Submission Information

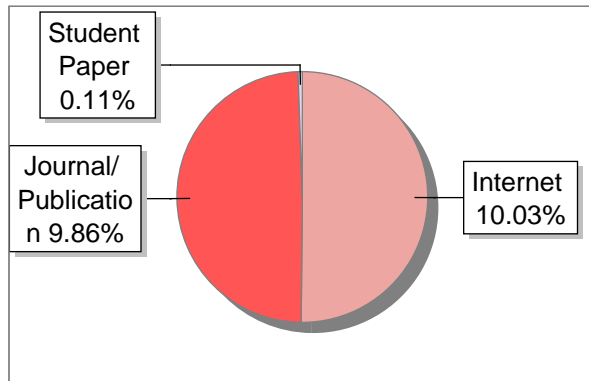|	
Author Name	Rohith Marath
Title	E-STAMPING IN DIGITAL VOTING SYSTEM USING BLOCK..
Paper/Submission ID	773144
Submission Date	2023-06-13 18:47:46
Total Pages	47
Document type	Project Work

Result Information

Similarity **20 %**

1	10	20	30	40	50	60	70	80	90

Sources Type

Student Paper 0.11%

Journal/Publication 9.86%

Internet 10.03%

Report Content

Words < 14, 3.81%

Ref/Bib 7.64%
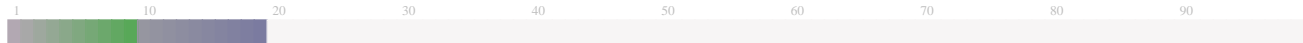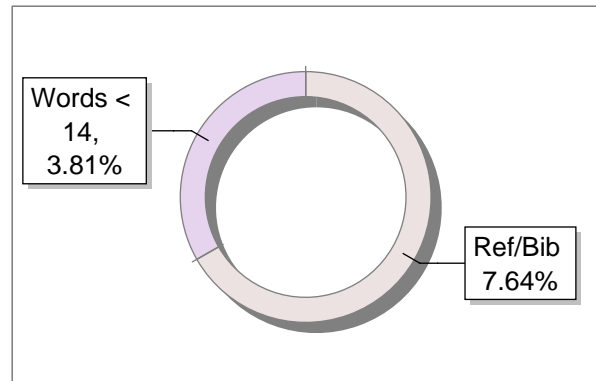
Exclude Information

Quotes	Not Excluded
References/Bibliography	Not Excluded
Sources: Less than 14 Words Similarity	Not Excluded
Excluded Source	**0 %**
Excluded Phrases	Not Excluded

A Unique QR Code use to View/Download/Share Pdf File

DrillBit

				A-Satisfactory (0-10%)
				B-Upgrade (11-40%)
20	**91**	**B**		C-Poor (41-60%)
SIMILARITY %	MATCHED SOURCES	GRADE		D-Unacceptable (61-100%)

LOCATION	MATCHED DOMAIN	%	SOURCE TYPE
1	IEEE 2018 International Conference on Smart City and Emerging Techn, by Purandare, Himanshu- 2018	1	Publication
2	qdoc.tips	1	Internet Data
3	en.wikipedia.org	1	Internet Data
4	www.mdpi.com	1	Internet Data
5	papers.ssrn.com	1	Internet Data
6	dspace.daffodilvarsity.edu.bd 8080	1	Publication
7	www.ncbi.nlm.nih.gov	1	Internet Data
8	www.tjprc.org	<1	Publication
9	Design of the multicast service for mobile users in the 8216 network by Chun-Shia-21	<1	Publication
10	www.eurchembull.com	<1	Publication
11	www.itm-conferences.org	<1	Publication
12	www.academia.edu	<1	Internet Data
13	www.dx.doi.org	<1	Publication

14	Thesis Submitted to Shodhganga Repository	<1	Publication
15	www.eurchembull.com	<1	Publication
16	www.tjprc.org	<1	Publication
17	epdf.pub	<1	Internet Data
18	www.academia.edu	<1	Internet Data
19	Blockchain a paradigm shift in business practices by Kizildag-2019	<1	Publication
20	ijeat.org	<1	Internet Data
21	www.ijert.org	<1	Internet Data
22	qdoc.tips	<1	Internet Data
23	www.tjprc.org	<1	Publication
24	studymoose.com	<1	Internet Data
25	www.ncbi.nlm.nih.gov	<1	Internet Data
26	ijircce.com	<1	Publication
27	ijircce.com	<1	Publication
28	OCR applied to an electronic voting system, by J. K. Espinosa I. - 2007	<1	Publication
29	Proceedings of First International Conference on Computing, Communications, and by Pradee-2020	<1	Publication
30	IEEE 2020 IEEE International IOT, Electronics and Mechatronics Conference (IEM	<1	Publication
31	www.slideshare.net	<1	Internet Data
32	www.scribd.com	<1	Internet Data

33	moam.info	<1	Internet Data
34	Lecture Notes in Computer Science E-Voting and Identity Volume 9269, by Haenni, Rolf Koeni- 2015	<1	Publication
35	www.jcreview.com	<1	Publication
36	eproceeding.undiksha.ac.id	<1	Internet Data
37	smec.ac.in	<1	Publication
38	www.dx.doi.org	<1	Publication
39	Jaganath University Thesis Published - www.inflibnet.ac.in	<1	Publication
40	Programming Parallel Vision Algorithms a Dataflow Language Approach by Shapiro-1988	<1	Publication
41	moam.info	<1	Internet Data
42	Model-checking Driven Design of Interactive Systems by Antoni-2007	<1	Publication
43	Multi-Capacity Bin Packing with Dependent Items and its application to the packi by Bassem-2016	<1	Publication
44	Thesis Submitted to Shodhganga, shodhganga.inflibnet.ac.in	<1	Publication
45	docplayer.net	<1	Internet Data
46	jips-k.org	<1	Publication
47	www.omicsonline.org	<1	Internet Data
48	americanaffairsjournal.org	<1	Internet Data
49	A Parallel Ghosting Algorithm for The Flexible Distributed Mesh Database by Mubarak-2013	<1	Publication
50	qdoc.tips	<1	Internet Data

51	1library.co	<1	Internet Data
52	energyinformatics.springeropen.com	<1	Internet Data
53	giapjournals.com	<1	Publication
54	ijisrt.com	<1	Publication
55	Institution of Engineering and Technology IET International Confere, by Gunjal, B.L. Mali,- 2012	<1	Publication
56	www.freepatentsonline.com	<1	Internet Data
57	www.ncbi.nlm.nih.gov	<1	Internet Data
58	IEEE 2018 IEEE 11th Conference on Service-Oriented Computing and Applications by -2018	<1	Publication
59	ijitee.org	<1	Internet Data
60	Submitted to Visvesvaraya Technological University, Belagavi	<1	Student Paper
61	Thesis submitted to dspace.mit.edu	<1	Publication
62	Thesis Submitted to Shodhganga, shodhganga.inflibnet.ac.in	<1	Publication
63	www.noveltyjournals.com	<1	Publication
64	Adapting Free, Prior, and Informed Consent (FPIC) to Local Contexts in REDD L by Pham-2015	<1	Publication
65	moam.info	<1	Internet Data
66	moam.info	<1	Internet Data
67	redcol.minciencias.gov.co	<1	Publication
68	www.ncbi.nlm.nih.gov	<1	Internet Data

A Project Report On E-STAMPING IN DIGITAL VOTING SYSTEM USING BLOCK CHAIN AND CLOUD TECHNOLOGY Department of Computer Science and Engineering Submitted in partial fulfillment of the requirement for the 8th semester Bachelor of Engineering in Computer Science and Engineering Department of Computer Science and Engineering DAYANANDA SAGAR COLLEGE OF ENGINEERING Department of Computer Science and Engineering (An Autonomous Institute affiliated to VTU, Belagavi, Approved by AICTE & ISO 9001:2008 Certified) Accredited by National Assessment & Accreditation Council (NAAC) with 'A' grade Shavige Malleshwara Hills, Kumaraswamy Layout, Bengaluru-560078 Submitted By Rohith Marath 1DS19CS132 Sachin C B 1DS19CS137 Sanjay S 1DS19CS140 Sanjeev F Annigeri 1DS19CS142 Department of Computer Science and Engineering Under the guidance of Abhinav R B Assistant Professor CSE , DSCE And Mr. Monu Singh Coguide - Industry Department of Computer Science and Engineering 2022 - 2023 Department of Computer Science and Engineering Department of Computer Science and Engineering DAYANANDA SAGAR COLLEGE OF ENGINEERING Bangalore - 560078 Department of Computer Science and Engineering

