graphs or other information unless specifically acknowledged as being sourced from other persons.

(iv) This Project Work does not contain other persons’ writing unless specifically acknowledged as being sourced from other researchers. Where other written sources have been quoted, then:
a) their words have been re-written, but the general information attributed to them has been referenced;
b) where their exact words have been used, their writing has been placed inside quotation marks and referenced.

(v) This Project Work does not contain text, graphics or tables copied and pasted from the Internet, unless specifically acknowledged, and the source is detailed in the thesis and the References sections.

NAME	USN	Signature
Prateek G	1NT18CS117	
Sheetal S Harshini	1NT18CS149	Sheetal-S. Harshini.
Shreya A Hegde	1NT18CS153	
V Venkata Sree Harsha	1NT18CS181	Harsha V.V

Date: 12/07/2022

ACKNOWLEDGEMENT

The satisfaction and euphoria that accompany the successful completion of any task would be incomplete without the mention of the people who made it possible, whose constant guidance and encouragement crowned our effort with success. I express my sincere gratitude to our Principal **Dr. H. C. Nagaraj**, Nitte Meenakshi Institute of Technology for providing facilities.

We wish to thank our HoD**, Dr. Sarojadevi H.** for the excellent environment created to further educational growth in our college. We also thank him for the invaluable guidance provided which has helped in the creation of a better project.

I hereby like to thank our mentor **Mr. P. Ramesh Naidu, Assistant Professor,** Department of Computer Science & Engineering for his periodic inspection, time to time evaluation of the project and help to bring the project to its present form.

Thanks to our Departmental Project coordinators. We also thank all our friends, teaching and non-teaching staff at NMIT, Bangalore, for all the direct and indirect help provided in the completion of the project.

NAME	USN	Signature
Prateek G	1NT18CS117	
Sheetal S Harshini	1NT18CS149	Sheetal-S. Harshini
Shreya A Hegde	1NT18CS153	
V Venkata Sree Harsha	1NT18CS181	Harsha V.V

Date: 12/07/2022

ABSTRACT

Only about half of the elections are deemed to be free and fair, according to a study. Electoral fraud not only distorts the quality of representation, but also has an impact on political, social, and economic results. Homomorphic encryption and blockchain technologies can be utilized to secure free and fair elections.

In this paper, we aim to allow only the eligible citizens to vote by automatically checking their eligibility status from a federally approved application and then securing the voter's data using homomorphic encryption rather than encrypting the vote cast by the voter. By doing this, statistical analysis can be performed on the data which results in a unique set of insights that may otherwise remain unknown.

1.1 Background

CONTENTS

CHAPTER 1: INTRODUCTION

The right to vote is a constitutionally protected right that all citizens are granted, and it is the foundation of democracy. [1] A democracy is a popular form of government i.e., popular sovereignty but limited by a constitution that guarantees individual freedoms (such as speech) and rights (such as a fair trial).

However, [2] through research, it has been found that only about half the elections are free and fair. Electoral fraud not only distorts representation quality, but also has an impact on political, social, and economic results.

The drawbacks of the conventional voting systems include [3] security threats, lack of transparency, centralization of authority and [4] general difficulties faced by citizens to cast a vote.

To overcome these drawbacks, an electronic voting system could be introduced.

1.2 A brief history of Technology/Concept

A blockchain is a type of decentralized i.e., a distributed ledger technology (DLT) - a shared file/database of transactions that can be accessed and inspected by every participant in the Peer-to-Peer network. It is not subject to any form of central control authority. In summary, a blockchain is a decentralized, digitized & consensus-based secure digital storage mechanism [5].

A blockchain is distinguished by the rules it follows if inconsistencies arise, or the ledger does not tally. The Blockchain stores information sequentially in “blocks” in an ordered chain.

When information is effectively added to Blockchain, it will be put away forever. Accordingly, the dependability and unwavering quality of information in Blockchain are extremely high [6].

Blockchain is basically a developing chain of blocks that have been associated cryptographically. Each block incorporates a hash, timestamp and exchange information from the past block [7].

Lately, blockchain innovation incorporates the blockchain information structure itself, conveyed agreement calculation, public-key cryptography & smart contracts [6].

1.3 Applications

To securely and successfully carry out federal and state-level election processes while maintaining the integrity of the votes cast.

1.4 Research motivation and Problem statement

1.4.1 Research Motivation

Through research [2], it has been found that only about half the elections are free and fair. Not only does electoral malpractice distort the quality of the representation, but it also impacts the political, social, and economic outcomes.

To ensure free and fair elections, homomorphic encryption and blockchain technologies can be used [8]. Lack of security, ballot forgery, coercion, lack of transparency, centralization of authority and the possibility to tamper with the database [9] are disadvantages of a traditional voting system. Secure e-voting on the blockchain with the help of smart contracts would eliminate this threat to democracy.

1.4.2 Statement of the Problem

In this paper, we aim to allow only the eligible citizens to vote by automatically checking their eligibility status from a federally approved application and then securing the voter's data using homomorphic encryption rather than encrypting the vote cast by the voter. By doing this, statistical analysis can be performed on the data which results in a unique set of insights that may otherwise remain unknown.

1.5 Research objectives and contributions

1.5.1 Primary objectives

The primary objective of this project is to ensure that the elections are conducted in a free and fair manner without any data tampering.

1.5.2 Main contributions

This paper's key contribution is that it allows only the eligible citizens to vote by automatically checking their eligibility status from a federally approved application and once the vote has been cast, the voter's data can be secured using homomorphic encryption rather than encrypting the vote cast by the voter. By doing this, statistical analysis can be performed on the data which results in a unique set of insights that may otherwise remain unknown. The encrypted data of the voter along with the unencrypted vote cast by the voter is added to a blockchain so that the voter's identity can be protected while also maintaining the integrity of the election data.

1.6 Summary

In this paper, we aim to allow only the eligible citizens to vote by automatically checking their eligibility status from a federally approved application and then securing the voter’s data using homomorphic encryption rather than encrypting the vote cast by the voter. By doing this, statistical analysis can be performed on the data which results in a unique set of insights that may otherwise remain unknown.

CHAPTER 2: LITERATURE SURVEY

2.1 Introduction

Democracy is the sovereignty of the people — "government of the people, by the people, for the people," in the words of Abraham Lincoln. At its core is the notion of the people choosing a government through frequent, free, and fair elections.[10]

Elections are democratic in the sense that they permit citizens to choose and hold their political representatives responsible. The right to vote is the cornerstone of democracy, and it is a constitutional right that every citizen of a democratic country enjoys. [11]

Decisions should be free and fair. A free political decision is one in which all residents have the potential chance to decide in favor of their favored competitor, and A fair political decision is one in which all votes are counted precisely and have equivalent weight. [12]

Elections conducted by the advantages of the paper ballot system include a voter who casts a ballot using paper and a stamp. [13]

Each voter uses one ballot, and ballots are not shared.[14] People who appreciate conventional paper ballots may disagree in their study [15] that:

- Elections with paper ballots are impossible to hack.
- Paper ballots are, for the most part, very user-friendly; voters do not need to be tech-savvy to use them.
- There's no chance of a power outage or a server outage.
- Paper ballots are less expensive and require less setup.
- A paper ballot election can be held at any time and in any location.

But the traditional Paper ballot system comes with a few drawbacks [14][15]

- Traditional voting necessitates the printing and mailing of ballots.
- It might be inconvenient and time-consuming to wait for mail-in paper votes.
- This system cannot be audited unless the votes are manually recounted.
- The use of proxy voting may result in the tampering of cast votes.
- Paper votes are prone to damage and can only be kept for a limited duration.
- Counting paper ballots necessitates a secure procedure, which is normally left to the administration's judgment.

[15] Any type of voting that uses modern technology to cast and count votes is referred to as electronic voting. This type of voting has advantages over the paper ballot system as e-voting provides faster results, ease of use, voters can access the ballot anytime, efficiency, and security, It makes it impossible for voters to make a mistake and vote for several candidates because online ballots are configured to reject it.

Through research,[16] it has been found that approximately half the elections are free and fair. Electoral fraud not only affects the quality of representation, but it also has a negative impact on the economy, but it also has political, social, and economic effects. The major vulnerabilities faced by the [15,16] voters are:

- Validity of voters
- The integrity of the ballot
- Secure transmission of the ballot
- Transparency
- Centralized System
- Possibility to tamper with the database

To ensure free and fair elections [17] and to overcome the above vulnerabilities faced, homomorphic encryption and blockchain technologies can be used.

In this paper, we aim to allow only the eligible citizens to vote by automatically checking their eligibility status from a federally approved application and then securing the voter's data using homomorphic encryption rather than encrypting the vote cast by the voter. By doing this, statistical analysis can be performed on the data which results in a unique set of insights that may otherwise remain unknown.

2.2 Related work

REFERENCES	PROPOSED	FINDING
[19] Lemuria Carter and France Bélanger, 2012	Web casting a ballot and political investment: an exact examination of innovative and political variables	Secure Internet transmission of a ballot has the potential to boost public engagement in the political process. This occurrence has the potential to boost citizen participation in the political process.

[20] (Ruhi Taş and Ömer Özgür Tanrıöver,2021)	A Manipulation Prevention Model for Blockchain-Based E-Voting Systems	The model with voter anonymity is ensured by a decentralized design and cryptographic data storage security strategy, eliminates the need for a central authority, and keeps the recorded votes in a distributed structure, which may have the ability to solve these concerns.
[21] (Uzma Jafar, Mohd Juzaiddin Ab Aziz and Zarina Shukur,2021)	Blockchain for Electronic Voting System-Review and Open Research Challenges	Decentralized, digitized, consensus-based secure information storage mechanism which makes it perfect for the e-voting system
[22] (Shreya Gupta and Ginni Arora,)	Use of Homomorphic Encryption with GPS in Location Privacy	The proposed model uses homomorphic encryption to encrypt.
[23] (Kashif Mehboob Khan, Junaid Arshad and Muhammad Mubashir Khan)	Secure Digital Voting System based on Blockchain Technology	We can understand the Main Requirements Of E-Voting: • Privacy-Privacy entails keeping a person's vote hidden. • Eligibility - Only registered voters are allowed to vote, and each voter is only allowed to vote once.

		- Receipt Freeness - Voters should not be able to show that they voted in a specific way to a third party. - Convenience - Voters must be able to cast their ballots easily, and everyone who is entitled to vote must be able to do so. - Verifiability - The User Interaction and Front-end Security layer is responsible for communicating with a voter and ensuring that the vote tallying process is trustworthy.
[24] (Wenan Tan, Hai Zhu, Jinjing Tan, Yao Zhao, Li Da Xu & Kai Guo,2021)	Internet voting and political participation: an empirical comparison of technological and political factors: ACM SIGMIS Database: the DATABASE for Advances in Information Systems: Vol 43, No 3	The distributed consensus technique and the blockchain data structure. According to the author, blockchain technology includes public-key cryptography and smart contracts.
[25] (Haibo Yi,2019)	Securing E-Voting Based on Blockchain in P2P Network	The block definition, ECC-based user credentials, determining the hash value using

		SHA-256, and All aspects of voting block mining and production are explained.
[26] (V. F. Rocha and Julio López,2018).	An Overview on Homomorphic Encryption Algorithms	Homomorphic encryption is a type of encryption that allows clients to do computations on encrypted information without needing to decrypt it first. This allows data to be encrypted before being sent to commercial cloud environments to be processed.
[27] (Nileshkumar Kakade; Utpalkumar Patel,2020)	Secure Secret Sharing Using Homomorphic Encryption	The proposed system in transfers secrets using homomorphic encryption. • Each party can choose the number of shares to be made. • Each party can choose the security of the share. Non-deterministic property of Paillier encryption

2.3 Study of Tools

A blockchain is a type of decentralized i.e., a distributed ledger technology (DLT) - a shared file/database of transactions that can be accessed and inspected by every participant in the Peer-to-Peer network. It is not subject to any form of central control authority.[26]

A block is a data structure that is inserted in a distributed manner as a chain structure. A distributed ledger of recorded transactions is what blockchain is. [27]

A blockchain is distinguished by the rules it follows if inconsistencies arise, or the ledger does not tally [28]. The Blockchain stores information sequentially in “blocks” in an ordered chain.

Whenever information is added to a blockchain effectively, it will be put away indefinitely [29] As a result, the data in Blockchain is extremely stable and reliable.

In summary, a blockchain is a decentralized, digitized and consensus-based secure digital storage mechanism [30].

Web3:

The improvement of Web3 gets an opportunity to move our social worldview, with decentralized, computerized answers for a portion of society's most concerning issues. American governmental issues could give Web3 the principal significant venture a valuable open door to fabricate trust, fuel standard reception, and get boundless media consideration.

Web3 gives another way ahead to citizen cooperation, the general norm for the soundness of a majority rule government. An October overview by IoT organization Metova uncovered that 66% of American respondents who didn't cast a ballot in 2016 would have casted a ballot on the off chance that there was a portable choice. That compares to almost 60 million additional electors.

All American races are overseen at the state level and controlled with unified, actual democratic areas. Exactness, straightforwardness, security and availability are the main four political decision objectives; however, guidelines shift generally by state.

The following are a couple of issues that influence the entire framework:

- Paper polling forms can be messed with and precluded.
- Electronic democratic machines can be hacked, went after and reconstructed.

- Each vote is hand-counted (counting electronic passages), and results require hours to report.

Races are as concentrated, non-independent and shortcoming inclined as any foundation can be.

To see how homomorphic encryption helps keep data transfer and operation on data safe we need to first understand what homomorphic encryption is and its types. Homomorphic encryption is a sort of encryption that allows us to communicate with one other to perform computations on encrypted material without having to first decrypt it. There are three different types of homomorphic encryption. mainly [24] An Overview on Homomorphic Encryption Algorithms:

- PHE (Partial Homomorphic Encryption)
- SWHE (Somewhat Homomorphic Encryption)
- FHE (Fully Homomorphic Encryption)

As soon as the Diffie-Hellman cryptosystem made its way through the crypto world, it also marked the beginning of the public key cryptosystem model. In no time the RSA cryptographic algorithm paved the way for partial homomorphic encryption model systems and that’s how the entire homomorphic encryption system started making its way into the industry. Partial homomorphic encryption includes:

- RSA
- El-Gamal
- Goldwasser-Micali
- Benaloh
- Paillier

Firebase Authentication:

In the current period, client validation is one of the main prerequisites for any secure application. It is fundamental to confirm clients, and it is a lot harder in the event that we need to compose this code all alone. This is done effectively with the assistance of Firebase.

Having the option to validate our clients safely, it offers a modified encounter to them in view of their inclinations and inclinations.
We can guarantee that they have no issues getting to their confidential information while utilizing our application from different gadgets.
Firebase Authentication gives all the server-side stuff for validating the client. Firebase Authentication turns out to be simple with SDK. It makes API simple to utilize.
Firebase Authentication likewise gives some UI libraries which empower evaluates for us when we are able to log in.

We initially get confirmation qualifications from the client to sign a client into our application.
Qualifications can be the client's email address and secret key.
The qualification can be an OAuth token from a personality supplier. We then pass these accreditations to the Firebase Authentication SDK. Backend administrations will then check those certifications and return a reaction to the client.

After a fruitful sign in We can get to the client's admittance to information put away in other Firebase items. We can get to the client's essential profile data. We can utilize the gave confirmation token to check the personality of clients in our own backend administrations.
Knowing who are the clients are a significant piece of building an application, and Firebase Authentication gives a simple to utilize, secure, client side just answer for verification. Firebase Security
Rules for Cloud Storage ties into Firebase Authentication for client security. When a client is confirmed with Firebase authentication, the request.auth variable in Cloud Storage Security Rules confirms the authenticity of the client using Firebase Authentication. The request.auth variable turns into an item that contains the client’s extraordinary ID (request.auth.uid) and any remaining client data is stored in the token (request.auth.token). When the client cannot validate, request.auth is invalid.

Cipher Text:

Ciphertext is text that has been altered from plaintext using an encryption algorithm.

Before being converted into plaintext (decoded) with a key, ciphertext must first be converted before being read. The computation that converts the ciphertext back into plaintext is known as the unscrambling figure.