VISVESVARAYA TECHNOLOGICAL UNIVERSITY Department of Computer Science and Engineering Dayananda Sagar College of Engineering Department of Computer Science and Engineering (An Autonomous Institute affiliated to VTU, Belagavi, Approved by AICTE & ISO 9001:2008 Certified) Accredited by National Assessment & Accreditation Council (NAAC) with 'A' grade Shavige Malleshwara Hills, Kumaraswamy Layout, Bengaluru-560078 Department of Computer Science and Engineering Department of Computer Science & Engineering CERTIFICATE This is to certify that the project entitled E-STAMPING IN DIGITAL VOTING SYSTEM USING BLOCKCHAIN AND CLOUD TECHNOLOGY is a bonafide work carried out by Rohith Marath [1DS19CS132], Sachin C B [1DS19CS137], Sanjay S [1DS19CS140] and Sanjeev F Annigeri [1DS19CS142] in partial fulfillment of 8th semester, Bachelor of Engineering in Computer Science and Engineering under Visvesvaraya Technological University, Belgaum during the year 2022-23. Abhinav R B vicei Dr. Ramesh Babu D R Dr. B G Prasad (Guide) vicfi Vice Principal & HOD Principal Asst Prof. CSE, DSCE CSE, DSCE DSCE Signature:........... Signature:........... Signature:........... Name of the Examiners: Signature with date: 1........................... .... 2........................... ....

Acknowledgement

We are pleased to have successfully completed the project **E-Stamping in Digital Voting System Using BlockChain and Cloud Technology**. We thoroughly enjoyed the process of working on this project and gained a lot of knowledge doing so.

We would like to take this opportunity to express our gratitude to **Dr. B G Prasad**, Principal of DSCE, for permitting us to utilize all the necessary facilities of the institution.

We also thank our respected Vice Principal, HOD of Computer Science & Engineering, DSCE, Bangalore, **Dr. Ramesh Babu D R**, for his support and encouragement throughout the process.

We are immensely grateful to our respected and learned guide, **Abhinav R B**, Asst Professor CSE, DSCE and our co-guide **Monu Singh** for their valuable help and guidance. We are indebted to them for their invaluable guidance throughout the process and their useful inputs at all stages of the process.

We also thank all the faculty and support staff of Department of Computer Science, DSCE. Without their support over the years, this work would not have been possible.

Lastly, we would like to express our deep appreciation towards our classmates and our family for providing us with constant moral support and encouragement. They have stood by us in the most difficult of times.

Rohith Marath 1DS19CS132
Sachin C B 1DS19CS137
Sanjay S 1DS19CS140
Sanjeev F Annigeri 1DS19CS142

Abstract

Election is a process of establishing democracy in the country. It is also one of the most challenging tasks, one whose constraints are remarkably strict. Each voter should receive assurance that her vote is cast as intended, recorded as cast and tallied as recorded.Democracy and voting are pillars of modern society, but the traditional paper ballots are prone to fraud and failure,ballots can be miscounted, or ballots sent via mail might get lost in transit. The traditional voting system also carries the costs of human resources, ballot deployment, and security measures. A massive amount of money is usually spent every election in every country.We propose a e-stamping technique in Digital voting System which allows the voter to cast only one vote.Here we are implementing the Android Application for E-voting system using Block chain and Cloud Server.usage of Decentralized system eliminates the Single point failure and gives more transparency,anonymity for the voters.Hence,Ensures the Trust by the voters.Voters can cast the vote remotely from anywhere with the help of Android Device.We are using Two Stage Authentication system for the Application.i.e,Facial recognition and Fingerprint.Facial image of the Voter is stored in the database along with voter id ,fingerprint authentication of voter using Android Device.after Successful login the voter can cast vote.During each vote castes, timestamp of the vote is recorded.Usage of E-stamping will ensure that voter can only vote once for the particular election.

Table Of Contents

List of Figures

Chapter 1

Introduction

1.1 Introduction to Project

E-voting also known as Electronic voting is a concept that has evolved recently due to the explosion in internet popularity over the last three decades providing a large number of citizens access to the internet. Unlike traditional voting which involves going to a designated polling booth to cast a vote, e-voting uses electronic means to aid casting and counting of ballots. It can be implemented either through an EVM (Electronic voting machines) or by taking votes from computers on the internet which is known as Online voting. EVMs can include machines such as voting kiosks, punched cards or optical scan systems. These systems can perform a wide variety of tasks depending on the amount of automation required such as marking a paper ballot, vote recording, data encryption and consolidation and tabulation of an elections results.

An e-voting systems positives far outweigh the negatives. It solves various problems that plague the traditional systems such as voter intimidation and voter fraud by utilizing various technologies and algorithms to overcome them. It encourages more voter participation by allowing voters to cast their vote conveniently from their homes and in turn also is more environmental friendly as voters do not need to travel long distances to cast their vote. The vote results can also be counted in a more accurate, cheap and rapid manner by using automated systems instead of manually counting them by hiring workers which is more expensive. The voters who are disabled or live in a remote location reap the most benefits from such a system. But it also introduces some downsides which include being vulnerable to Cyber Attacks and a lack of transparency. Cyber Attacks can be prevented by using a more secure encryption standard such as 256-bit encryption. An e-voting system can be implemented by several methods which include Public network DRE voting system, Direct recording electronic voting system, Paper-based electronic voting system, Online voting or

1

it can be a combination of the aforementioned models leading to a Hybrid system.

1.2   Problem Statement

Current voting systems like ballot box voting or electronic voting is subject to numerous security risks such as polling booth capturing, vote alteration and manipulation, malware attacks, etc. and also require huge amounts of paperwork, human resources, Money and time. So, implementing E-stamping in a digital voting system using Block chain technology provides additional Security for Current Voting System.

1.3   Purpose and Scope

1.3.1   Purpose of Online Voting System:

- Provision of improved voting services to the voters through fast, timely and convenient voting.

- Reduction of the costs incurred by the Electoral Authority during voting time in paying the very many clerks employed for the sake of the success of the manual system.

- Check to ensure that the members who are registered are the only ones to vote.

- Online voting system will require being very precise or cost cutting to produce an effective election management system.

- Increased number of voters as individual will find it easier and more convenient to vote.

Scope of Online Voting System:

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

- Less effort and less labor intensive, as the primary cost and focus primary on creating, managing, and running a secure web voting portal.

- Increasing number of voters as individuals will find it easier and more convenient to vote, especially those abroad.

1.4   Real World Application

Online surveys are available in more places than traditional surveys. Some important uses of online voting are:

1. Political elections: Online voting can simplify the voting process for political elections by allowing citizens to vote easily from anywhere with an internet connection. This could result in a large turnout and faster announcement of election results.

2. Corporate Governance: Online voting systems can be used for corporate governance, allowing shareholders to vote electronically at annual meetings or other actions where pressure is important. It improves member engagement, simplifies the voting process and reduces administrative costs.

3. Organizations and associations: Online elections can facilitate elections in organisations, trade unions and other membership organisations. Members can participate in simple decision-making processes such as electing leaders, approving policies or accepting contracts.

4. Opinion polls: Opinion polls and polls can be conducted through online voting. This enables governments, researchers, and organizations to efficiently and cost-effectively gather opinions and measure public opinion on a variety of issues.

5. Student Voting: Universities from schools to schools can use online voting for student voting.It simplifies the voting process, encourages student participation and provides a transparent and accountable platform for the election of student representatives.

6. Elections and Elections: Online voting systems can be used to create ballot papers or voting plans on specific issues. This allows citizens to express their views directly, providing a more independent and effective process.

7. Voting for citizens abroad: Online voting allows citizens abroad to participate in elections, making their voices heard even when they are far from their home country. This promotes unity and allows integration of citizens.

8. Organizational decision making: Online voting can be used to make decisions such as board meetings, approval of rights, and project selection in an organization. It simplifies the decision-making process, facilitates remote participation, and controls the way you vote.

It is important to note that the use of online voting must take into account the specific requirements and risks associated with each application. Robust security measures, authentication mechanisms and transparency mechanisms should be in place to ensure the integrity and reliability of the voting process on all matters.

Chapter 2

Proposed Solution

2.1 Challenges in the Existing System

- The existing system does not provide combination of face detection and biometric to identify person. Our System Achieve this with the help of Image Processing and Use of finger print recognition.

- High In cost, as traditional system of voting is very high in cost, because there is need to setup voting booth at every place and cost of machines is also increase whole cost.

- Time Consuming, as traditional system of voting takes lot of time to complete whole process of voting, there are lots of plans are prepare to conduct voting which is time consuming process also in setting up voting booth and categories the regions and also rest process after voting that is counting vote is also time consuming.