The term figure is in some cases utilized as an equivalent for ciphertext. Be that as it may, it alludes to the strategy for encryption as opposed to the outcome Symmetric codes, which are regularly used to get online correspondences, are integrated into various organization conventions to be utilized to scramble trades. For instance, Transport Layer Security utilizes codes to encode application layer information.

Conventions using symmetric codes are used by virtual confidential organizations that connect telecommuters or distant branches to corporate organizations to protect information correspondences. In the majority of organizations utilizing Wi-Fi, online banking, online business administrations, and mobile communication, symmetric codes protect information security.

Different conventions, including secure shell, OpenPGP and Secure/Multipurpose Internet Mail Extensions utilize deviated cryptography to scramble and verify endpoints yet additionally to safely trade the symmetric keys to encode meeting information. For execution reasons, conventions frequently depend on codes to encode meeting information.

One of earliest and least difficult codes is the Caesar figure, which utilizes a symmetric key calculation. The vital goes about as a common mystery between (at least two) parties that can be utilized to send privileged intel nobody can peruse without a duplicate of the key.

The Caesar figure is a replacement figure where each letter in the plaintext is "relocated" a predetermined number of positions down the alphabet.

For example, if the shift was 1, A would come before B, B would be replaced by C, and so on.

The method is named for Julius Caesar, who is reputed to have used it to communicate with his generals.

Here is an illustration of the encryption and decoding steps associated with the Caesar figure. The text to be scrambled is "protect the east mass of the palace," with a shift (key) of 1.

Plaintext: shield the east mass of the palace
Ciphertext: efgfoe uif fbtu xbmm pg uif dbtumf

We have utilized decentralize network all together to store casting a ballot information as blocks. Blocks are interconnected with one another to making the chain of casting a ballot record. In the proposed framework the blockchain is utilized for security reason and furthermore we have made various degrees of confided in contacts. On the off chance that the more significant position permits the information to get put away in blocks then just it will be stored in the blockchain data set. When the information gets put away it can't be alter as blockchain is immutable. The blocks will contain the data as: username, past hash esteem, timestamp.

The block is one exchange of blockchain, which will broadcast in the entire framework when it gets check. Whenever new block is verified by the framework, block is added at end of the blockchain with assistance of hash, this construction seems to be similar to a Linked list data structure. This grouping of blockchain continues expanding as the blocks get added. The essential block in the blockchain is called as the Genesis Block. It has esteem as zero for past block since beginning block has no past block.

A blockchain is intended to be gotten to across a distributed organization, every hub/peer then speaks with different hubs for block and exchange trade. Once associated with the network, peers begin sending messages about different companions on the organization, this makes a decentralized technique for peer revelation. The reason for the hubs inside the organization is to approve unsubstantiated exchanges and as of late mined blocks, before another hub can begin to do this it initially needs to complete an underlying block download. The underlying block download makes the new hub download and approve all blocks from block 1 to the latest blockchain, when this is done the hub is thought of as synchronized.

Partial Homomorphic Encryption:

A crypto system is considered somewhat homomorphic assuming it displays either added substance or multiplicative homomorphism, yet not both. A few models of to some extent homomorphic cryptosystems are:

- RSA - multiplicative homomorphism
- El Gamal multiplicative homomorphism
- Paillier added substance homomorphism

RSA shows multiplicative homomorphism. By duplicating (at least two) RSA ciphertexts together, the decoded outcome is identical to the multiplication of the (at least two) plaintext values.

El Gamal displays multiplicative homomorphism. By increasing every part of numerous with their comparing components, the unscrambled outcome is comparable to the multiplication of plain-text values.

Paillier displays added substance homomorphism. By multi-handling every part of various ciphertexts with their comparing separate parts, the de-crypted result is comparable to the expansion of the plaintext values.

Homomorphic encryption has many advantages and applications. One such kind of advantage is that of upgraded security. Security is one of the objectives of cryptography by and large, yet homomorphic encryption can give much further protection than regular encryption plans.

Think about applications in the banking world. Assume that a client of a bank has the complete worth of their records scrambled utilizing their confidential key and that is put away on the bank's servers. Without unscrambling the client's account values, things like revenue and moves could hypothetically be figured without at any point needing to see the client's particular dollar sum connected to their records. This protection additionally can be applied to casting a ballot framework. Similar as the Paillier ex-more than adequate gave before, secure democratic frameworks could be executed to such an extent that votes are encoded and stay obscure until all calculations are completed and the outcomes are decoded.

Paillier is fast with computations like addition and multiplication, it is selected for the case of this project for the same reason. It is fast and one of the last ones in partially homomorphic encryption.

Somewhat homomorphic encryption schemes weren't that famous but fully homomorphic encryption was seen as an opportunity when introduced by Gentry in 2009[31].

There were many more improvisations [32] and combinations to achieve the best fully homomorphic encryption, the original version of Gentry's design, however, set the norm for the others. There were so many more combinations of the same made with different researchers involved in the research aspect:

- DGHV [33]
- BGV [34]
- BFV [35][36]
- GSW [37]

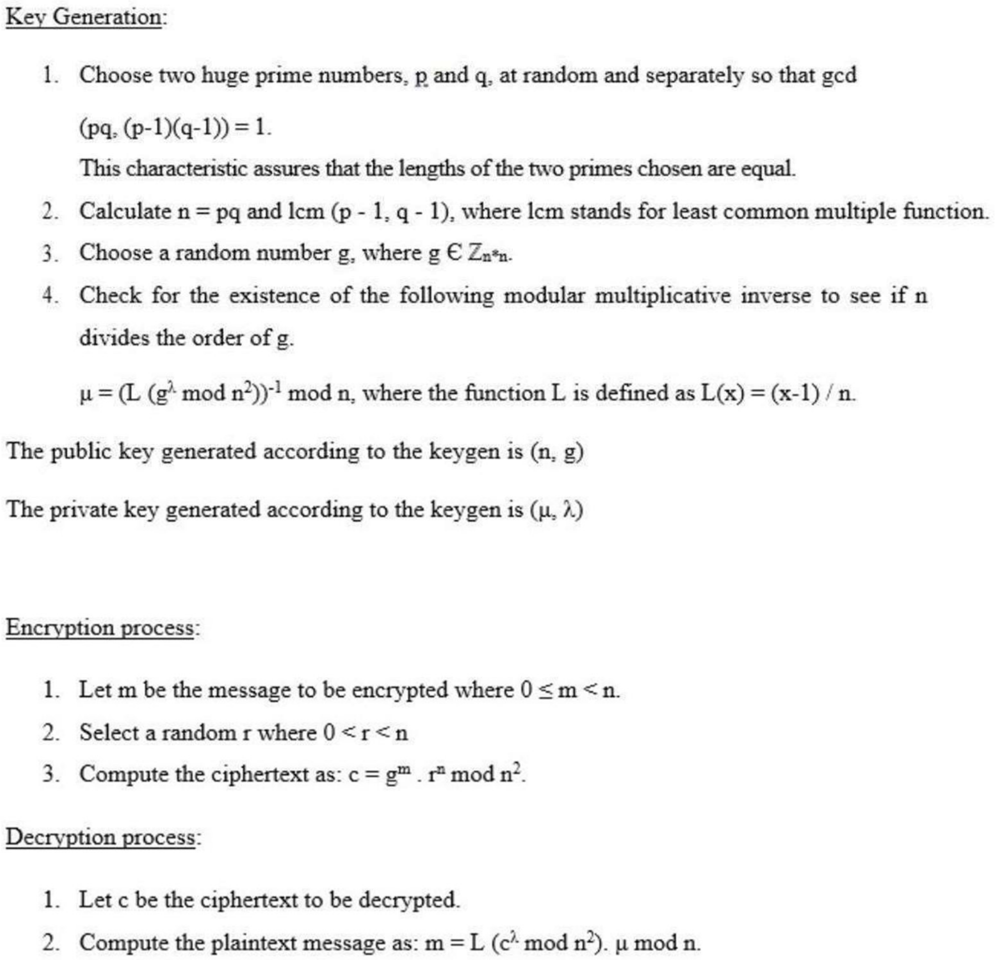
There are many libraries also present for the implementation encryption systems that are entirely homomorphic, some are based on bespoke research and others are commercially developed by companies like Microsoft and IBM. They are listed below:

- GH [38]
- SEAL [39]
- HElib [40]

There are many recent research applications of the homomorphic algorithms of all types:

- The type of HE is PHE and the cryptosystem used is Paillier cryptosystem in [41].
- Partial Homomorphic Encryption is used and the Paillier cryptosystem is implemented for its ease of implementation in [42].
- For the comparative study for an application in [43] Fully Homomorphic Encryption is used and the schemes BGV, BFV is implemented using HElib and PALISADE respectively.
- For the proposed secure system in [44] Fully Homomorphic Encryption is used, and improvements are suggested for the same as FHE is comparatively slower.

The homomorphic encryption type is Partial Homomorphic Encryption and the algorithm being implemented is Paillier cryptosystem [44]. For the Paillier cryptosystem, the algorithms below are utilized for key generation, encryption, and decryption.



Key Generation:

1. Choose two huge prime numbers, p and q, at random and separately so that gcd (pq, (p-1)(q-1)) = 1.
   This characteristic assures that the lengths of the two primes chosen are equal.
2. Calculate n = pq and lcm (p - 1, q - 1), where lcm stands for least common multiple function.
3. Choose a random number g, where g $\in Z_{n*n}$.
4. Check for the existence of the following modular multiplicative inverse to see if n divides the order of g.

   $\mu = (L\ (g^{\lambda} \bmod n^2))^{-1} \bmod n$, where the function L is defined as $L(x) = (x-1) / n$.

The public key generated according to the keygen is (n, g)

The private key generated according to the keygen is (μ, λ)

Encryption process:

1. Let m be the message to be encrypted where $0 \leq m < n$.
2. Select a random r where $0 < r < n$
3. Compute the ciphertext as: $c = g^m \,.\, r^n \bmod n^2$.

Decryption process:

1. Let c be the ciphertext to be decrypted.
2. Compute the plaintext message as: $m = L\ (c^{\lambda} \bmod n^2).\ \mu \bmod n$.

2.4 Summary

In our opinion, the authorities may be able to perform fraud or manipulations using online voting systems due to a security problem which and other participants have a hard time detecting the security breach. Many of the problems that were discovered in these early attempts at online voting can be remedied with blockchain technology. Homomorphic encryption now provides an irrefutable method of ensuring the accuracy of each vote cast.

So, the blockchain-based homomorphic voting app is unconcerned about the security of its Internet connection, since any hacker with terminal access will be unable to harm other nodes. Eligible voters are not required to reveal their identity when casting their ballots or political views to the public at large. This allows only the eligible citizens to vote by automatically checking their eligibility status from a federally approved application and then securing the voter's data using homomorphic encryption rather than encrypting the vote cast by the voter. By doing this, statistical analysis can be performed on the data which results in a unique set of insights that may otherwise remain unknown.

After the design phase, the desired service was implemented. To ensure the proper functioning of the system, we have created six constituencies where citizens can vote to elect their representatives. The general objective was to test the speed, security, and usefulness of the proposed framework. The testing was conducted on a <device details>, Chrome Web Browser with JavaScript enabled and the Metamask plugin installed. The Metamask plugin provides a simple interface to interact with the local Ethereum network which is used for testing the system. The local Ethereum test network was created using Ganache, and the Ropsten test network was used for the closest simulation of the real Ethereum Network.

CHAPTER 3: SYSTEM REQUIREMENTS SPECIFICATIONS

3.1 General Description

This chapter outlines the kinds of material that has to be collected before we can begin the implementation of the project.

3.1.1 Product Perspective

The main goal of this product is to securely and successfully carry out federal and state-level election processes while maintaining the integrity of the votes cast.

This system will have a simple user interface. However, it must not disadvantage any candidate while showing the options (for example, by asking the user to scroll down to view the final few options). Also, voters who are authorized are only able to register and cast their votes. Any voter who cast their vote once cannot do so again. It should be feasible to verify that all votes in the final election tally have been appropriately accounted for, and there should be trustworthy and legitimate election records in the form of a physical, permanent audit trail (which should not betray the user's identity in any way). At last, if a voter cast their vote, then it will be shown that they have already cast their vote. If possible, a ticket will be generated after they cast their vote.

3.2 System Requirements

3.2.1 Hardware Requirements

Processor	i3 and above
Speed	1.2 GHZ
Hard disk	20 GB
Ram	4 GB

3.2.2 Software Requirements

Any personal computer that meets the following specifications:

Operating system	Linux, Windows 7 and above
Language	JavaScript, Solidity
Tools	VS Code

3.2.2.1 Functional Requirements & Non-functional Requirements

Functional Requirements: An application that runs the election board and bulletin board and allows a voter to cast a vote and once the voting process stops, the application should automatically declare the results on clicking a button. It can also be stopped manually.

Non-Functional Requirements: The keys which are shared between the election board and bulletin board must be secure and trusted. We need to make sure that the bulletin board and election board systems are secure. The connection between Bulletin Board (BB) and Election Board (EM) must be secure and trusted.

3.2.2.2 User Requirements

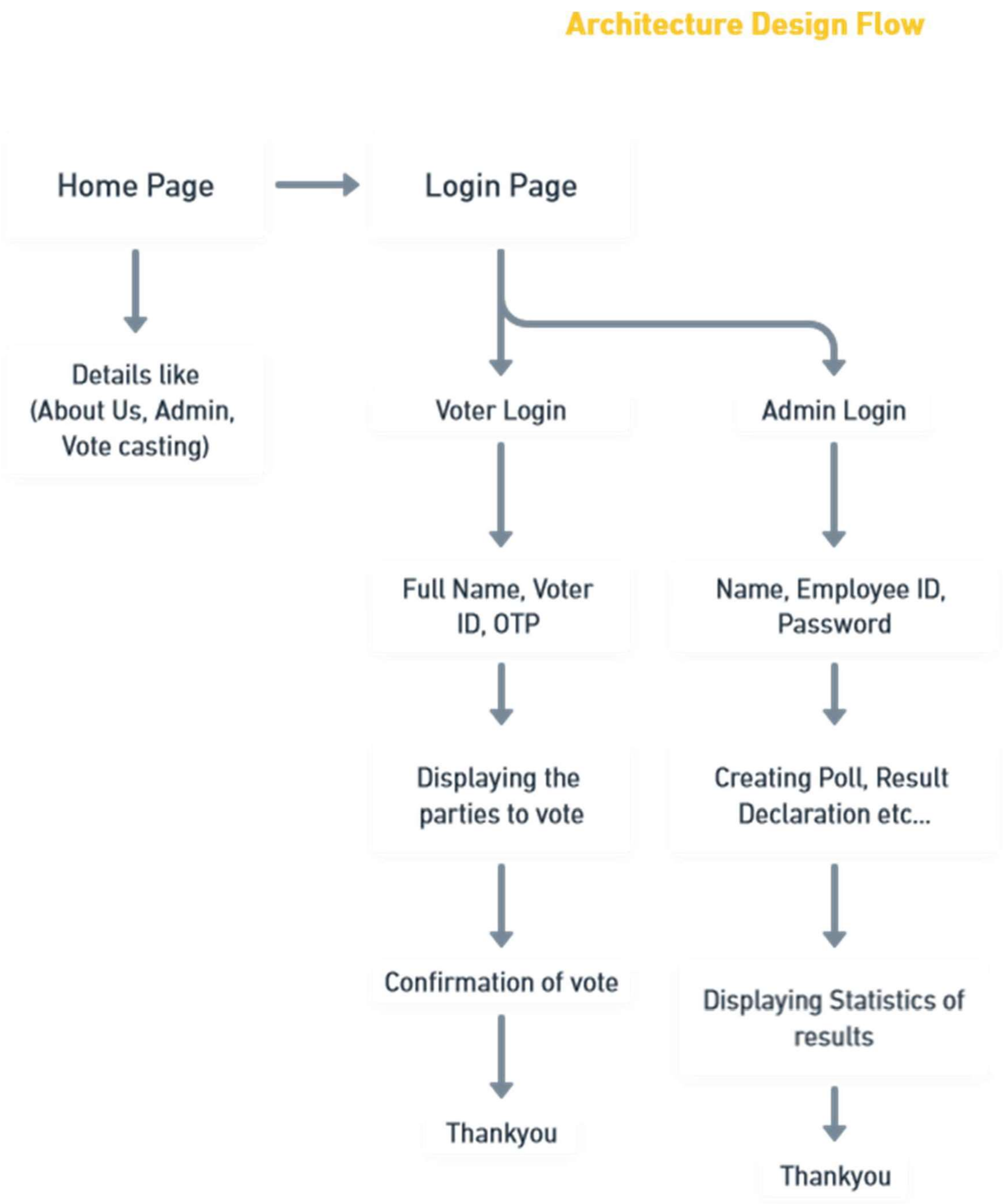
- He/she must be eligible to cast their vote.
- A Mobile Phone/Laptop with an Internet Connection.
- Proof of identity.
- Convenience: The framework will permit the citizens to project their votes rapidly, in one meeting and shouldn't need any exceptional abilities for the elector to make a choice (to guarantee Equality of Access to Voters).