2.2 Objectives of Proposed Solution

Our goal is to use blockchain technology to address the problems associated with electronic voting. Blockchain-enabled electronic voting may lower voter fraud and broaden voter participation.

Using a Blockchain, the most important requirements are satisfied:

- Authentication: Only registered voters will be allowed to vote

- Anonymity: The system prevents any interaction between the votes casted by the voters and their identities.

- Accuracy: Votes once cast are permanently recorded and cannot be modified or changed under any circumstances.

- Verifiability: The system will be verifiable such that the number of votes is accounted for.

4

2.3   Data Flow Diagram(User Module)
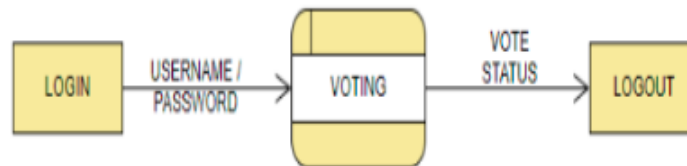
Figure 2.1: Overview of the Model

A data flow diagram is a graphical representation that depicts information flow and the transforms that are applied as data move from input to output. The basic form of a data flow diagram, also known as a data flow graph or a bubble chart. Data flow diagram is an abstract description of the system. The data flow diagram may be used to represent a system or software at any level of abstraction. Data flow diagrams may be partitioned into levels that represent increasing information flow and functional detail. Therefore, the Data flow diagram provides a mechanism for functional modeling as well as information flow modeling.The above shown diagram describes about the detailed view on the application process.It mainly shows User side architecture,where the user will login using username and password. After a successful login and verification user will vote for candidate from candidate list and logout.

The above diagram shows the user module. First user has to create a account with details like Name,phone number and Password.After creating a account user can login with phone number and password. after a Successful login, user will be directed to Home page which shows Vote button mentioned with Click here to vote now.After that it will ask for the Fingerprint Authentication. we have added the fingerprint registered with the Android Device.After a Successful authentication ,user will be asked to enter a ID for voting process. Once he enters the details here,it will be directed to Facial recognition system. Here we capturing the image of the voter like who is voting in the election process. after capturing the face, user will be directed Voting page where candidate or party name is mentioned. user will vote to single candidate and after a successful vote , user will be logged out from application.
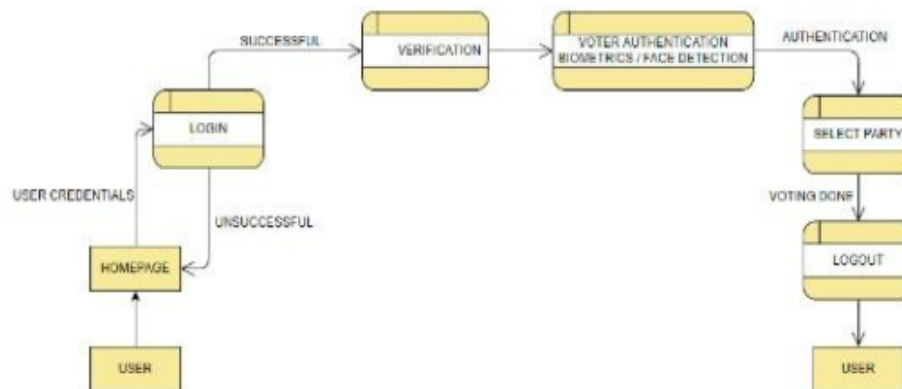
Figure 2.2: Data Flow of the Model

2.4   ER Diagram(Admin Module)

An entity–relationship model (ER model) describes interrelated things of interest in a specific domain of knowledge. A basic ER model is composed of entity types (which classify the things of interest) and specifies relationships that can exist between instances of those entity types. In software engineering, an ER model is commonly formed to represent things that a business needs to remember in order to perform business processes. Consequently,The ER model is transformed into an abstract data model that specifies a data or information structure that can be used in a database, most frequently a relational database.

Entity–relationship modeling was developed for database design by Peter Chen and published in a 1976 paper. However, variants of the idea existed previously. Some ER models show super and sub-type entities connected by generalization-specialization relationships, and an ER model can be used also in the specification of domain-specific applications.

We used Firebase as the underlying technological stack for our e-voting system. The Realtime Database supports the system's admin module and gives administrators access to crucial features. Administrators can add new users within this module, logging their phone numbers, constituencies, and district names. Along with candidates, a helpdesk with a helpline number and helpline email, registration locations, and voter information, the module also has a polling division feature. Important voter information, such as names, passwords, village IDs, and voting preferences (expressed as "yes" or "no") are efficiently stored in the Realtime Database.The figure describes the Overall process managed by Ad-

mins.
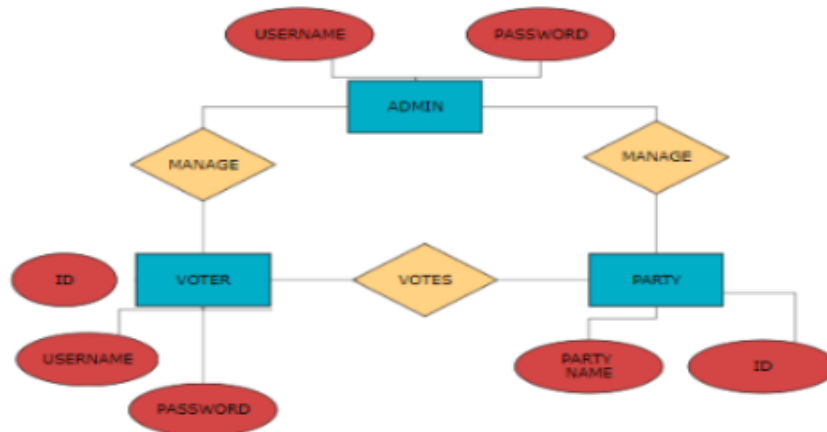
Figure 2.3: Admin Module

- Create Voting Candidate and Voters: The voter's name, voter date and other information is first entered in the application. After the successful registration, the voters sign in into the application. Then the photo of the voters is taken and then sends it to the centralized database. Voter's list will be uploaded using excel sheet to the database to create credential to the voting system.

- Election Candidate: Admin will update the candidate details with voter id, date and ward of election going to participate.

- Allocate Voting Data with candidate: Provides the detailed information about the Voting, such as Voting name, voting date, and Voting department and Voting disc.

- Here Admin can manage both candidate or party list in the elections and list of voters for a particular election.

Chapter 3

Literature Survey

Ramya Govindaraj et.al worked to implement an online voting system using Microsoft SQL Server 2012 and Microsoft Azure as a cloud. The main reason for this shift from manual voting system to digital voting system is that people can consume their time and vote from anywhere through online. The system has no need of ballot papers and all authorized and eligible persons can register through online and vote by logging into their own systems.The most important details in this text are that India currently uses a manual race framework, which causes issues due to the paper tally based race framework. An online framework, which includes strategies like enlistment of voters, vote throwing, vote checking, and pronouncing results, would be a decent answer for supplanting the current framework .The proposed framework will reduce the risk of defilment by using NADRA's online database and Computerized National Identity Cards (CNIC) to enlist all voters of the age 18 or above and check and verify their information.

Ali Kaan Koç et.al had proposed how blockchain is a powerful tool for digitizing everyday services, such as administrative operations, fintech procedures, and everyday services that can only be done offline and/or in person. Smart contracts are meaningful pieces of codes, to be integrated in the blockchain and executed as scheduled in every step of blockchain updates . Blockchain with the smart contracts is a good candidate to use in developments of safer, cheaper, more secure, more transparent, and easier-to-use e-voting systems. This work has implemented and tested a sample e-voting application as a smart contract for the Ethereum network using the Ethereum wallets and the Solidity language. Android platform is also considered to allow voting for people who do not have an Ethereum wallet. This project aims to provide a secure voting environment and show that a reliable e-voting scheme is possible using blockchain.

Purandare et.al described voting is an important aspect for democratic countries, but the existing voting system has flaws such as time consuming process and lack of security. To improve the existing voting system they proposed, an online voting system using Android devices has been designed to provide better security, less time consuming process, and better results. Voters can cast their vote remotely from anywhere in the country with the help of an Android device and voting application on their device.Android applications are compatible with almost all Android devices and have two stage authentication techniques: facial recognition and One Time Password (OTP). Results of the election will be displayed on individual voter's device in terms of notification and voter will get updates about the election to enhance the system performance.

The proposed system will use instant messaging service to obtain OTP after image authentication, which relies on the user's ability to recognize pre-chosen pictures. The proposed system will mainly target the urban population to overcome these flaws. AOVSAD is a project of internet voting with facial recognition and one time password to overcome the drawbacks of conventional voting systems. It consists of an Android application with voter ID and camera for face detection and recognition. Data of voters is stored in a database, images of faces are stored with various angles, and voter IDs are stored in a local server. This proposed system uses XAMPP server which is not real time server. To improve performance of system some real time server may be used. One of such platform is AmazonWeb Services (AWS).

Ullah et.al proposed a mobile phone voting protocol based on hybrid cryptosystem. There are three stages to it: online registration, voting, vote counting, and outcome phase. The suggested protocol allows for efficient and safe online voting and can be used in conjunction with the current system of paper ballot voting. Due to its emphasis on SMS messaging and lack of dependence on internet connectivity, it is effective, secure, and deployable in poor countries.The planned e-voting system is intended to get rid of security risks such vote buying and coercion, online registration, ballot confidentiality, voter anonymity, and double voting. It makes use of a mobile phone that is compact, economical, and powered by the Global System for Mobile Communication (GSM) standard.There are four main characteristics of the proposed Mobile Phone Voting System (MPVS): eligibility, distinctiveness, accuracy, integrity, fairness, confidentiality, and cost-effectiveness.

The system consists of four parts: mobile phone, authentication server, verification server, and counting server. Three stages make up the proposed system: pre-voting, voting, and post-voting. By adopting a blind signing mechanism, voter confidentiality is protected. In this paper, a hybrid cryptosystem-based mobile phone voting system (MPVS) with an online mobile voting registration phase is proposed. The system prevents voting twice if a ballot is cast first from a mobile device and then from a polling place. The proposed solution is more dependable and efficient because information would be sent to the election commission server via secure SMS. Because our solution didn't require the internet or any specialised gear, the cost was lower.

Adiputra et.al proposes a blockchain-based electronic voting system to improve the Estonian electronic voting system's universal verifiability issues. A blockchain is a distributed database, where the complete data is shared among all participants in the network. We need a voting system that does not allow third-party to easily disturb or dismiss a legal referendum or election. By utilizing the strengths of blockchain that distributes trust to participant in its network, we can improve the availability of a voting system without relying on third-party interference.

They proposed system is a centralized e-voting system with dedicated servers in one data center, but has not allowed the public to verify it. Vulnerabilities, such as state-level attackers, have been identified in the Estonian e-voting system, which is a centralized e-voting system with dedicated servers in one data center.Our proposed system still has wide room for improvements as described. Also, it needs time to popularize blockchain for a voting system as it is a novel idea and voting itself is a crucial matter in a democratic country. However, we believe improvements in future e-voting systems will provide a better solution to the current issues.

Kanika Garg et.al discusses the challenges in the centralized voting system and explores the potential of blockchain technology to address these challenges. The authors highlight the importance of voting in a democratic country like India and the need for a more secure and reliable voting system.The paper begins with an introduction to the problems of trust, autonomy, and intermediaries in current systems, emphasizing the potential of blockchain as a decentralized and trustable solution. The authors explain that blockchain, being a read and write only database, can offer security and immutability to build a decentralized voting platform.

The authors then discuss various challenges faced in the voting process, including privacy, lack of evidence, fraud-resistance, ease-of-use, scalability, speed, and low cost. They emphasize the importance of addressing these challenges to create a more efficient and inclusive voting system.The paper proceeds with a literature review, where the authors analyze different research papers and methodologies related to e-voting. They discuss various approaches such as e-voting with IoT and fingerprint, e-voting with blockchain and Aadhar verification, and more. The review provides insights into different techniques used to make voting systems more robust and secure. In the conclusion, the authors highlight the importance of user authentication and the role of blockchain-based solutions in enhancing the security and transparency of voting systems. They acknowledge the ongoing debate surrounding e-voting and emphasize the need for strong foundations and mutual understanding to prevent misuse.

Rabeya Bosri et.al proposed a secure electronic voting system using blockchain technology. The writers discuss the voting process's impartiality, independence, transparency, and security. Traditional paper-based voting systems are vulnerable to a number of security problems, including ballot paper theft, booth capture, and uneven counting. Electronic voting machines (EVMs) have contributed to some of the solutions to these issues, although security issues such vote tampering and manipulation still exist. The authors suggest incorporating blockchain technology into the voting mechanism to address these issues. The benefits of blockchain include data integrity, voter anonymity, privacy, and security. Each voter receives their own Ethereum account thanks to the system's use of the Ethereum blockchain network. Voters can cast their ballots at a designated voting location or using a smartphone.

Voters verify themselves as part of the two-step verification process included in the proposed system, and the votes of election candidates are confirmed by a group of consensus observers. The votes may be rejected if any anomalies are found. This guarantees the confidentiality and safety of the voting process. The authors emphasise the shortcomings of current strategies and examine relevant efforts in the area of blockchain-based voting systems. They outline the architecture and layout of their suggested system, putting special emphasis on how blockchain technology will create a safe and transparent voting environment. Overall, the paper aims to enhance the electronic voting systems' confidentiality and security by leveraging blockchain technology. It proposes a novel approach to address the challenges associated with traditional and electronic voting methods.

Zhao Yuehua et.al discusses a voting algorithm designed to improve the accuracy and output of voting systems, particularly in intrusion-tolerant systems. The algorithm is based on testing information and historical record values. It aims to immediately extract runtime error messages from the memory and arithmetic logic unit, combining them with the historical record values of copy-computers to improve voting accuracy. The paper identifies shortcomings in the commonly used Large Number Voting strategy, such as high failure rates and inflexible voting parameters. It then presents an improved algorithm that addresses these shortcomings. The algorithm calculates the voting contribution value for each copy, divides the voting results, and selects the set with the largest collection as the voting set. The final voting output is determined based on the prior contribution values and the response results of the copies.

To further enhance the algorithm, the paper introduces detection codes to extract service running information during the voting process. This information becomes the basis for copy response results. The algorithm considers both the detection information and the recently history records of copies in each round of voting to determine the voting output. It also incorporates a threshold to judge the consistency between copies' input values. The experimental results compare the performance of the improved algorithm with the Majority Voting algorithm based on copy reliable weight. The experiments are conducted in an intrusion-tolerant system environment using multiple servers. The results show that the improved algorithm outperforms the Majority Voting algorithm in terms of successful voting numbers, even in the presence of errors.

The research paper highlights the importance of intrusion-tolerant systems and the role of voting algorithms in ensuring system integrity and continuous service. The proposed algorithm offers a more accurate and reliable approach to voting, considering both real-time faults and historical records. It provides insights into improving voting systems' performance and is suitable for intrusion-tolerant systems.

Menon et.al proposes the use of ID-based signature schemes for electronic voting systems. The authors suggest the use of two ID-based signature schemes to ensure the security, anonymity, and verifiability of votes. The paper describes a designated verifier ring signature scheme, which ensures the security and anonymity of votes. In this scheme, a group of voters (e.g., board members or shareholders) each signs their vote and designates the Voting Authority as the verifier. The Voting Authority can verify the votes' authenticity

without knowing the exact person who voted, thus maintaining anonymity. To allow voters to check if their votes have been taken into account, the paper proposes an ID-based designated verifier signature scheme for generating receipts. The Receipt Generator, using an ID-based scheme, provides a receipt to the voter, which proves that their vote has been recorded without revealing the actual vote to a third party.

The paper provides a detailed explanation of the proposed ID-based signature schemes and discusses their security properties. It also mentions related work in the field of electronic voting systems and ID-based signatures. Overall, the paper presents a novel approach to address the challenges in electronic voting systems using ID-based signature schemes. It provides a secure and anonymous voting scheme while allowing voters to verify the correctness of their votes through receipts.

Roopak et.al discusses the use of blockchain technology in an electronic voting system that is based on the Virtual ID (VID) of Aadhaar, an identification system used in India. The goal is to ensure the security and integrity of the voting process and prevent tampering with votes. The proposed system involves the integration of Aadhaar's VID, which is a unique identifier, with the e-voting system. During the registration process, users provide their VID, and the system retrieves their demographic details, including fingerprint data, from the Aadhaar database. The fingerprint is then processed and converted into a digital signature to ensure the integrity of the vote. The voting process involves users casting their votes online using their VID and scanning their fingerprint for authentication. The vote is encrypted using asymmetric encryption, where the election commission's public key is used for encryption and their private key is used for decryption. The encrypted vote is stored in a block in the blockchain.