3.3 Summary

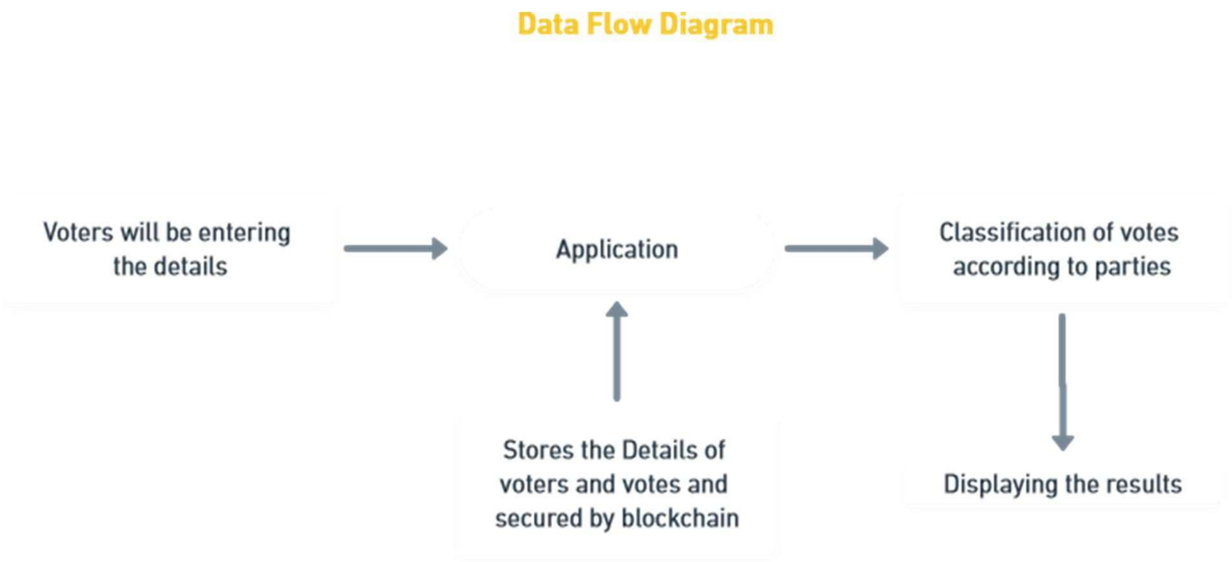
By having the above hardware & software requirements we can develop the e-voting system and also users should have these minimum requirements to cast their vote and also whenever the user proves that the same identity is casting their vote then he/she will proceed to further steps and cast their vote and after casting their vote the ticket will be issued whether he cast the vote (or) not.

CHAPTER 4: DESIGN

4.1 Architectural Design


Architecture Design Flow
Home Page
Login Page
Details like (About Us, Admin, Vote casting)
Voter Login
Admin Login
Full Name, Voter ID, OTP
Name, Employee ID, Password
Displaying the parties to vote
Creating Poll, Result Declaration etc...
Confirmation of vote
Displaying Statistics of results
Thankyou
Thankyou

4.2 Data Flow Diagram



Data Flow Diagram

Voters will be entering the details

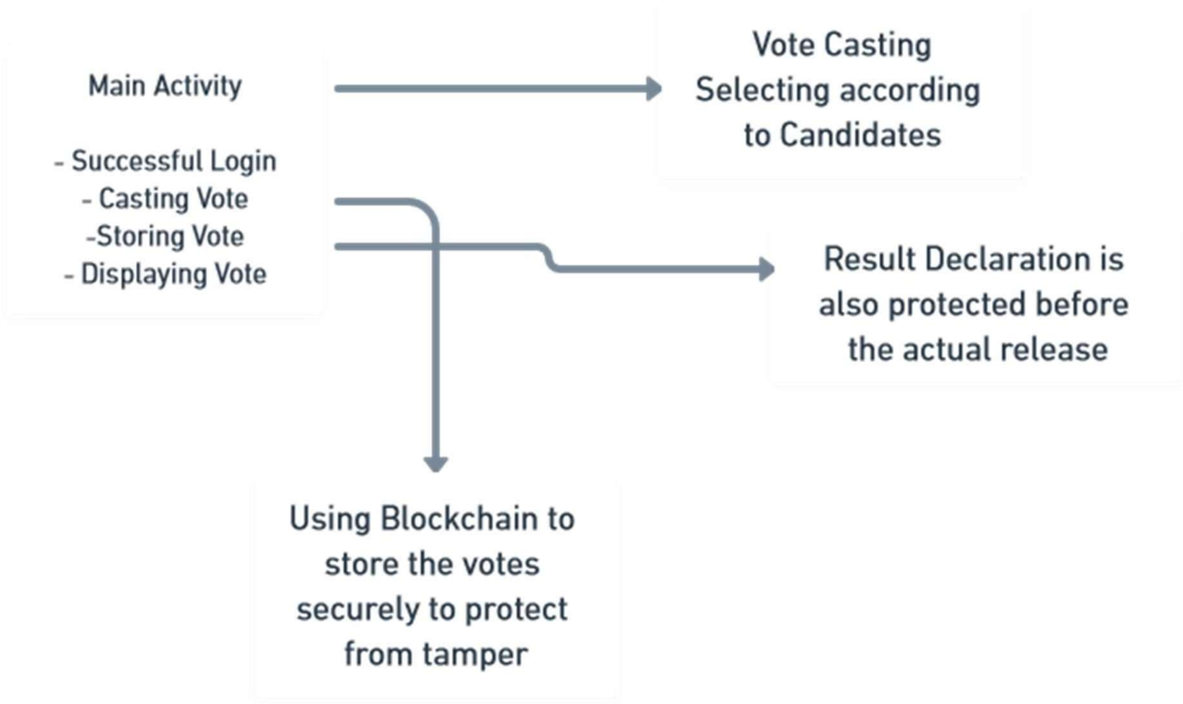
Application

Classification of votes according to parties

Stores the Details of voters and votes and secured by blockchain

Displaying the results

4.3 Class Hierarchy Diagram



Main Activity

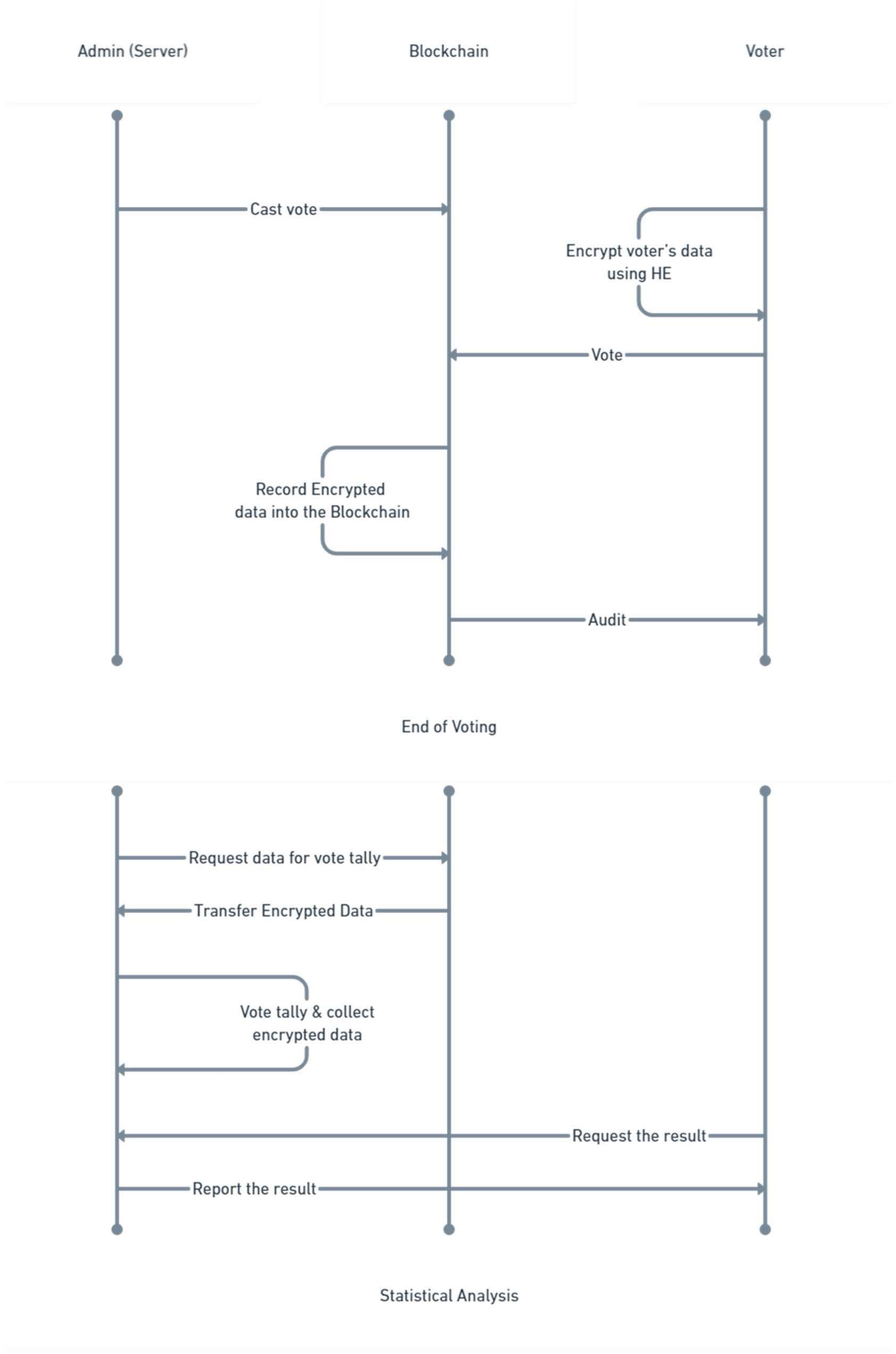
- Successful Login
- Casting Vote
- Storing Vote
- Displaying Vote

Vote Casting Selecting according to Candidates

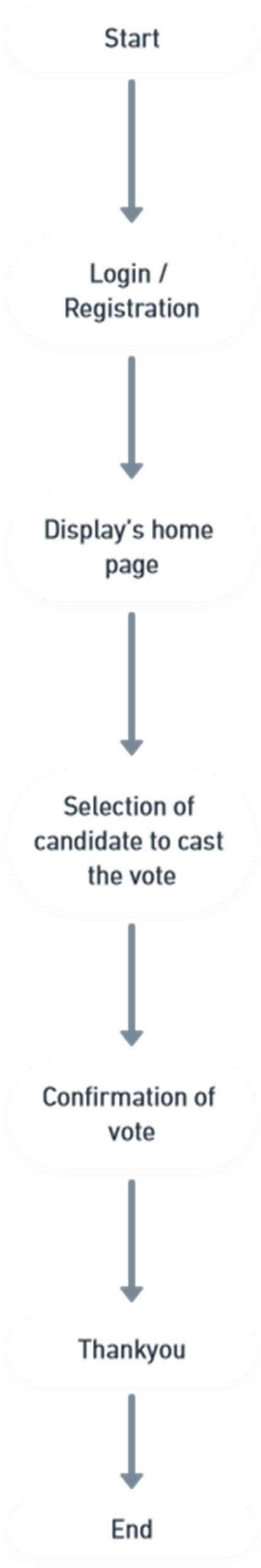
Result Declaration is also protected before the actual release

Using Blockchain to store the votes securely to protect from tamper

4.4 Sequence Diagram



4.5 Activity Diagram



CHAPTER 5: IMPLEMENTATION

5.1 Methodology

Blockchain is one of the most secure, reliable way to store the data because of its decentralization and immutability. In this project the primary focus is building a system in a way that vote cast by the voter is secure and cannot be tampered. The votes cast and the details of the voter will securely be stored using blockchain technology, a web application is developed which will be acting as a frontend or the Dapp where voters can securely cast their vote at ease and at their convenience. The voter is required to have a mobile phone (or) a laptop (or) a pc which is connected to internet in order to cast the vote.

Firstly, a voter logs into the system by entering his Name (as per VoterId), VoterId and Phone Number (linked with the VoterId), the system will verify the details and an OTP is sent to the registered phone number to authenticate the user. Further upon verification of the OTP the voter is authenticated and redirected to the voting page according to the voter’s constituency, the voting page would display registered candidates of the parties participating in the election of that constituency.

After the successfully voting of the voter these details and information get stored into the blockchain and the vote gets successfully recorded. The voting process (i.e.) security of the system is based on blockchain technology, the vote of each voter is considered as a transaction inside the blockchain and the data inside the backend of the database. To make sure the person is voting only one time the web application will notify that the voter has already voted and needs to wait for the next eligible election, so there is a least possibility of any duplicate entries being recorded. Once the voting process if completed the voter will be logged out and cannot login once more, this mechanism is present as a static security feature present in the application in order to preclude any possibility of a duplicate voting.

5.2 Description of Process

Admin process:

The administrator can sign in to the application by using any device connected to the internet and entering the correct login credentials (email and the password) which is stored on the database. Upon successful authentication of the email and the password, the admin is redirected to the admin options page, where the admin has the option to

i. Logout

ii. Create a new poll

iii. Declare the election results of a particular constituency; and

iv. Declare the overall results of the election

i. Logout

Logout will take the administrator back to the admin login page.

ii. Create New Poll

The create new poll functionality allows the admin to create and/or add a new constituency for which elections are to be conducted. The form accepts the candidate details for the particular constituency.

iii. Declare the elections results of a particular constituency

The declare election results for a particular constituency functionality allows the admin to enter the details of the constituency, such as the constituency name and number, for which the election results are to be displayed to the voters.

iv. Declare the overall results of the election

Declare the overall election results functionality allows the admin to enter the details of the election, such as poll ID, for which the election results are to be displayed to the voters.

Voter process:

The voter is required to have a mobile phone (or) a laptop (or) a pc which is connected to internet to cast the vote, the voter can cast their vote through the Dapp which is the website and the wallet account provide by the government. The voter is provided with a public and private key of an account of the registered user which has some cryptocurrency in it for dealing with the gas fee, for simplicity purposes in this project Metamask is used as wallet and Ganache is used for local blockchain and accounts deposited with ethers.

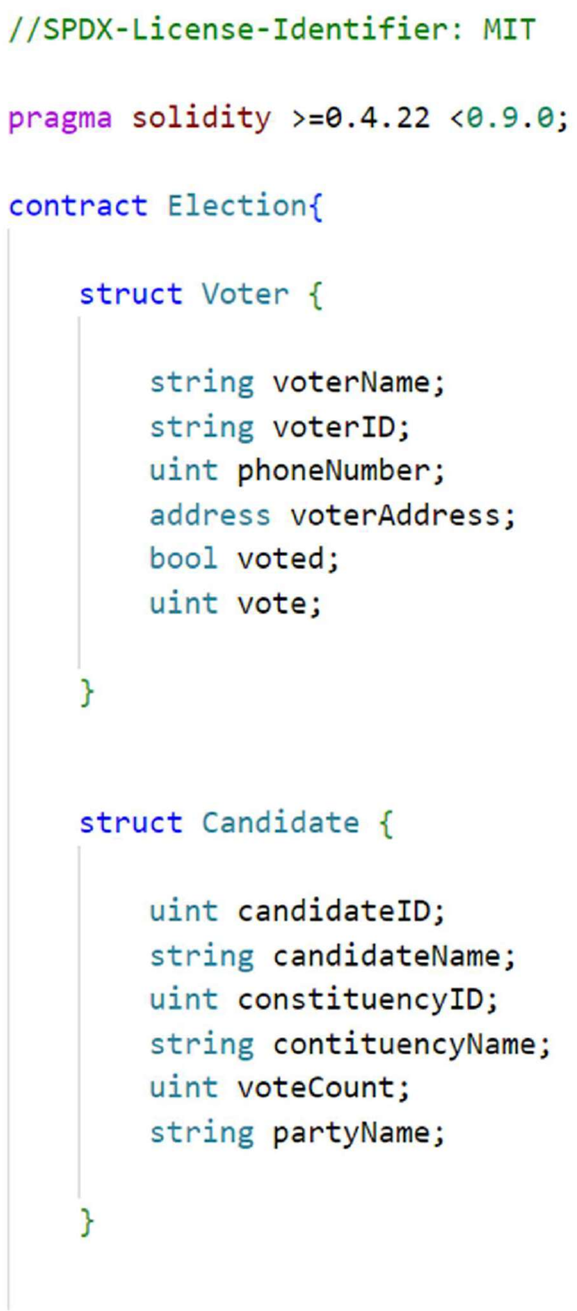
Firstly, a voter logs into the system by entering his Name (as per VoterId), VoterId and Phone Number (linked with the VoterId), the system will verify the details and an OTP is sent to the registered phone number to authenticate the user. Further upon verification of the OTP the voter is authenticated and redirected to the voting page according to the voter's constituency, the voting page would display registered candidates of the parties participating in the election of that constituency.

After the successfully voting of the voter these details and information get stored into the blockchain and the vote gets successfully recorded. The voting process (i.e.) security of the system is based on blockchain technology, the vote of each voter is considered as a transaction inside the blockchain and the data inside the backend of the database. To make sure the person is voting only one time the web application will notify that the voter has already voted and needs to wait for the next eligible election, so there is a least possibility of any duplicate entries being recorded. Once the voting process if completed the voter will be logged out and cannot login once more, this mechanism is present as a static security feature present in the application to preclude any possibility of a duplicate voting.

Homomorphic Encryption:

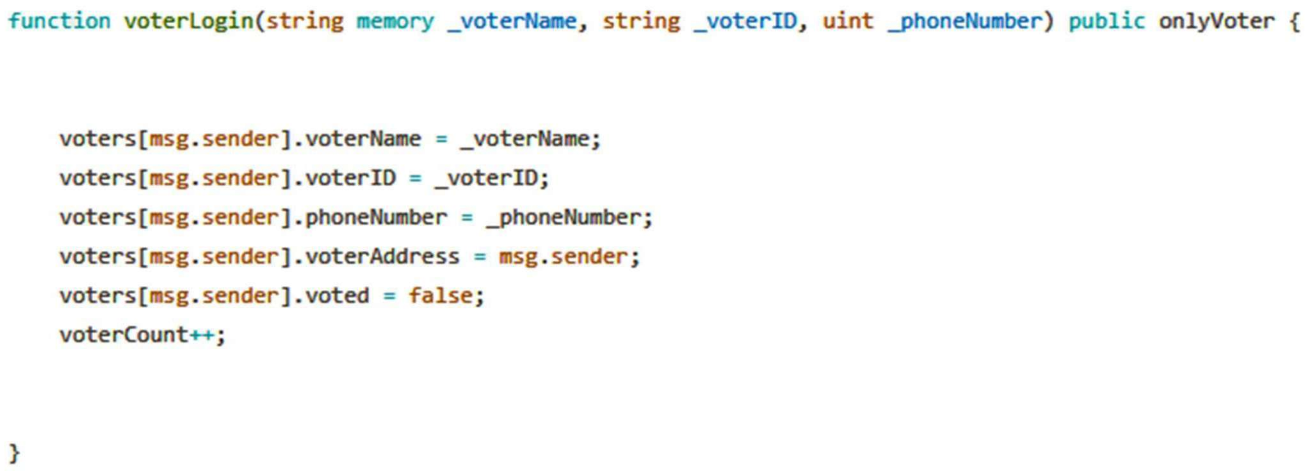
The algorithm used for the homomorphic encryption is Paillier cryptosystem which is already mentioned in the different sections above but in this section an idea will be provided as to how or why it is being used. Homomorphic Encryption in basic terms is that you can perform arithmetic operations on encrypted data which is the feature given the most importance for being selected and implemented in this project. The algorithm is used encrypt the voter data along with the vote cast, which was recorded on the blockchain this encrypted can be provided to the companies that perform statistical analysis which could give a chance to perform an analysis about the election in a secure manner.

5.3 Pseudo Code:



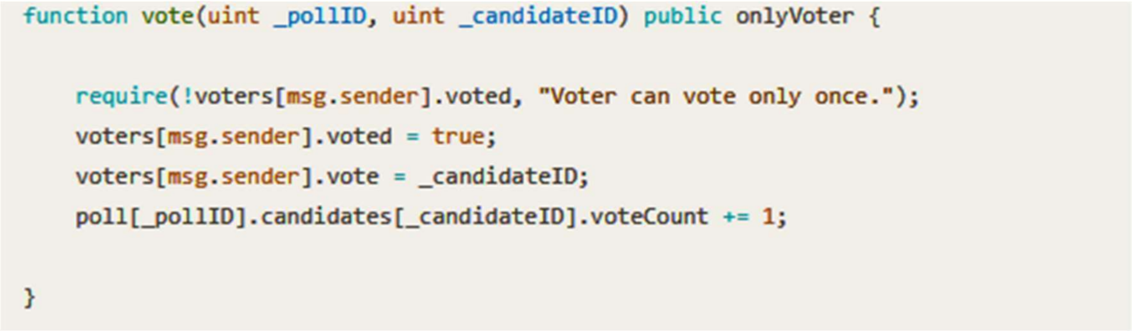
```
//SPDX-License-Identifier: MIT

pragma solidity >=0.4.22 <0.9.0;

contract Election{

    struct Voter {

        string voterName;
        string voterID;
        uint phoneNumber;
        address voterAddress;
        bool voted;
        uint vote;

    }


    struct Candidate {

        uint candidateID;
        string candidateName;
        uint constituencyID;
        string contituencyName;
        uint voteCount;
        string partyName;

    }
```

The above depicted pseudo code is the structure created in smart contract for the entire process.



```
function voterLogin(string memory _voterName, string _voterID, uint _phoneNumber) public onlyVoter {


    voters[msg.sender].voterName = _voterName;
    voters[msg.sender].voterID = _voterID;
    voters[msg.sender].phoneNumber = _phoneNumber;
    voters[msg.sender].voterAddress = msg.sender;
    voters[msg.sender].voted = false;
    voterCount++;


}
```

The above depicted pseudo code is the function used in the smart contract for the recording the voter details being logged in for the voting process.

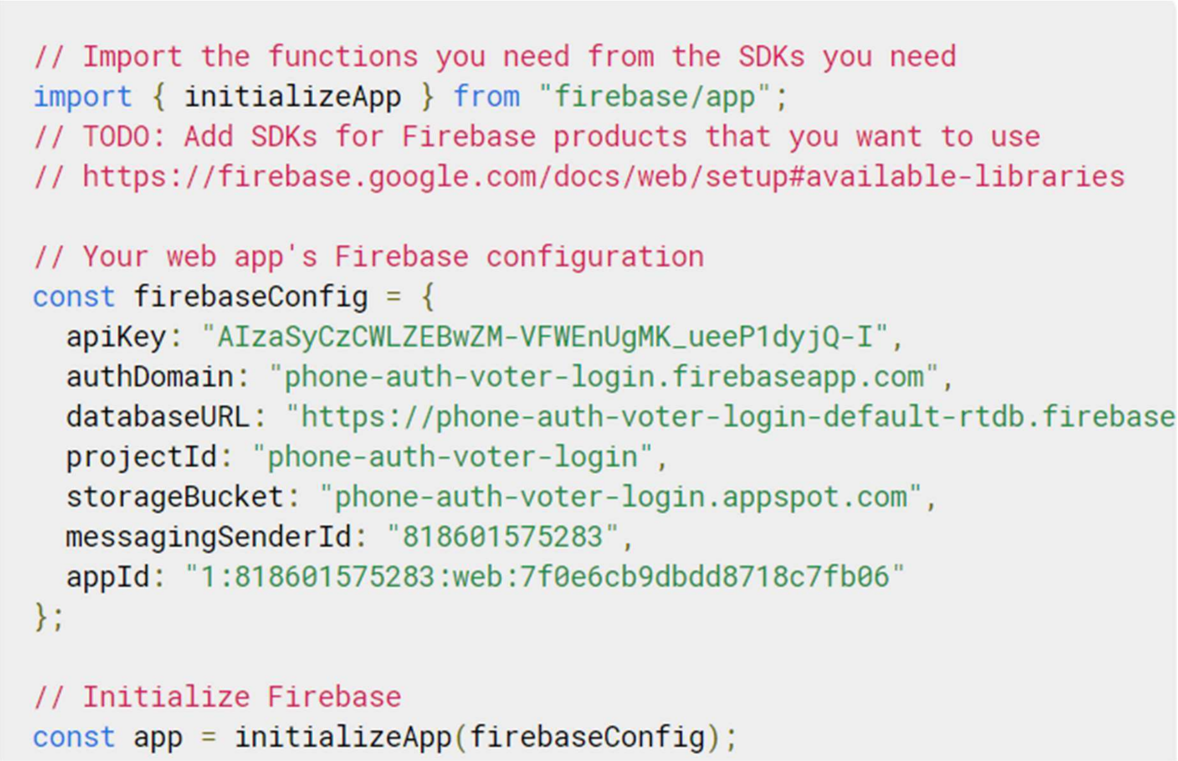


```
function vote(uint _pollID, uint _candidateID) public onlyVoter {

    require(!voters[msg.sender].voted, "Voter can vote only once.");
    voters[msg.sender].voted = true;
    voters[msg.sender].vote = _candidateID;
    poll[_pollID].candidates[_candidateID].voteCount += 1;

}
```

The above depicted pseudo code is the function used in the smart contract for the recording the voter’s vote during the voting process.

CHAPTER 6: TEST CASES

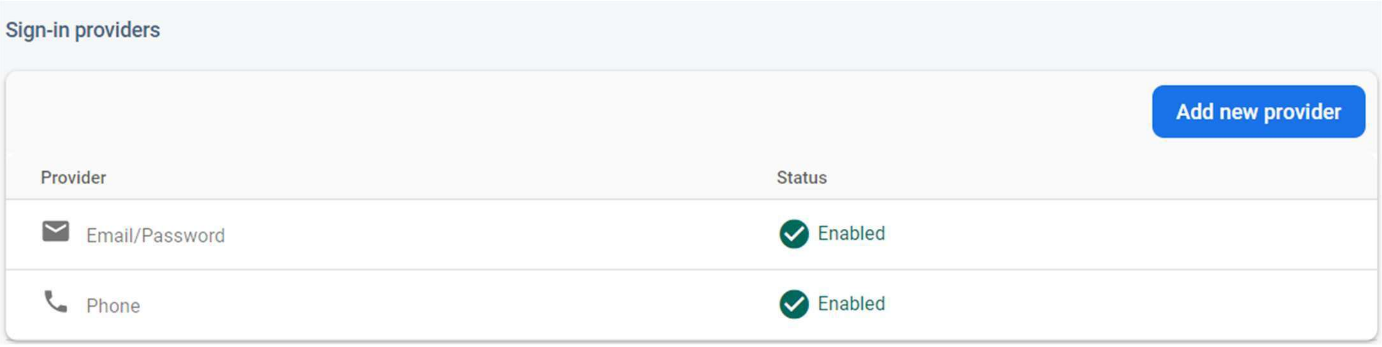
6.1 Firebase Configuration File Used to Import Services:



```
// Import the functions you need from the SDKs you need
import { initializeApp } from "firebase/app";
// TODO: Add SDKs for Firebase products that you want to use
// https://firebase.google.com/docs/web/setup#available-libraries

// Your web app's Firebase configuration
const firebaseConfig = {
  apiKey: "AIzaSyCzCWLZEBwZM-VFWEnUgMK_ueeP1dyjQ-I",
  authDomain: "phone-auth-voter-login.firebaseapp.com",
  databaseURL: "https://phone-auth-voter-login-default-rtdb.firebase
  projectId: "phone-auth-voter-login",
  storageBucket: "phone-auth-voter-login.appspot.com",
  messagingSenderId: "818601575283",
  appId: "1:818601575283:web:7f0e6cb9dbdd8718c7fb06"
};

// Initialize Firebase
const app = initializeApp(firebaseConfig);
```

After installing firebase using the command *npm install firebase*, it can be initialized and we can begin using the SDKs for the products used in the project.

6.2 Firebase Authentication Providers:

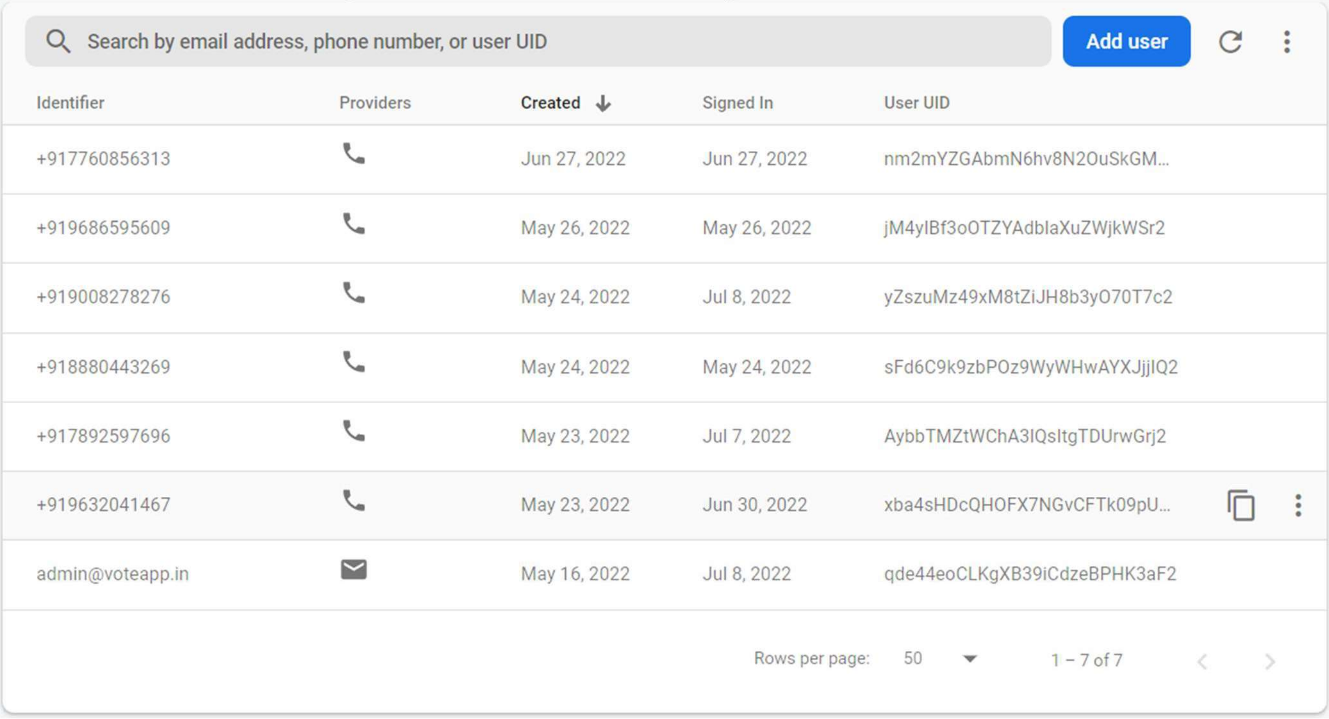


Sign-in providers

Provider	Status
Email/Password	✓ Enabled
Phone	✓ Enabled

The sign in providers allow us to select the medium using which the users of the application can securely gain access to the application by means of using an OTP (One Time Password).