The blockchain ensures the security and integrity of the votes by using hashing techniques. Each block in the blockchain contains data, the hash of the block, and the hash of the previous block. The properties of the proposed blockchain e-voting system using VID are discussed. The system provides authentication, availability, public verifiability, and integrity. The SHA-256 algorithm is mentioned as one of the hashing algorithms used to ensure integrity. In conclusion, the paper suggests that integrating blockchain technology with Aadhaar's VID can provide a secure and tamper-proof electronic voting system. The use of fingerprint data, digital signatures, and hashing techniques enhances the security and integrity of the votes. However, it's important to note that the implementation and effectiveness of such a system would depend on various factors, including the robustness

of the underlying technology and the regulatory framework.

Evgeniy V. Palekha et.al proposed the architecture of web applications, specifically focusing on their application in secure voting systems. The main idea put forth is to utilize the Hierarchical Model-View-Controller (HMVC) modification, which offers several advantages in terms of the structure, maintainability, and security of web applications. By incorporating the HMVC approach, the author aims to improve the overall design and functionality of web applications utilized in the voting process. This modification allows for a more organized and modular development approach, where the application components are divided into separate layers: the model, responsible for providing data and responding to controller commands; the view, responsible for presenting data to users and reacting to changes in the model; and the controller, acting as the link between the model and view, facilitating user interactions and notifying the model accordingly.

In addition to the HMVC modification, the proposal suggests the implementation of digital signatures to ensure the integrity and authenticity of voting results. Digital signatures serve as a means of verifying that the selected candidate by each voter remains unchanged and untampered with. By applying digital signatures, the author intends to provide an additional layer of security, preventing any potential compromise of the electronic voting system and instilling trust in the accuracy of the results. The proposed enhancements to web application architecture aim to create a more robust and reliable platform for conducting secure elections. By leveraging the benefits of HMVC and incorporating mechanisms such as digital signatures, the author seeks to enhance the transparency, integrity, and trustworthiness of the voting process in electronic systems.

Mrs.Harsha V. Patil et.al discussing the issues present in the current election voting systems worldwide and proposing the use of electronic voting (e-voting) models based on blockchain technology to address these problems. They highlight that trust in the election system is a major concern in modern democracies, even in countries like India, the United States, and Japan. The major issues in the current voting system include vote rigging, hacking of electronic voting machines (EVMs), election manipulation, and polling booth capturing. The paper aims to investigate the problems in the current voting systems and proposes the use of blockchain technology to create distributed electronic voting systems. It explores the application of blockchain as a service and discusses popular blockchain frameworks that offer solutions for electronic voting systems. The proposed system based

on blockchain technology addresses the limitations of traditional voting systems while preserving participants' anonymity and allowing public inspection.

While existing research explores how blockchain can improve e-voting schemes and meet the listed requirements, the author points out that these papers often overlook the implementation challenges and limitations of blockchain technology in large-scale voting schemes. Therefore, this paper aims to explore both the possibilities and challenges of implementing e-voting schemes using blockchain technology. The author discusses the limitations of traditional e-voting systems, such as secure digital identity management, anonymous vote-casting, individualized ballot processes, ballot casting verifiability by the voter, high initial setup costs, increasing security problems, lack of transparency and trust, and voting delays or inefficiencies related to remote/absentee voting. They argue that blockchain technology can address many of these issues and make e-voting cheaper, easier, and more secure to implement. They explain the basic concepts of blockchain, its decentralized nature, and its immutability, which make it suitable for e-voting systems. The author conveys the importance of addressing the trust and security issues in current voting systems by adopting e-voting models based on blockchain technology.

Supeno Djanali et.al presented a comprehensive and secure e-voting system that maintains voter privacy and guarantees the accuracy and integrity of the voting process. The proposed system aims to address the shortcomings of traditional paper-based voting methods and provide a robust electronic alternative. To achieve this, the author introduces a sophisticated cryptographic framework that combines several techniques to ensure the confidentiality, authenticity, and verifiability of voting data. The system utilizes cryptographic hash functions like SHA256 to securely store and retrieve sensitive information. Digital signatures are employed to authenticate the identity of voters and prevent tampering with their votes. Additionally, the system employs RSA asymmetric encryption, which involves the use of public and private keys, to protect the transmission of voting data across various levels of the voting hierarchy. Each level, including voting places, districts, cities, states, and the country, follows a similar process to verify and count the votes. The focus of the paper is primarily on the district level, as it represents a fundamental unit of the voting system. They acknowledge the significance of prior research in the field of e-voting and highlights the key areas of concern, such as data encryption, voter privacy protection, and ensuring the verifiability of the vote counts. Several existing methods are discussed in relation to these concerns, emphasizing the importance of secure database design to uphold

privacy and maintain data integrity.

In conclusion, the author argues that their proposed e-voting system effectively addresses the security issues associated with electronic voting. By leveraging cryptographic techniques and following a multi-level verification process, the system offers enhanced privacy protection for voters while ensuring the accuracy and trustworthiness of the voting results. The paper presents the proposed system as a potential replacement for traditional voting methods, offering a more efficient, secure, and transparent approach to democratic processes.

Irina Dyachkova et.al primary goal is to address the shortcomings of traditional voting methods, which heavily rely on the human factor and are susceptible to manipulation. By leveraging cryptographic protocols, the author argues that it is possible to create a secure and reliable digital voting system. The paper provides an overview of the specific cryptographic protocol implemented in a real-world voting system developed at the Institute of Computational Technologies SB RAS. This protocol employs a "blind" signature algorithm, originally introduced by David Chaum in 1982, which allows participants to generate and sign voting ballots without disclosing their choices to the server. The algorithm is based on the RSA protocol but can be adapted to other digital signature algorithms as well. The step-by-step process of the algorithm is outlined, emphasizing the generation of secret and open parameters, the creation of data for signature, and the signing process itself. In addition to the blind signature algorithm, the paper also explores the establishment of an anonymous data transfer channel to ensure the privacy and security of the voting process. Various approaches are mentioned, including decentralized anonymous networks, hybrid networks, TOR, and VPN. By incorporating a random selection of participants and the server as potential recipients of the ballots, the protocol enhances the difficulty of determining the origin of each ballot.

The author suggests that by recording voting transactions as blocks in a blockchain, the system can ensure the integrity of the data and prevent tampering. The openness of the blockchain database allows participants to verify the correctness of their votes and confirm the total number of voters, thus promoting transparency and accountability. They aim to demonstrate the feasibility and advantages of an anonymous digital voting system backed by cryptographic protocols. The paper provides insights into the specific protocol utilized in a real-world voting system and highlights the benefits of incorporating an anonymous data transfer channel and blockchain technology.

Ashish Singh et.al is presenting a research paper that focuses on the implementation of blockchain technology in digital e-voting systems to address security issues and fulfill system requirements. The paper emphasizes the shift from paper-based voting systems to digital systems and highlights the advantages of digital e-voting, such as transparency, decentralization, irreversibility, and non-repudiation. The abstract also references previous research on electronic voting systems that have utilized blockchain technology, highlighting the limitations and vulnerabilities of some existing solutions. Examples of electronic voting systems from Estonia, Norway, and Scytl are mentioned, pointing out issues such as transparency, cyber attacks, and compromised confidentiality.

The proposed electronic voting system is specifically designed for university elections and aims to provide a secure and robust solution. The abstract mentions the participants in the system, including voters, election organizers, and inspectors. It outlines the framework of the digital voting system, which involves voter registration, authentication, candidate selection, encryption, signing, and the generation of blockchain blocks. The security analysis of the proposed system includes considerations such as privacy of data transmission, voter confidentiality, prevention of duplication and forgery, and protection against system-level threats and attacks. The abstract asserts that the proposed system addresses these security concerns through the use of encryption, hashing, and other security measures. The papers main objective is to introduce a secure and decentralized electronic voting system using blockchain technology, specifically targeting university elections. The abstract highlights the advantages of the proposed system and suggests that it offers improved security compared to existing solutions.

3.1   Case Study : Estonia's e-Election System

Estonia's e-Election System is widely recognized as one of the most advanced and successful implementations of online voting. It has been in operation since 2005 and has been used in various parliamentary, local, and European Parliament elections in Estonia.

Overview of Estonia's Online voting System:

- Digital Identity : The sophisticated digital identity infrastructure of Estonia forms the basis of the nation's e-Election System. Electronic ID cards with secure digital certificates are given to Estonian people, enabling them to securely verify themselves and access a range of e-services, including online voting.

- Secure Authentication: The e-Election System employs advanced authentication techniques to guarantee the accuracy and legitimacy of votes. When accessing the online voting platform, citizens must authenticate themselves using their electronic ID cards, PIN codes, or mobile ID.

- Cryptographic Protocols: To guarantee voting privacy, accuracy, and transparency, Estonia's online voting system uses cryptographic protocols. Votes are digitally signed and encrypted to prevent tampering and unauthorised access. Voters can use cryptographic proofs to confirm that their vote was counted without disclosing the particular vote they placed.

- Multiple Voting Channels: The e-Election System offers multiple voting channels to cater to different voter preferences. Voters can choose to vote electronically using their computers or through polling stations equipped with special voting devices. This allows citizens to select the most convenient method while maintaining the security and integrity of the voting process.

- Independent Verification: To increase trust and transparency, Estonia's e-Election System allows independent observers, including political parties and non-governmental organizations, to participate in the verification process. They have access to the cryptographic proofs and can verify the accuracy of the counting and tabulation of votes.

- Continuous Development and Auditing: Internal and external security assessments of Estonia's e-Election System are conducted on a regular basis to look for weaknesses and make sure it is still reliable and safe. Based on comments and audits, the system has undergone numerous revisions and enhancements.

- Public Trust and Acceptance: Estonia's strong e-governance culture and high levels of digital literacy among its citizens can be partly credited for the success of the country's e-Election System. Through open communication, educational initiatives, and ongoing system development, the public has grown to trust and accept digital services, including online voting.

For other nations wishing to build safe and dependable online voting systems, Estonia's e-Election System serves as a model. Despite its success, it's important to note that the system is not without its problems, and ongoing watchfulness is needed to handle potential security issues, uphold public confidence, and guarantee the fairness of the democratic process.

3.2   Case Study : Swiss Post's e-voting System

Swiss Post's e-voting system is another notable example of an online voting system. Developed by Swiss Post, the national postal service of Switzerland, the system aims to provide a secure and accessible means for citizens to cast their votes. Here's an overview of Swiss Post's e-voting system:

- End-to-End Encryption: To protect the privacy and accuracy of votes, the e-voting system uses end-to-end encryption. Each vote is encrypted on the voter's device before being transferred, and only authorised election authorities are able to decrypt the votes throughout the counting process.

- Verifiability and Transparency: wiss Post's e-voting system focuses on providing verifiability and transparency to maintain trust in the voting process. Cryptographic proofs and digital signatures enable voters and independent observers to verify that their votes have been correctly recorded and counted without compromising the privacy of individual votes.

- Pilot Programs and Security Assessments: To find weaknesses and ensure the system's robustness, the system has undergone comprehensive pilot programmes and security audits. In order to address potential threats and enhance the system's overall security, these assessments involve external security specialists who carefully examine the system's code, architecture, and implementation.

- Multi-Level Authentication: The multi-level authentication used by Swiss Post's e-voting system ensures voter identity and prevents unauthorised access. Using their

Swiss Post user accounts, which are connected to their SwissID digital identity credentials, voters must verify their identity. For added protection, one-time passwords (OTPs) or mobile ID can be utilised as additional forms of authentication.

- Voter Privacy and Anonymity: By keeping voter identity separate from the ballots themselves, the electronic voting system preserves voter privacy and anonymity. Voters' identities are separated from their ballots, which prevents the association of votes with particular people.

- Public Confidence and Scrutiny:Public trust and openness are highly valued in Swiss Post's electronic voting system. The system is subject to intense inspection from stakeholders, political parties, and independent organisations to make sure it complies with legal requirements, fulfils high security and privacy standards, and both.

The e-voting platform provided by Swiss Post demonstrates Switzerland's dedication to safe and reliable online voting. Although there have been arguments and questions about the system's security and transparency, it shows the nation's commitment to looking into further digital voting options and using technology to boost civic engagement. Ongoing evaluations, audits, and public discussions help to maintain the integrity of the democratic process while also ensuring that the e-voting technology meets the expectations of voters.

Chapter 4

Implementation

4.1 Front-End(XML)

A Extensible Markup Language (XML) establishes a set of guidelines for encoding documents in a way that is both machine- and human-readable.The simplicity, generality, and Internet-wide usability of XML are its design focuses.It is a textual data format with robust support for many human languages thanks to Unicode.XML was created with documents in mind, but it is also frequently used to represent other types of data structures, including those used in online services.

1. XML stands for extensible Markup Language.

2. XML is a markup language like HTML.

3. XML is designed to store and transport data.

4. XML is designed to be self-descriptive.

4.1.1 UI Designs:

We have used Android Studio Platform for Developing Voting Application.We used XML for User Interface Designs in Android Studio. XML offers a structured and intuitive approach to designing user interfaces, allowing developers to define the layout and appearance of their app screens. With XML, developers can easily arrange elements such as buttons, text views, images, and more, in a hierarchical manner. XML's flexibility enables precise control over various UI qualities including size, placement, colour, and fashion. Additionally, XML promotes code re-usability by enabling the creation of reusable UI components through layout inflation and view binding. Android Studio's XML editor provides a visual preview of the UI, facilitating efficient design iterations and ensuring a seamless user experience.
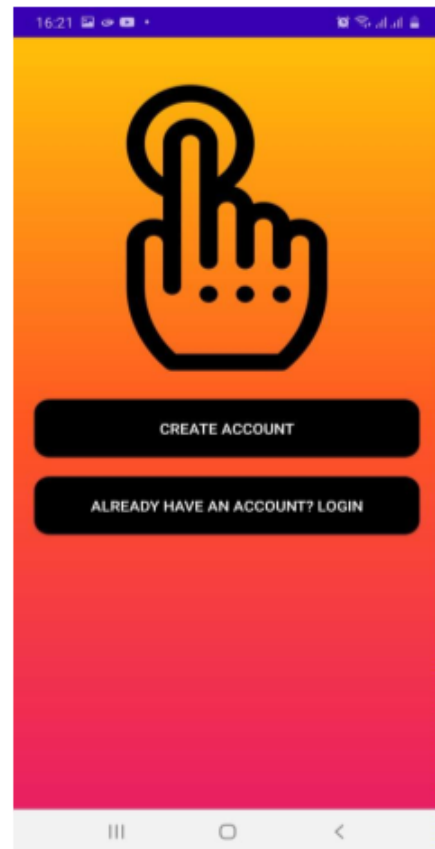
Figure 4.1: Application Screen