6.3 Firebase Storage of Authentication Requests:

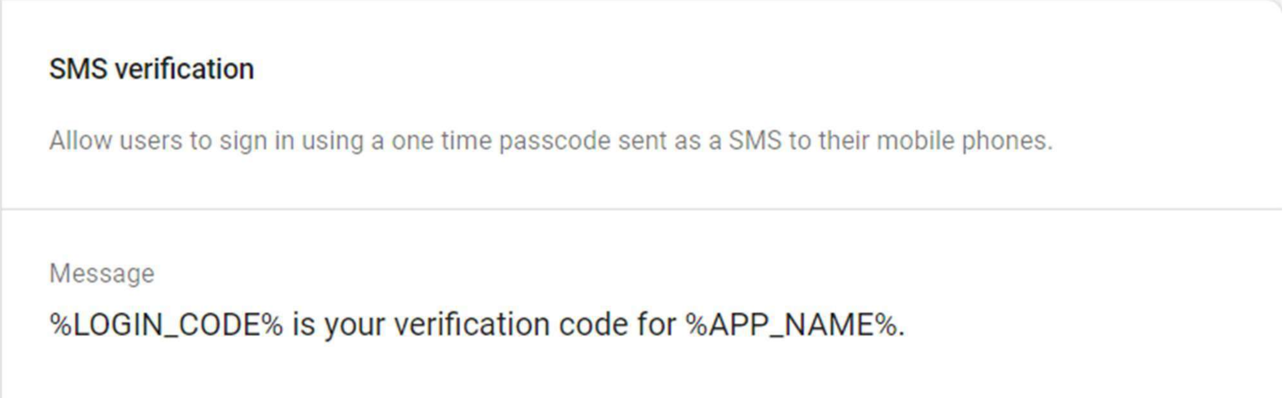


Identifier	Providers	Created ↓	Signed In	User UID
+917760856313	☎	Jun 27, 2022	Jun 27, 2022	nm2mYZGAbmN6hv8N2OuSkGM...
+919686595609	☎	May 26, 2022	May 26, 2022	jM4yIBf3oOTZYAdblaXuZWjkWSr2
+919008278276	☎	May 24, 2022	Jul 8, 2022	yZszuMz49xM8tZiJH8b3yO70T7c2
+918880443269	☎	May 24, 2022	May 24, 2022	sFd6C9k9zbPOz9WyWHwAYXJjjIQ2
+917892597696	☎	May 23, 2022	Jul 7, 2022	AybbTMZtWChA3IQsItgTDUrwGrj2
+919632041467	☎	May 23, 2022	Jun 30, 2022	xba4sHDcQHOFX7NGvCFTk09pU...
admin@voteapp.in	✉	May 16, 2022	Jul 8, 2022	qde44eoCLKgXB39iCdzeBPHK3aF2

Rows per page: 50 1 – 7 of 7

Shows the most recent authentication requests which were processed along with information such as the date created, the user ID and the date when the user signed in.

6.4 Firebase OTP Verification Template:



SMS verification

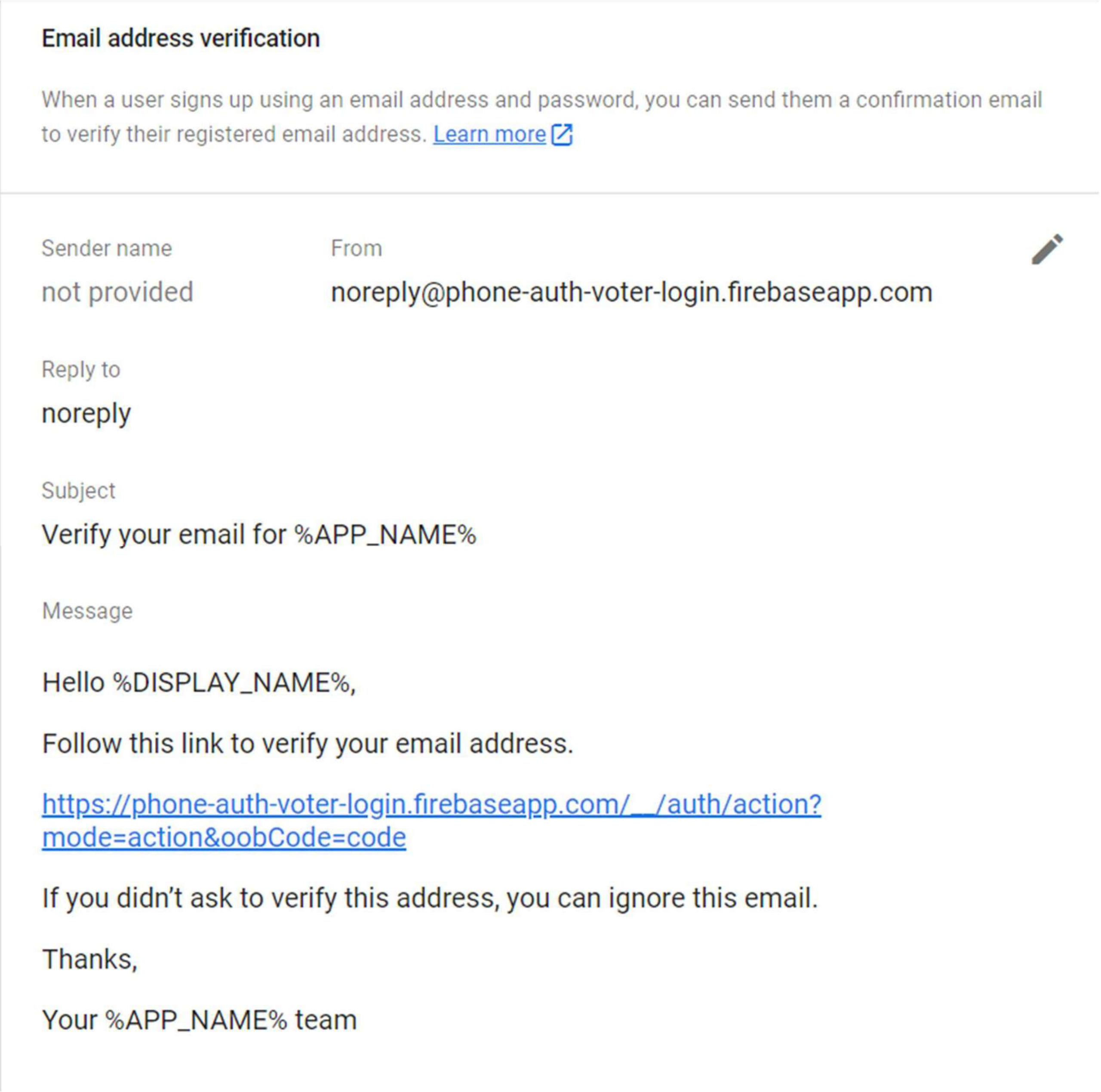
Allow users to sign in using a one time passcode sent as a SMS to their mobile phones.

Message

%LOGIN_CODE% is your verification code for %APP_NAME%.

The Firebase OTP Verification Template allows the users to sign in using a one-time passcode which is sent as an SMS to their mobile phone in the format “562532 is your verification code for Vote App”.

6.5 Firebase Email Verification Template:



Email address verification

When a user signs up using an email address and password, you can send them a confirmation email to verify their registered email address. Learn more

Sender name
not provided

From
noreply@phone-auth-voter-login.firebaseapp.com

Reply to
noreply

Subject
Verify your email for %APP_NAME%

Message

Hello %DISPLAY_NAME%,

Follow this link to verify your email address.

https://phone-auth-voter-login.firebaseapp.com/__/auth/action?mode=action&oobCode=code

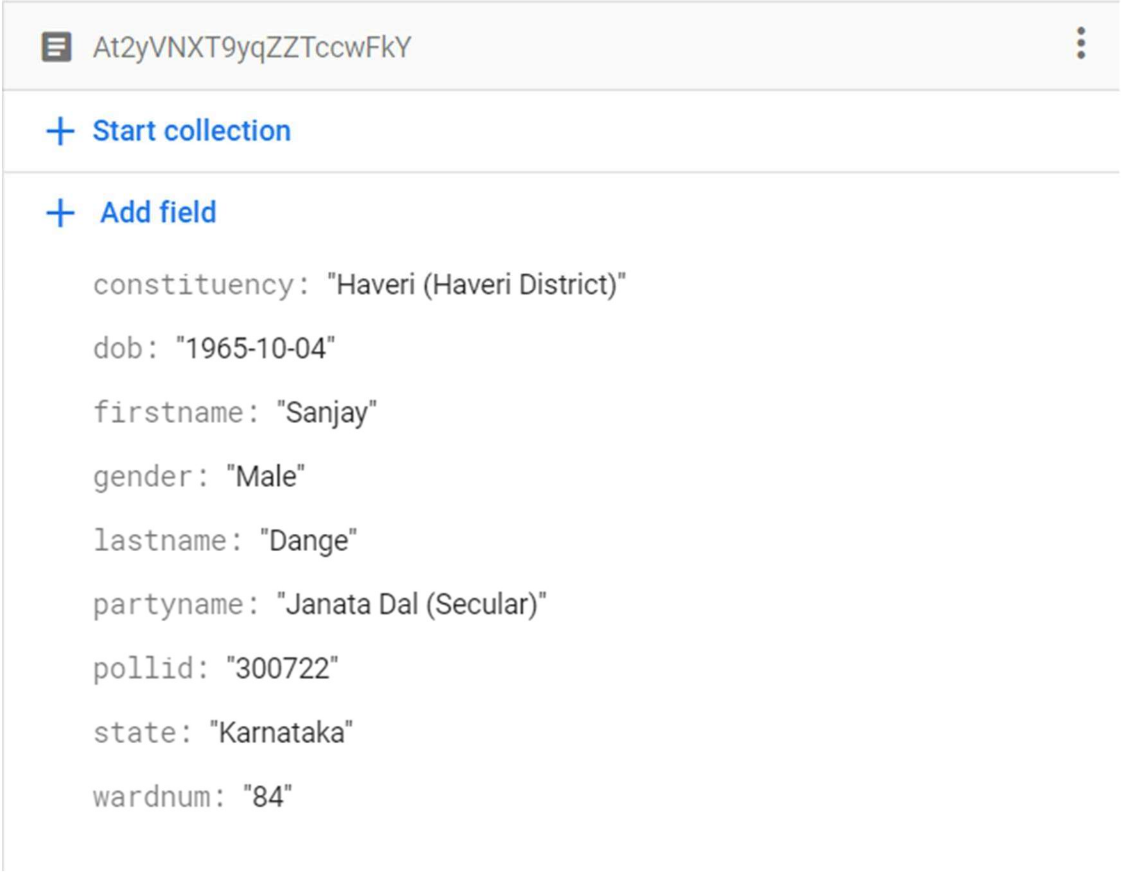
If you didn't ask to verify this address, you can ignore this email.

Thanks,

Your %APP_NAME% team

The admin can sign into the application using the login credentials provided by the Election Commission of India to facilitate the elections.

6.6 Firebase Database of Constituency Details (Sample):



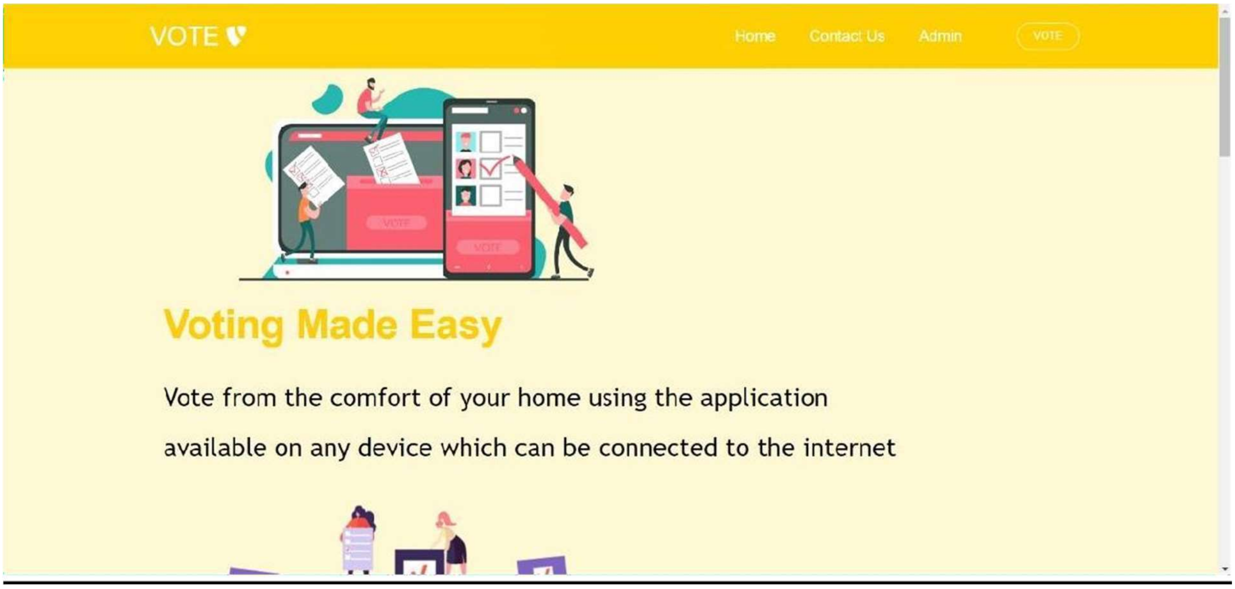
At2yVNXT9yqZZTccwFkY

```
constituency: "Haveri (Haveri District)"
dob: "1965-10-04"
firstname: "Sanjay"
gender: "Male"
lastname: "Dange"
partyname: "Janata Dal (Secular)"
pollid: "300722"
state: "Karnataka"
wardnum: "84"
```

The candidate details are entered into the database from the create poll page in the application. The page accepts details like the candidate's name, date of birth, constituency, ward number, etc. which is later displayed in the voting page so the voters can vote for the candidates of their choice.

CHAPTER 7: RESULTS

7.1 Home Page:

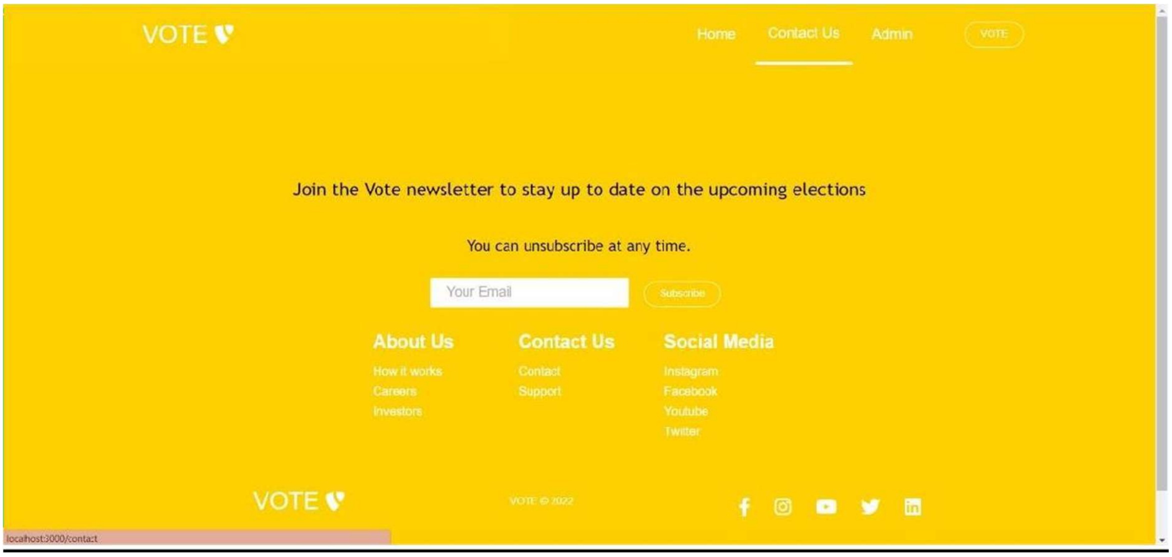


Voting Made Easy

Vote from the comfort of your home using the application available on any device which can be connected to the internet

The home page gives a brief introduction to the users of the benefit of using the application to cast the vote during the elections.