Figure 4.2: Login Screen
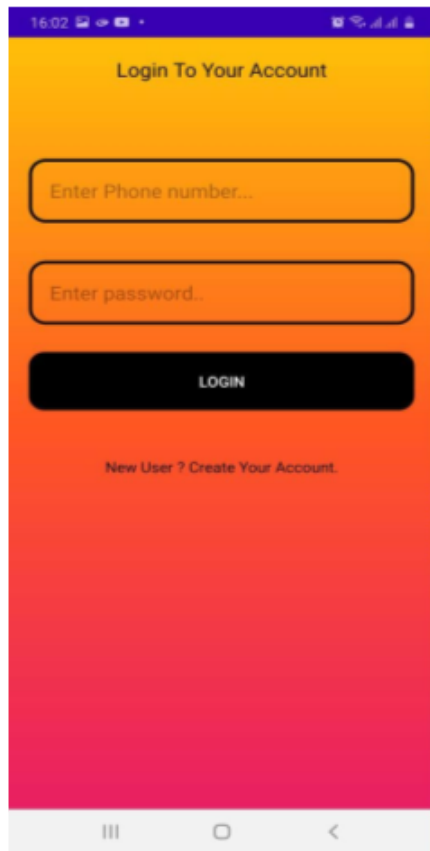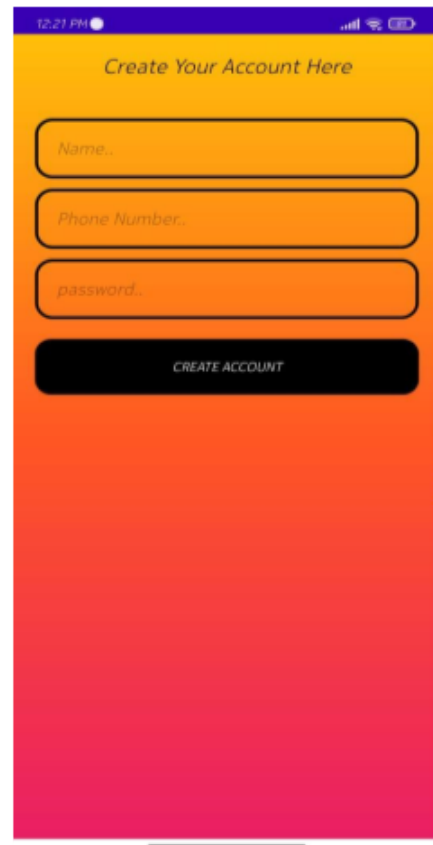
Figure 4.3: Login Page
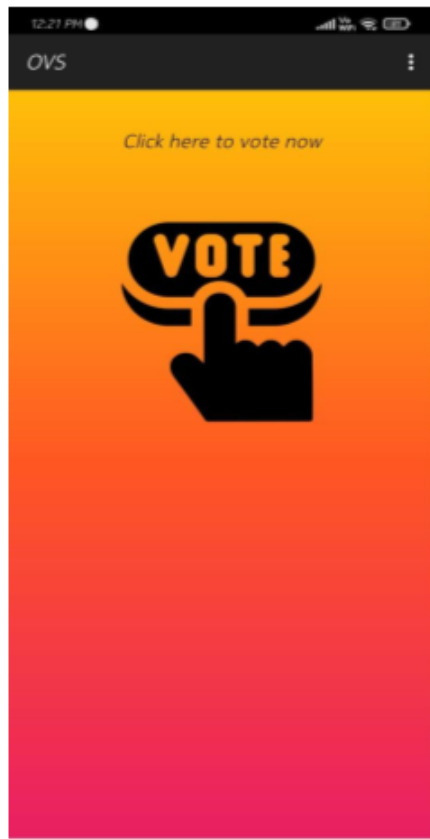
Figure 4.4: Registration Page
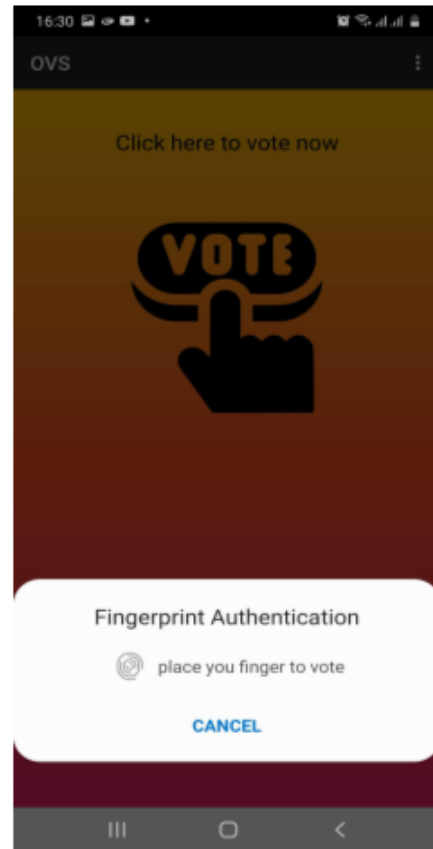
Figure 4.5: User Home Page
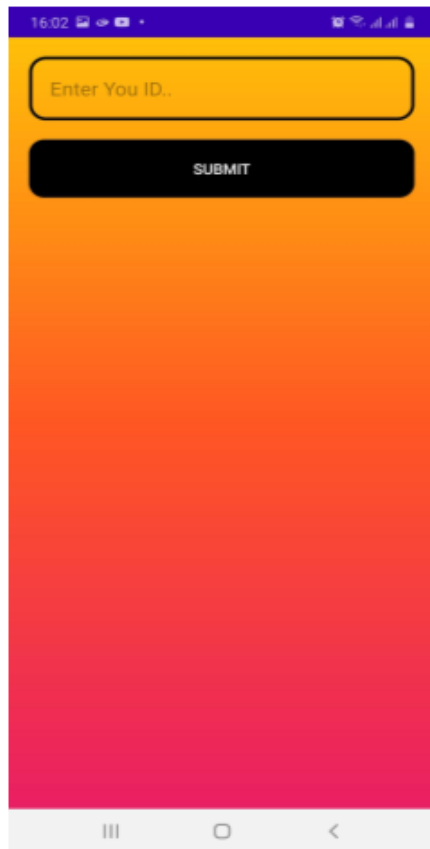

Figure 4.6: Fingerprint Authentication

Figure 4.7: User Id Screen
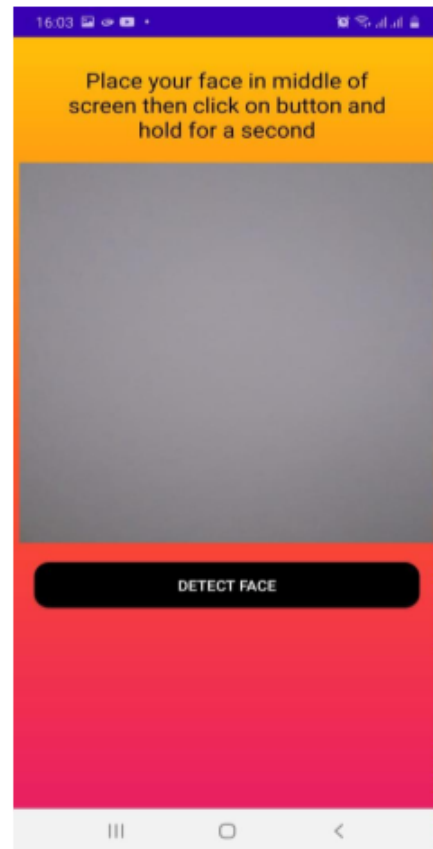
Figure 4.8: Face Detection
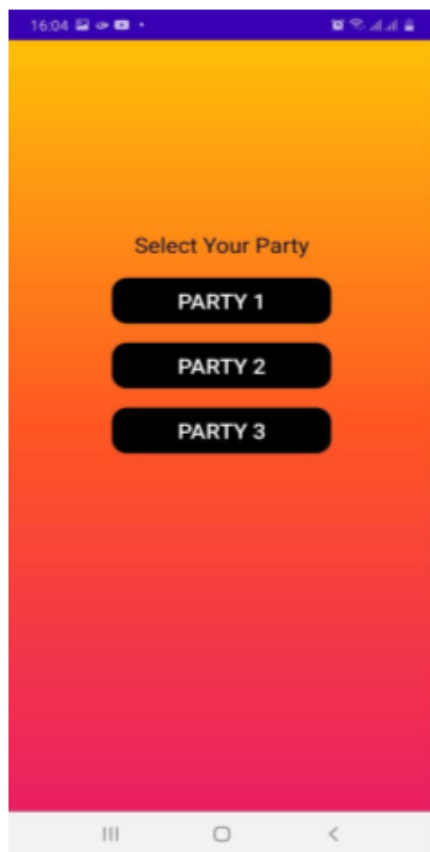
Figure 4.9: Voting Page
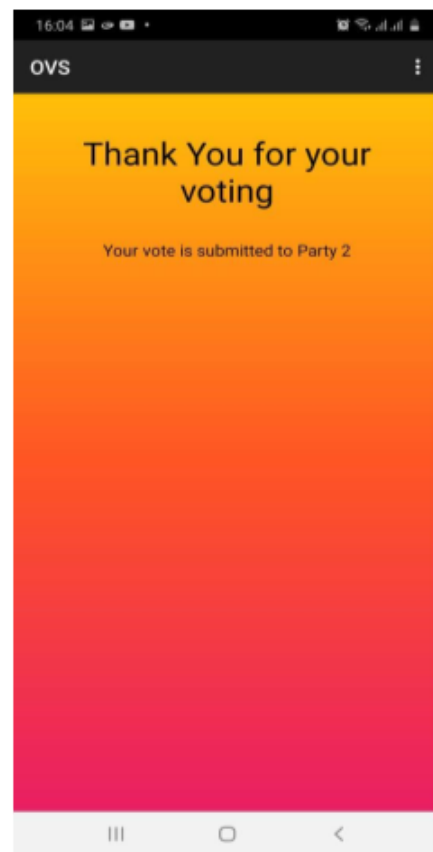
Figure 4.10: Vote Confirmation

4.2   Back-End

4.2.1   Firebase

Figure 4.11: Firebase Realtime monitor

Firebase, developed by Google, is a powerful platform for mobile and web app development. It provides a suite of tools and services that simplify the creation and management of applications.

Key features include a real-time database that enables synchronized data updates, authentication services for secure user management, cloud storage for storing and serving files, hosting for deploying web apps with ease, and additional tools for serverless computing, performance monitoring, and testing. With Firebase, developers can accelerate their development process and build robust, scalable, and user-friendly applications. The window shown above displays the analytics of the database in realtime to monitor the data usage of the e-voting system.

Firebase Authentication provides a secure and straightforward way to authenticate users. It supports various authentication methods like email and password, phone number, Google, Facebook, etc. we can make sure that only authenticated users can take part in the voting process by integrating Firebase Authentication into your voting system.