7.2 Newsletter, About Us, Contact Us and Social Media:

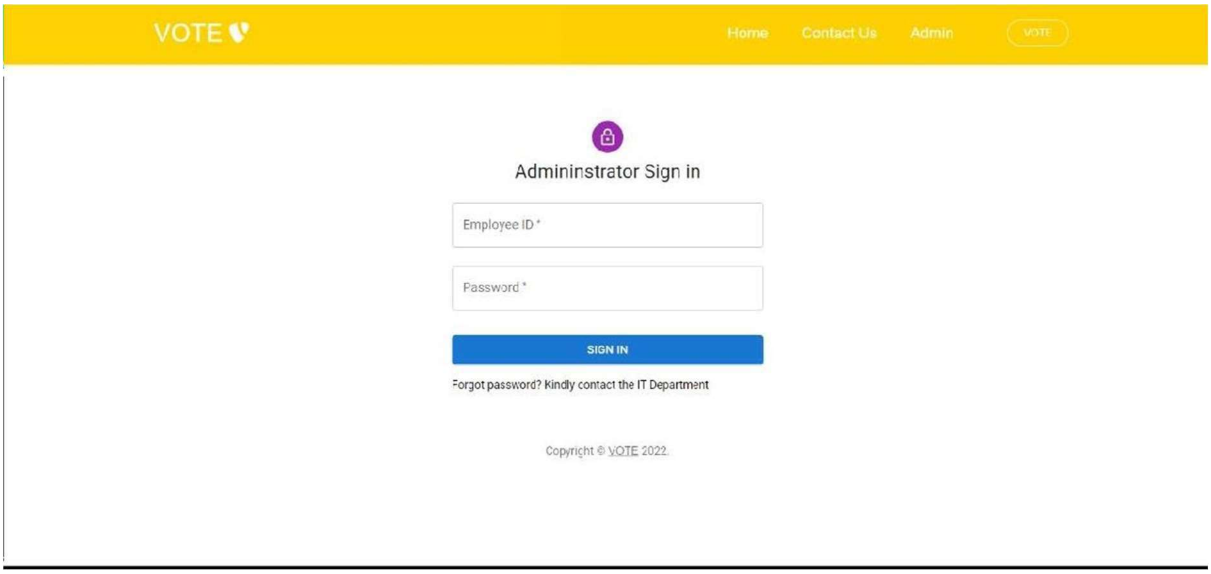


Join the Vote newsletter to stay up to date on the upcoming elections

You can unsubscribe at any time.

Your Email

7.3 Admin Login:



Forgot password? Kindly contact the IT Department

Copyright © VOTE 2022.

The administrator can sign in to the application by using any device connected to the internet and entering the correct login credentials (email and the password) which is stored on the database. Upon successful authentication of the email and the password, the admin is redirected to the admin options page, where the admin has the option to

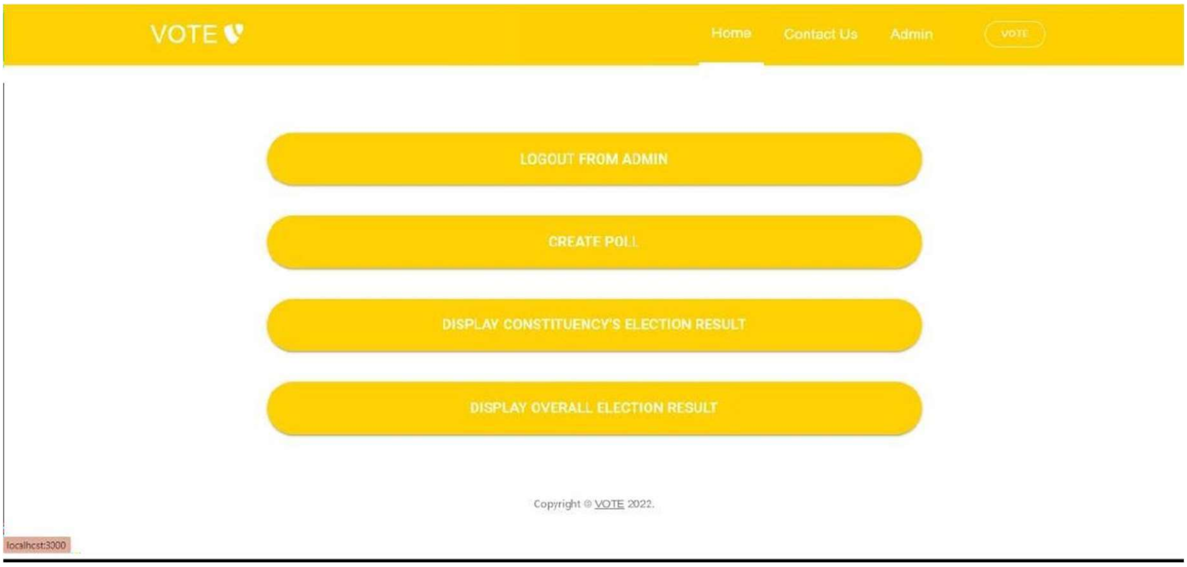
i. Logout

ii. Create a new poll

iii. Declare the election results of a particular constituency; and

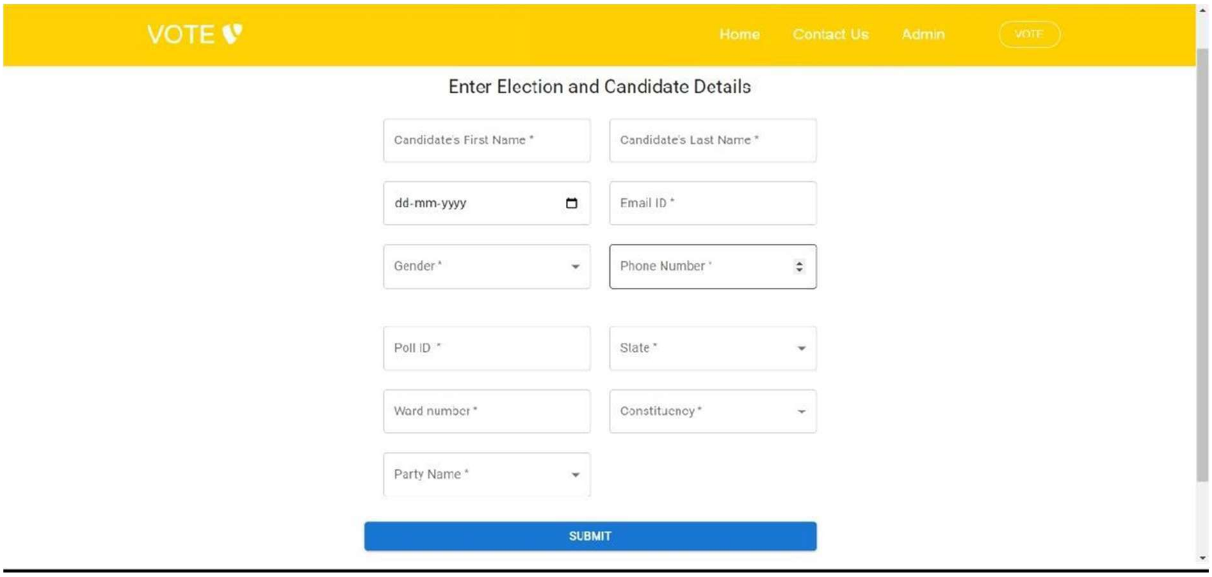
iv. Declare the overall results of the election

7.4 Admin Dashboard:


VOTE
Home
Contact Us
Admin
VOTE
LOGOUT FROM ADMIN
CREATE POLL
DISPLAY CONSTITUENCY'S ELECTION RESULT
DISPLAY OVERALL ELECTION RESULT
localhost:3000

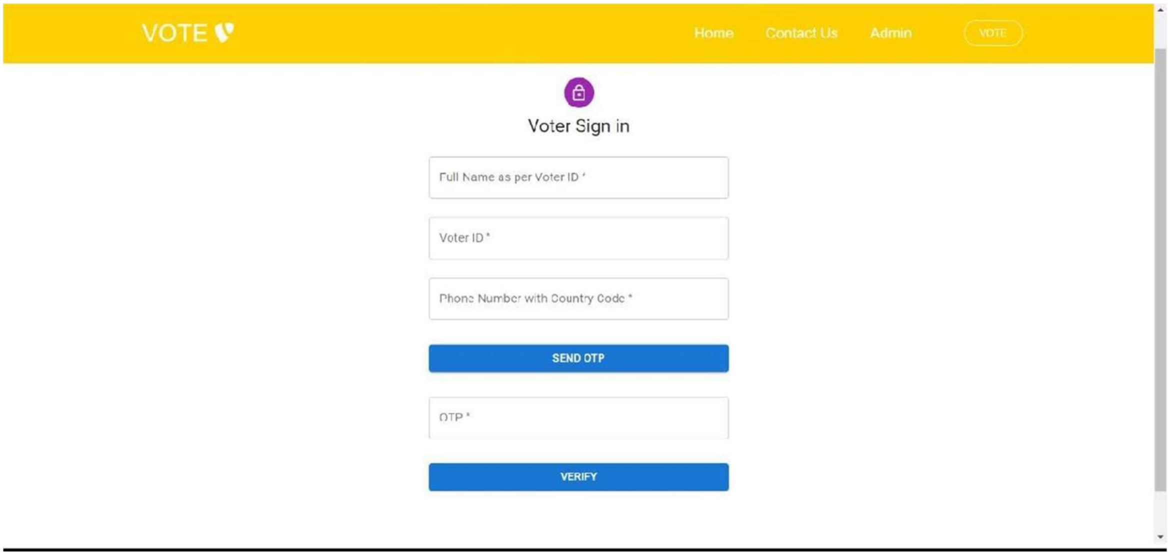
Copyright © VOTE 2022.

7.5 Admin Function – Creating Poll:



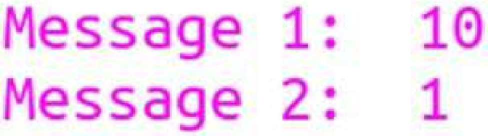
The create new poll functionality allows the admin to create and/or add a new constituency for which elections are to be conducted. The form accepts the candidate details for the particular constituency.

7.6 Voter Login:



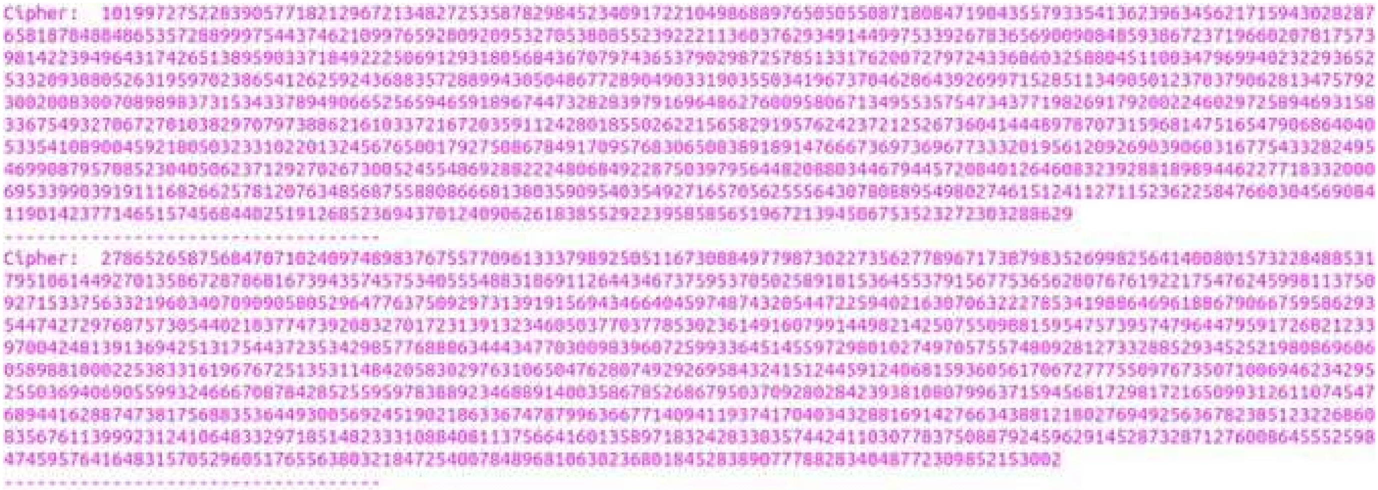
The voter is required to have a device which is connected to internet to cast the vote. The voter can cast their vote through the Dapp which is the website and the wallet account provide by the government. The voter is provided with a public and private key of an account of the registered user which has some cryptocurrency in it for dealing with the gas fee, for simplicity purposes in this project Metamask is used as wallet and Ganache is used for local blockchain and accounts deposited with ethers.

7.7 Homomorphic Encryption Properties:



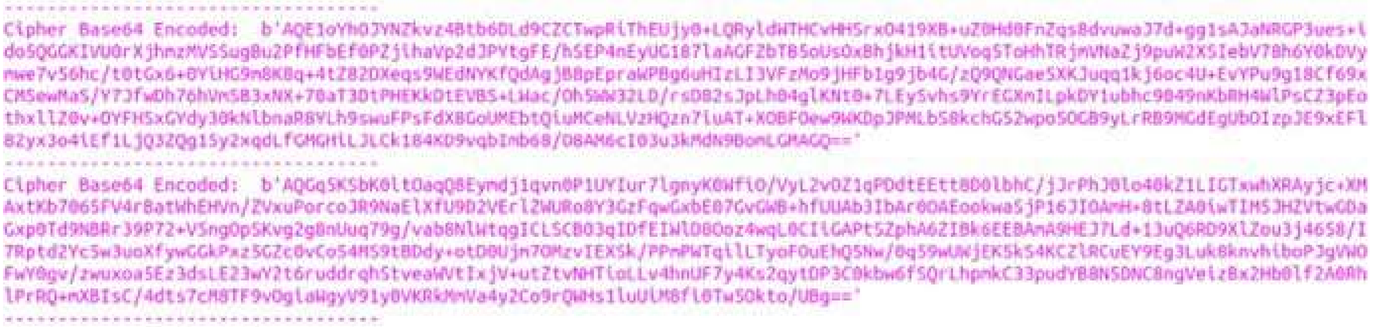
```
Message 1:  10
Message 2:  1
```

The entire demonstration of the Paillier Algorithm and homomorphic properties is done using a toolkit developed considering the example of 10 & 1 for plaintext.



```
Cipher:  1019972752283905771821296721348272535878298452340917221049868897650505508718084719043557933541362396345621715943028287
6581878488486535728899975443746210997659280920953270538085523922211360376293491449975339267836569009084859386723719660207817573
9814223949643174265138959033718492225069129318056843670797436537902987257851331762007279724336860325880451100347969940232293652
5332093880526319597023865412625924368835728899430504867728904903319035503419673704628643926997152851134905012378379062813475792
3002008380708989837315343378949066525659465918967447328283979169648627600958067134955357547343771982691792002246029725894693158
3367549327067270103829707973886216103372167203591124280185502622156582919576242372125267360414448978707315968147516547906864040
5335410890045921805032331022013245676500179275086784917095768306508389189147666736973696773332019561209269039060316775433282495
4699087957085230405062371292702673005245548692882224806849228750397956448208803446794457208401264608323928818989446227718332000
6953399039191116826625781207634856875588086668138035909540354927165705625556430780889549802746151241127115236225847660304569084
119014237714651574568440251912685236943701240906261838552922395858565196721394506753523272303288629
-----------------------------------
Cipher:  2786526587568470710240974898376755770961333798925051167308849779873022735627789671738798352699825641400801573228488531
7951061449270135867287868167394357457534055548831869112644346737595370502589181536455379156775365628076761922175476245998113750
9271533756332196034070909058052964776375092973139191569434664045974874320544722594021630706322278534198864696188679066759586293
5447427297687573054402103774739208327017231391323460503770377853023614916079914498214250755098815954757395747964479591726821233
9700424813913694251317544372353429857768886344434770300983960725993364514559729801027497057557480928127332885293452521980869606
0589881000225383316196767251353114842058302976310650476280749292695843241512445912406815936056170672777550976735071006946234295
2550369406905599324666708784285255959783889234688914003586785268679503709280284239381080799637159456817298172165099312611074547
6894416288747381756883536449300569245190218633674787996366771409411937417040343288169142766343881218027694925636782385123226860
8356761139992312410648332971851482333108840811375664160135897183242833035744241103077837508879245962914528732871276008645552598
47459576416483157052960517655638032184725400784896810630236801845283890777882834048772309852153002
-----------------------------------
```

The above is the ciphertext generated upon encryption of 10 & 1 using the Paillier Algorithm.

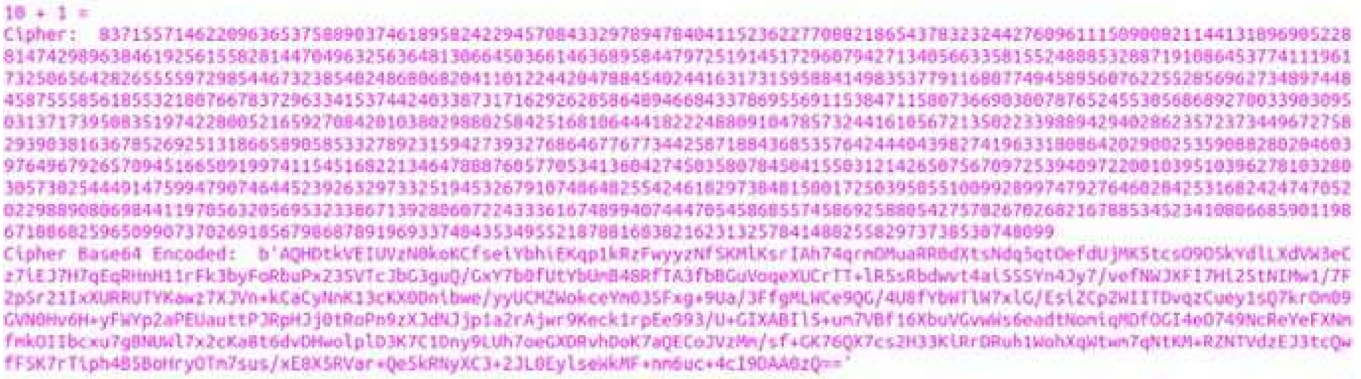


```
-----------------------------------
Cipher Base64 Encoded:  b'AQE1oYhOJYNZkvz4Btb6DLd9CZCTwpRiThEUjy0+LQRyldWTHCvHH5rx0419XB+uZ0Hd0FnZqs8dvuwaJ7d+gg1sAJaNRGP3ues+l
do5QGGKIVU0rXjhmzMVS5ugBu2PfHFbEf0PZjlhaVp2dJPYtgfE/hSEP4nEyUG187laAGFZbTB5oUsOxBhjkH1ltUVoq5ToHhTRjmVNaZj9puW2X5IebV78h6Y0kDVy
mwe7v56hc/t0tGx6+0YlHG9m8K8q+4tZ82DXeqs9WEdNYKfQdAgjB8pEpraWPBg6uHIzLI3VFzMo9jHFb1g9jb4G/zQ9QNGae5XKJuqq1kj6oc4U+EvYPu9g18Cf69x
CM5ewMaS/Y7JfwDh76hVm5B3xNX+70aT3DtPHEKkDtEVBS+lWac/Oh5WW32LD/rsDB2sJpLh04glKNt0+7LEy5vhs9YrEGXmILpkDY1ubhc9849nKbRH4WlPsCZ3pEo
thxllZ0v+OYFH5xGYdy30kNlbnaR8YLh9swuFPsFdXBGoUMEbtQiuMCeNLVzHQzn7luAT+XOBFOew9WKDpJPMLb58kchG52wpo5OGB9yLrRB9MGdEgUbOIzpJE9xEFl
8Zyx3o4lEf1LjQ3ZQg15y2xqdLfGMGHlLJLCk184KD9vqbImb68/O8AM6cI03u3kMdN9BomLGMAGQ=='
-----------------------------------
Cipher Base64 Encoded:  b'AQGq5K5bK0ltOaqQ8Eymdj1qvn0P1UYIur7lgnyK0WfiO/VyL2vOZ1qPDdtEEtt8D0lbhC/jJrPhJ0lo40kZ1LIGTxwhXRAyjc+XM
AxtKb7065FV4rBatWhEHVn/ZVxuPorcoJR9NaElXfU9D2VErl2WURo8Y3GzFqwGxbE07GvGWB+hfUUAb3IbAr0OAEookwa5jP16JIOAmH+8tLZA0iwTIM5JHZVtwGDa
Gxp0Td9NBRr39P72+V5ngOp5Kvg2g8nUuq79g/vab8NlWtqgICL5CB03qIDfEIWlD8Ooz4wqL0CIlGAPt5ZphA6ZIBk6EE8AmA9HEJ7Ld+1JuQ6RD9XlZou3j4658/I
7Rptd2Yc5w3uoXfywGGkPxz5GZc0vCo54M59t8Ddy+otD0Ujn7OMzvIEX5k/PPmPWTqilLTyoFOuEhQ5Nw/0q59wUWjEK5k54KCZlRCuEY9Eg3Luk8knvhiboPJgVWO
FwY0gv/zwuxoa5Ez3dsLE23wY2t6ruddrqhStveaWVtIxjV+utZtvNHTloLLv4hnUF7y4Ks2qytDP3C0kbw6f5QrLhpnkC33pudYB8N5DNC8ngVeizBx2Hb0lf2A0Rh
lPrRQ+mXBIsC/4dts7cM8TF9vOglaWgyV91y0VKRkMmVa4y2Co9rQWHs1luUlM8fl0Tw5Okto/UBg=='
-----------------------------------
```

The above is the ciphertext upon encoding of 10 & 1 using the toolkit utils, the encoding scheme selected is base64 encoding scheme.

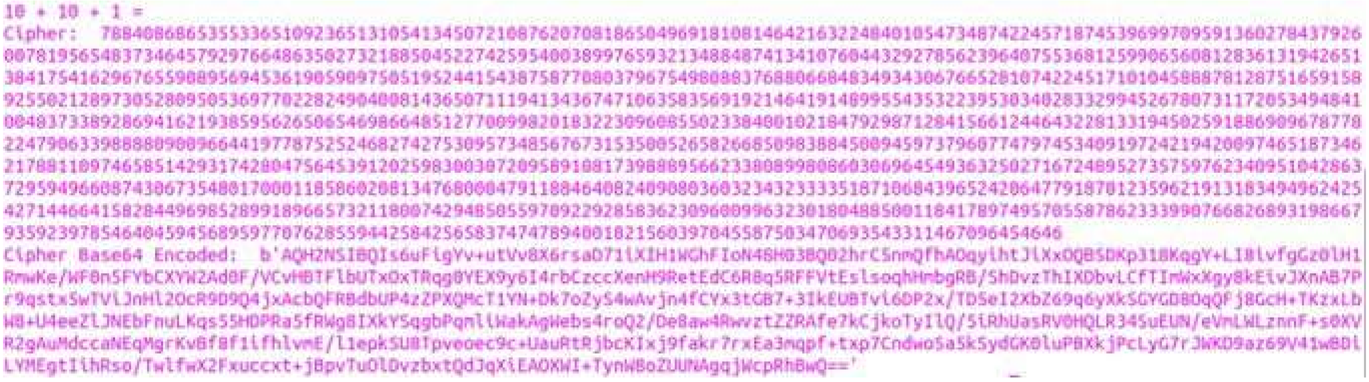
7.8 Cipher Text:

The below screenshots are the properties of homomorphic encryption being demonstrated.



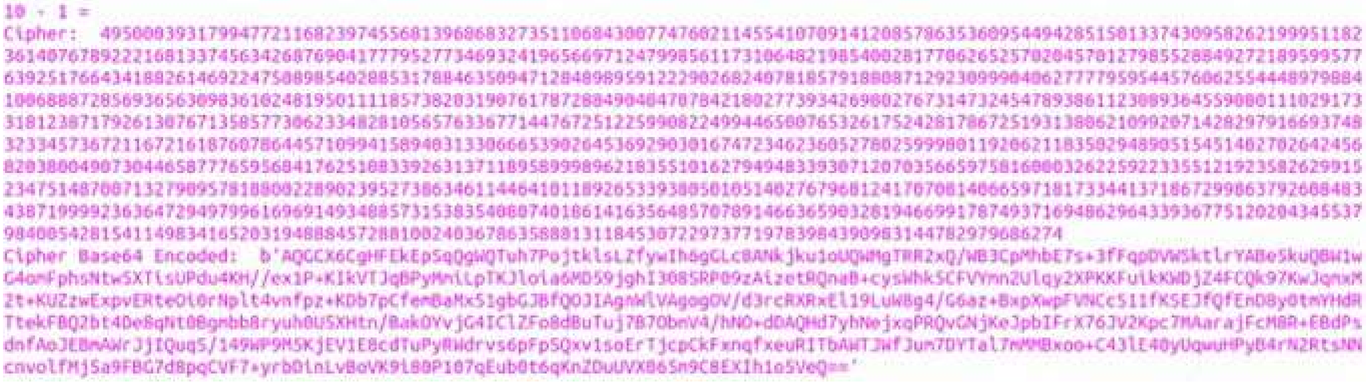
```
10 + 1 =
Cipher:  8371557146220963653758890374618958242294570843329789478404115236227708821865437832324427609611150900821144131896905228
8147429896384619256155828144704963256364813066450366146368958447972519145172960794271340566335815524888532887191086453774111961
7325065642826555597298544673238548248680682041101224420478845402441631731595884149835377911688774945895607622552856962734897448
4587555856185532180766783729633415374424033873171629262858648946684337869556911538471158073669038078765245530568689270033983095
03137173950835197422800521659270842010380298680258425168106444182224880910478573244161056721358223398894294028623572373449672758
2939038163678526925131866589058533278923159427393276864677677344258718843685357642444043982741963318086420290025359088280204603
9764967926570945166509199741154516822134647888760577053413604274503580784504155031214265075670972539409722001039510396278103280
3057382544491475994790746445239263297332519453267910748648255424618297384815001725039585510099289974792764602842531682424747052
02298890806984411970563205695323386713928806072243336167489940744470545868557458692588054275782670268216788534523410806685901198
671886825965099073702691856798687891969337484353495521878816838216231325784148825582973738530748099
Cipher Base64 Encoded:  b'AQHDtkVEIUVzN0koKCfseiYbhiEKqp1kRzFwyyzNfSKMlKsrIAh74qrmOMuaRRBdXtsNdq5qtOefdUjMK5tcsO9O5kYdlLXdVW3eC
z7iEJ7H7qEqRHnH11rFk3byFoRbuPx23SVTcJbG3guQ/GxY7b0fUtYbUm848RfTA3fbBGuVoqeXUCrTT+lR5sRbdwvt4alSSSYn4Jy7/vefNWJXFI7HL25tNIMw1/7F
2pSr21IxXURRUTYKawz7XJVn+kCaCyNnK13cKX0Dnibwe/yyUCMZWokceYm035Fxg+9Ua/3FfgMLWCe9QG/4U8fYbWTlW7xlG/EslZCp2WIITDvqzCuey1sQ7krOm09
GVN0Hv6H+yFWYp2aPEUauttPJRpHJj0tRoPn9zXJdNJjp1a2rAjwr9Kmck1rpEe993/U+GIXABIl5+um7VBf16XbuVGvwWs6eadtNomiqMDfOGI4eO749NcReYeFXNm
fmkOIIbcxu7gBNUWl7x2cKa8t6dvDHwolplD3K7C1Dny9LUh7oeGXDRvhDoK7aQECoJVzMm/sf+GK76QX7cs2H33KlRrDRuh1WohXqWtwn7qNtKM+RZNTVdzEJ3tcQw
fFSK7rTiph485BoHryOTm7sus/xE8X5RVar+Qe5kRNyXC3+2JL0EylseWkMF+nm6uc+4c19DAA0zQ=='
```

The above depicted output is one of the homomorphic encryption properties: addition is being demonstrated and the cipher is base64 encoded.



```
10 + 10 + 1 =
Cipher:  7884086865355336510923651310541345072108762070818650496918108146421632248401054734874224571874539699709591360278437926
0078195654837346457929766486350273218850452274259540038997659321348848741341076044329278562396407553681259906560812836131942651
38417541629676559088956945361905909750519524415438758770803796754980883768806684834934306766528107422451710104588878128751659158
9255021289730528095053697702282490400814365071119413436747106358356919214641914899554353223953034028332994526780731172053494841
0048373389286941621938595626506546986648512770099820183223096085502338400102184792987128415661244643228133194502591886909678778
2247906339888809009664419778752524682742753095734856767315350052658266850983884500945973796077479745340919724219420097465187346
2178811097465851429317428047564539120259830030720958910817398889566233808998086030696454936325027167248952735759762340951042863
7295949660874306735480170001185860208134768000479118846408240908036032343233335187106843965242064779187012359621913183494962425
4271446641582844969852899189665732118007429485055970922928583623096009963230180488500118417897495705587862333990766826893198667
935923978546404594568959770762855944258425658374747894001821560397045587503470693543311467096454646
Cipher Base64 Encoded:  b'AQH2NSIBQIs6uFlgYv+utVv8X6rsaD71iXIH1WGhFIoN48H03BQ02hrC5nmQfhAOqyihtJiXxOQBSDKp318KqgY+L18lvfgGz0lH1
RmwKe/WF0n5FYbCXYW2Ad0F/VCvHBTFlbUTxOxTRqg0YEX9y6I4rbCzccXenH9RetEdC6R8q5RFFVtEslsoqhHmbgRB/ShDvzThIXDbvLCfTImWxXgy8kEivJXnAB7P
r9qstx5wTVlJnHl2OcR9D9Q4jxAcbQFRBdbUP4zZPXQMcT1YN+Dk7oZyS4wAvjn4fCYx3tGB7+3IkEUBTvi6DP2x/TD5eI2XbZ69q6yXkSGYGD8DqQFj8GcH+TKzxLb
W8+U4eeZlJNEbFnuLKqs55HDPRa5fRWg8IXkY5qgbPqnliWakAgWebs4roQ2/De8aw4RwvztZZRAfe7kCjkoTy1lQ/5iRhUasRV0HQLR345uEUN/eVmLWLznnF+s0XV
R2gAuMdccaNEqMgrKv6f8f1ifhlvmE/l1epk5U8Tpveoec9c+UauRtRjbcKIxj9fakr7rxEa3mqpf+txp7Cndwo5a5k5ydGK0luPBXkjPcLyG7rJWKD9az69V41wBDi
LYMEgtIihRso/TwlfwX2Fxuccxt+jBpvTuOlDvzbxtQdJqXiEAOXWI+TynWBoZUUNAgqjWcpRhBwQ=='
```

The arithmetic addition isn’t restricted to only 2 number or plaintext form, it can be more than 2 also and that is being demonstrated in the above output.



```
10 - 1 =
Cipher:  4950003931799477211682397455681396868327351106843007747602114554107091412085786353609544942851501337430958262199951182
3614076789222168133745634268769041777952773469324196566971247998561173106482198540028177062652570204570127985528849272189599577
6392517664341882614692247508985402885317884635094712848989591222902682407818579188087129230999040627777959544576062554448979884
1006888728569365630983610248195011118573820319076178728849040470784218027739342698027673147324547893861123089364559080111029173
3181238717926130767135857730623348281056576336771447672512259908224994465007653261752428178672519313806210992071428297916693748
3233457367211672161876078644571099415894031330666539026453692903016747234623605278025999801192062118350294890515451402702642456
8203800490730446587776595684176251083392631371189589998962183551016279494833930712070356659758160003262259223355121923582629915
2347514870071327989578188002289023952738634611446410118926533938050105140276796812417070814066597181733441371867299863792608483
4387199992363647294979961696914934885731538354088740186141635648570789146636590328194669917874937169486296433936775120204345537
984005428154114983416520319488845728810024036786358881311845307229737719783984390983144782979686274
Cipher Base64 Encoded:  b'AQGCX6CgHFEkEpSqQgWQTuh7PojtklsLZfywIhagGLcBANkjku1oUQWMgTRR2xQ/WB3CpMhbE7s+3fFqpDVWSktlrYABeSkuQBW1w
G4omFphsNtwSXTisUPdu4KH//ex1P+KIkVTJgBPyMmiLpTKJloia6MD59jghI308SRP09zAizetRQnaB+cysWhk5CFVYmn2Ulqy2XPKKFuikKWDjZ4FCQk97KwJqmxM
2t+KUZzwExpvERteOi0rNplt4vnfpz+KDb7pCfemBaMx51gbGJBfQOJIAgnWlVAgogOV/d3rcRXRxEl19LuW8g4/G6az+BxpXwpFVNCc511fKSEJfQfEnD8y0tmYHdR
TtekFBQ2bt4DeBqNt0BgmbbBryuh0USXHtn/Bak0YvjG4IClZFo8dBuTuj7B7ObmV4/hNO+dDAQHd7yhNejxqPRQvGNjKeJpbIFrX76JV2Kpc7MAarajFcMBR+EBdPs
dnfAoJEBmAWrJjIQuq5/149WP9M5KjEV1E8cdTuPyRWdrvs6pFp5Qxv1soErTjcpCkFxnqfxeuRITbAWTJWfJum7DYTal7mMMBxoo+C43lE40yUqwuHPyB4rN2RtsNN
cnvolfMj5a9FBG7d8pqCVF7+yrb0inLvBoVK9i80P107qEub0t6qKnZDuUVX865n9C8EXIh1o5VeQ=='
```

The above depicted output is one of the homomorphic encryption properties: subtraction is being demonstrated and the cipher is base64 encoded.

CHAPTER 8: IMPACT OF YOUR PROJECT TOWARDS SOCIETY/ENVIRONMENT

In the society in every city, it is observed that the present voting system requires the people to visit the assigned voting center and stand in a queue for a long time to cast their vote. This seems like a cumbersome process in this digital era, this process is also a little tough for the aged people and the entire method is time consuming. The day of voting is a holiday and the educated and the other people who feel the same about the process try to avoid it by not voting at all. This becomes one of the major reasons why the voting percentages in the cities is way less compared to rural and sub-urban areas of a locality. The other major issue with this existing system is rigging and coercion at the place of voting, which makes the system of voting not so secure and lessen the freedom of choice.

In order to solve some of these problems there is a one stop solution that is online voting system and supplementing it with blockchain makes the process to be carried out in a secured way. With the system of e-voting voters neither need to worry about getting stuck in a long queue and waste their time to exercise their fundamental right nor get worked up about poll riggings and other malign methods of coercion. They can sit at their place of comfort and cast their vote to the candidate of their choice. They just need a mobile phone or a computer having access to a wallet containing their voting account and a connection to the internet.

CHAPTER 9: CONCLUSION

Online voting systems, in our opinion, have a security flaw that allows authority to commit fraud or manipulate the system in ways that are difficult to detect by other users.

The various issues uncovered in these early attempts at online voting can be solved using blockchain.

Homomorphic encryption now provides an irrefutable method of ensuring the correctness of each vote cast. Blockchain technology is one of the most secure ways to store the information. By opting for a decentralized method over a centralized and traditional voting system, the On-Stream voting system is made more secure.

This implies that by switching from a centralized database to a peer network of blockchain that store data the data/votes are safe and cannot be tampered with since the data in the blocks is immutable.

It even assures that the election rules do not change because they are kept as a Smart Contract of the blockchain, so because of this online e voting system using blockchain will be very helpful towards the society. It will also be very useful to the government where people need not to go to the polling station and cast their vote, they can conveniently cast their vote from their place, they just need a mobile phone (or) a laptop which is connected to internet, that it. And even for government there will be lot of resources and manpower will be saved because the officials of the voting party can be at one place, and they can take a count of the number ofvotes of the particular region with more accurate way so that there will be no overhead In the voting process.

CHAPTER 10: REFERENCES

[1] Bishop, Sylvia, and Anke Hoeffler. “Free and Fair Elections: A New Database.” Journal of Peace Research, vol. 53, no. 4, Sage Publications, Ltd., 2016, pp. 608–16, http://www.jstor.org/stable/43920613.

[2] R. Hanifatunnisa and B. Rahardjo, "Blockchain-based e-voting recording system design," 2017 11th International Conference on Telecommunication Systems Services and Applications (TSSA), 2017, pp. 1-6, DOI: 10.1109/TSSA.2017.8272896.

[3] Lemuria Carter and France Bélanger. 2012. Internet voting and political participation: an empirical comparison of technological and political factors. SIGMIS Database 43, 3 (August 2012), 26–46. DOI: https://doi.org/10.1145/2351848.2351851.

[4] Jafar, U.; Aziz, M.J.A.; Shukur, Z. Blockchain for Electronic Voting System—Review and Open Research Challenges. Sensors 2021, 21, 5874. https://doi.org/10.3390/s21175874

[5] Tan, W., Zhu, H., Tan, J., Zhao, Y., Xu, L. D., & Guo, K. (2021). A novel service level agreement model using blockchain and smart contract for cloud manufacturing in industry 4.0. Enterprise Information Systems, 1–26. doi:10.1080/17517575.2021.1939426

[6] S. Hakak, W. Z. Khan, G. A. Gilkar, M. Imran and N. Guizani, "Securing Smart Cities through Blockchain Technology: Architecture, Requirements, and Challenges," in IEEE Network, vol. 34, no. 1, pp. 8-14, January/February 2020, DOI: 10.1109/MNET.001.1900178.

[7] Kim, Hyunyeon, Kyung Eun Kim, Soohan Park and Jong-Mo Sohn. “E-voting System Using Homomorphic Encryption and Blockchain Technology to Encrypt Voter Data.” ArXiv abs/2111.05096 (2021): n. pag.

[8] Sadia, Kazi, Md. Masuduzzaman, Rajib Kumar Paul and Anik Islam. “Blockchain-Based Secure E-Voting with the Assistance of Smart Contract.” (2020).

[9] Jon Wallace, Hans Kundnani, Elizabeth Donnelly, “The importance of democracy”, https://www.chathamhouse.org/2021/04/importance-democracy(2021)

[10] Paul Cuff - Sanjeev Kulkarni - Mark Wang - John Sturm, “Voting Research – VotingTheory”, https://www.princeton.edu/~cuff/voting/theory.html (2021) Sylvia Bishop and Anke Hoeffler,” Free and Fair elections: A new database” https://www.jstor.org/stable/43920613 (2016)

[11] ” Paper-Ballot-Advantages-And-Disadvantages” https://www.ipl.org/essay/Paper-Ballot-Advantages-And-Disadvantages-PCUJ2FZSK5U

[12] Hina Khan, “Top 10 advantages and disadvantages of paper ballot voting”,(2017) https://www.worldblaze.in/advantages-disadvantages-of-paper-ballot-voting/

[13] Sarah Diamond, “Are You Voting “No” to Paper Ballots”, (2018) https://www.eballot.com/blog/voting-no-to-paper-ballots

[14] J Paul Gibson, Robert Krimmer, Vanessa Teague & Julia Pomares,” A review of E-voting: the past, present and future”,(2016),.DOI: 10.1007/s12243-016-0525-8

[15] Xing Shu Li, Hyang ran Lee, Marley Lee, Jae-young Choi, “ A Study of Vulnerabilities in E-Voting System”, May 2015 DOI:10.14257/astl.2015.95.25, (2015)

[16] F. Þ. Hjálmarsson, G. K. Hreiðarsson, M. Hamdaqa and G. Hjálmtýsson, "Blockchain-Based E-Voting System," 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), 2018, pp. 983-986, DOI: 10.1109/CLOUD.2018.00151.

[17] Lemuria Carter and France Bélanger, 2012,” Internet voting and political participation: an empirical comparison of technological and political factors” doi/10.1145/2351848.2351851

[18] Ruhi Taş and Ömer Özgür Tanrıöver, 2021 “A Manipulation Prevention Model for Blockchain-Based E-Voting Systems” DOI: 10.1155/2021/6673691

[19] Uzma Jafar, Mohd Juzaiddin Ab Aziz and Zarina Shukur,2021,” Blockchain for Electronic Voting System-Review and Open Research Challenges”, DOI: 10.3390/s21175874

[20] Kashif Mehboob Khan, Junaid Arshad and Muhammad Mubashir Khan,” Secure Digital Voting System based on Blockchain Technology”

[21] Wenan Tan, Hai Zhu, Jinjing Tan, Yao Zhao, Li Da Xu & Kai Guo, (2021)” Internet voting and political participation: an empirical comparison of technological and political factors: ACM SIGMIS Database: the DATABASE for Advances in Information Systems: Vol43, No 3”, DOI: 10.1080/17517575.2021.1939426

[22] Yi, H. Securing e-voting based on blockchain in the P2P network. J Wireless Com Network 2019, 137 (2019). https://doi.org/10.1186/s13638-019-1473-6

[23] V. F. Rocha and Julio López,2018,” An Overview on Homomorphic Encryption Algorithms”

[24] N. Kakade and U. Patel, "Secure Secret Sharing Using Homomorphic Encryption," 202011th International Conference on Computing, Communication and Networking Technologies (ICCCNT), 2020, pp. 1-7, DOI: 10.1109/ICCCNT49239.2020.9225325.

[26] Bhabendu Kumar Mohanta, Debasish Jena, Soumyashree S Panda, Srichandan Sobhanayak, (2019) “Blockchain Technology: A Survey on Applications and Security Privacy Challenges”, DOI:10.1016/j.iot.2019.100107

[27] Prof. Mrunal Pathak, Amol Suradkar. Ajinkya Kadam, Akansha Ghodeswar, “Blockchain-Based E-Voting System”, (2021), DOI:10.32628/IJSRST2182120

[28] K. Patidar and S. Jain, "Decentralized E-Voting Portal Using Blockchain," 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Kanpur, India, 2019, pp. 1-4, DOI: 10.1109/ICCCNT45670.2019.8944820.

[29] Samuel Fosso Wambaa Maciel M. Queirozb(2020)“ Blockchain in the operations and supply chain management: Benefits, challenges and future research opportunities" DOI: 10.1016/j.ijinfomgt.2019.102064

[30] Sharmat, F.M. & Ali, Md. Asraf & Mia, Md Rajib & Khatun, Mst.Arifa. (2020). The Future of Electronic Voting System Using Blockchain. International Journal of Scientific & Technology Research. 09. 4131-4134.

[31] Gentry, C. (2009). Fully homomorphic encryption using ideal lattices. Proceedings of the 41st annual ACM symposium on Symposium on the theory of computing-STOC '09. Vol. 9.

[32] Gentry, C. (2013). Homomorphic Encryption from Learning with Errors: Conceptually Simpler, Asymptotically Faster, Attribute-Based. CRYPTO Santa Barbara 2013.

[33] Van Dijk, M., Gentry, C., Halevi, S., & Vaikuntanathan, V. (2010, May). Fully homomorphic encryption over the integers. In Annual International Conference on the Theory and Applications of Cryptographic Techniques (pp. 24-43). Springer, Berlin, Heidelberg.

[34] Brakerski, Z., Gentry, C., & Vaikuntanathan, V. (2014). (Leveled) fully homomorphic encryption without bootstrapping. ACM Transactions on Computation Theory (TOCT), 6(3), 13.

[35] Brakerski, Z. (2012). Fully homomorphic encryption without modulus switching from classical GapSVP. In Advances in cryptology–crypto 2012 (pp. 868-886). Springer, Berlin, Heidelberg.

[36] Fan, J., & Vercauteren, F. (2012). Somewhat Practical Fully Homomorphic Encryption. IACR Cryptology ePrint Archive, 2012, 144.

[37] Gentry, C., Sahai, A., & Waters, B. (2013). Homomorphic encryption from learning with errors: Conceptually simpler, asymptotically faster, attribute based. In Advances inCryptology–CRYPTO 2013 (pp. 75-92). Springer, Berlin, Heidelberg.

[38] Gentry, C., & Halevi, S. (2011, May). Implementing gentry's fully homomorphic encryption scheme. In Annual international conference on the theory and applications of cryptographic techniques (pp. 129-148). Springer, Berlin, Heidelberg.

[39] Simple Encrypted Arithmetic Library (release 3.1.0). Microsoft Research, Redmond, WA

[40] Halevi, S., & Shoup, V. (2014, August). Algorithms in helib. In the International Cryptology Conference (pp. 554-571). Springer, Berlin, Heidelberg.

[41] S. Behera and J. R. Prathuri, "Application of Homomorphic Encryption in Machine Learning," 2020 2nd PhD Colloquium on Ethically Driven Innovation and Technology for Society (PhD EDITS), 2020, pp. 1-2, DOI: 10.1109/PhDEDITS51180.2020.9315305.

[42] Y. Yamada, K. Rohloff and M. Oguchi, "Homomorphic Encryption for Privacy-Preserving Genome Sequences Search," 2019 IEEE International Conference on Smart Computing (SMARTCOMP), 2019, pp. 7-12, DOI: 10.1109/SMARTCOMP.2019.00021.

[43] S. Gupta and G. Arora, "Use of Homomorphic Encryption with GPS in Location Privacy," 2019 4th International Conference on Information Systems and Computer Networks (ISCON), 2019, pp. 42-45, DOI: 10.1109/ISCON47742.2019.9036149.

[44] P. Paillier. Public-key cryptosystems based on composite degree residuality classes. In Proceedings of the 17th international conference on Theory and application of cryptographic techniques (EUROCRYPT'99), pages 223–238, Prague, Czech Republic, May 1999. Springer-Verlag.

CHAPTER 11: SELF ASSESSMENT OF PO-PSO ATTAINMENT

Program Outcomes (PO)	Justification
PO1. Engineering Knowledge:	We have learnt various concepts in engineering like blockchain and web development which we have used in this project
PO2. Problem Analysis:	We have come across to this problem where people and government spending lot of time on this election voting system. So, with this centralized system the problem can be solved
PO3. Design Development of solutions:	Understanding the problem and learned concepts of Web development and applied that knowledge to design the solution
PO5. Modern Tools:	Use of metamask, VS Code, ganache, Prettier etc.… is helped to solve this problem
PO6. The Engineer and society:	Observing the root cause of the problem and designing the solution as an engineer which helps society which will give the groundbreaking solution
PO8. Ethics:	Following the work ethics and approaching the problem to solve the issue
PO9. Individual and Teamwork:	Analyzing the whole problem statement and distributing the work among the team and having sync up to get to know the updates and solving if any issues faced by us
PO10. Communication:	Having group discussion among ourselves and discussing the practical approach towards the problem and understanding the point of view of each person on the specific topic
PO11: Project management and finance:	Distributing the project and reducing the cost

	by the dividing among the team so that no one will bear the overall price by single person.
PO12. Life-long learning:	This project will also be upgraded according to the requirement and also this will be lifelong learning along with the updating of the project

Program Specific Outcomes (PSO)	**Justification**
PSO1. Professional Skills:	We have applied web development and blockchain knowledge to analysis of the project. Outcomes and results were analyzed proficiently.
PSO2. Problem Solving Skills:	Solving different types of errors like blockchain connectivity issues and also web site responsiveness etc.…
PSO3. Ethics and career development:	Understanding every bit of the project so that it will help us to tackle any type of project in our career and with the help of ethics we will shape out our professional behavior

Plag1.docx

ORIGINALITY REPORT

6%	6%	3%	%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	whatis.techtarget.com Internet Source	2%
2	arxiv.org Internet Source	1%
3	firebase.google.com Internet Source	1%
4	Uzma Jafar, Mohd Juzaiddin Ab Aziz, Zarina Shukur. "Blockchain for Electronic Voting System—Review and Open Research Challenges", Sensors, 2021 Publication	1%
5	etd.uum.edu.my Internet Source	<1%
6	www.hindawi.com Internet Source	<1%
7	K Roopa, B S Gokul, S Kaushik Arakalgud. "Use case of Paillier Homomorphic Algorithm for Electronic-Voting Systems", 2021 5th International Conference on Electrical, Electronics, Communication, Computer	<1%

	Technologies and Optimization Techniques (ICEECCOT), 2021 Publication	
8	www.ijsrd.com Internet Source	<1%
9	www.x-mol.com Internet Source	<1%
10	www.ijariit.com Internet Source	<1%
11	j.mecs-press.net Internet Source	<1%
12	www.coursehero.com Internet Source	<1%
13	jwcn-eurasipjournals.springeropen.com Internet Source	<1%

Exclude quotes	On	Exclude matches	Off
Exclude bibliography	On		