4.2.2   Firebase Real-time Database

Figure 4.12: Firebase Real-time Database

Firebase's real-time database is a cloud-based No-SQL database that offers real-time synchronization capabilities. It allows developers to store and retrieve data in a structured JSON format. The database automatically synchronizes changes across all connected devices in real-time, e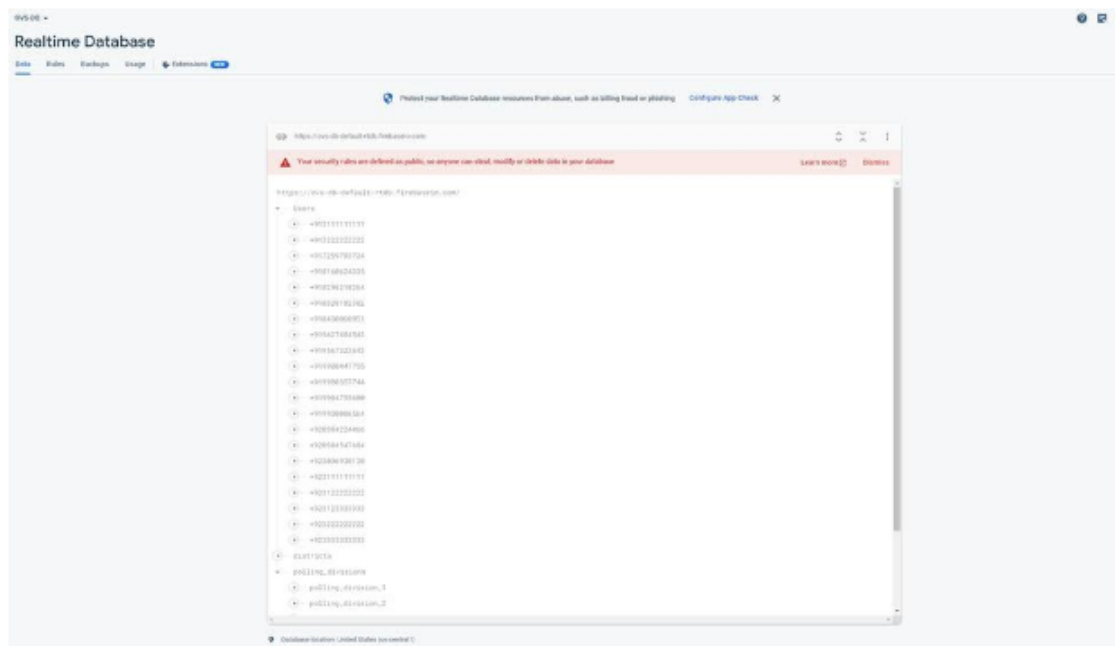nsuring that data is consistently up to date. This feature is particularly useful for building applications that require real-time updates, such as chat apps, collaborative tools, or live data streaming.

Developers can easily listen for changes in the database and update the user interface accordingly, providing a seamless and responsive user experience. For this purpose we have implemented it in our e-voting system to utilize the real time update system to ensure that any votes are immediately synced with the database and prevent any data loss from delays. It contains the following fields, Users, District and polling division.

In a voting system, the Realtime Database to store information such as candidates, vote counts, and user votes. As users cast their votes, the database can be updated in real-time, and the changes will be immediately reflected to all connected clients.
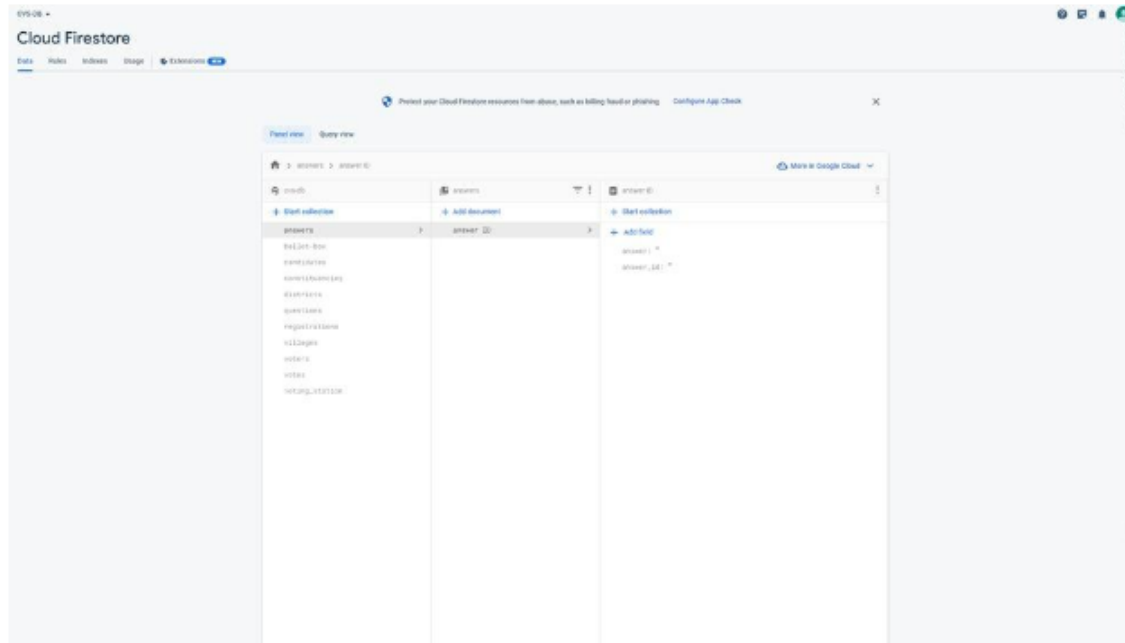
4.2.3 Cloud Firestore

Figure 4.13: Cloud Firestore

We have also utilized Firestore. Firestore is a serverless cloud database provided by Firebase for mobile and web applications. It is a NoSQL document database that offers real-time synchronization, allowing data changes to be instantly propagated to all connected clients. With Firestore, developers can organize data into collections and documents, and perform powerful queries based on various criteria.

Cloud Firestore automatically scales to handle large amounts of data and high traffic, making it suitable for applications with growing user bases. Firestore integrates seamlessly with other Firebase services and provides client SDKs for easy integration into different platforms. Overall, Firestore simplifies data management and enables developers to build scalable and responsive applications. Hence we have used it in our e-voting system for scalability and ensure fast responsiveness in our system in response to queries.

Firestore is database option provided by Firebase. It is a flexible, scalable, and document-oriented database that offers advanced querying capabilities. Firestore can be used to store more complex data structures related to a voting system, such as user profiles, candidate information, and voting history. Additionally, it offers real-time updates to make sure all customers have access to the most recent information.

4.2.4   Firebase ML-Kit

Firebase ML Kit was introduced to us at Google I/O '18. It is a mobile SDK that enables Android and iOS app developers to have advanced machine learning capabilities into their apps with ease.ML Kit APIs works both on the device and on the cloud. The on-device APIs are designed to work fast with no internet connection.

For typical mobile use cases, such as text recognition, face detection, landmark recognition, barcode scanning, image labelling, and text language identification, ML Kit includes a set of ready-to-use APIs. You can get the data you need by simply passing data to the ML Kit library.

Firebase ML Kit can be used in an Android voting app to enhance its functionality and provide machine learning capabilities. Firebase ML Kit can be integrated into an Android voting app for many purposes like:

1. Image Labeling: You can utilize the Image Labeling API to automatically label candidate images based on their content.

2. Text Recognition: The Text Recognition API can be employed to extract text from documents, such as voter identification cards or registration forms. This can automate the process of entering voter information, ensuring accuracy and saving time.

3. Face Detection: Face Detection can enhance the user experience by allowing users to capture their vote using a selfie. The Face Detection API can verify the presence of a face in the image to ensure the vote is cast by an actual person and not a photo.

4. Barcode Scanning: If the voting system employs physical voter IDs with barcodes, you can utilize the Barcode Scanning API to quickly scan and verify voter IDs.

5. Custom Models: Firebase ML Kit's custom model support allows us to train and deploy our models if you have particular needs or are implementing bespoke machine learning models. For instance, you could develop a model to identify patterns in fraudulent voting or analyse sentiment from social media data to determine the general consensus.

6. Language Identification: If voting app supports multiple languages, the Language Identification API can help determine the language of user inputs, such as comments or feedback. This can facilitate efficient language-based analysis and response handling.

By integrating these ML Kit features into Android voting app, we can enhance user experience, automate processes, improve data accuracy, and perform advanced analysis to gain insights into voter behavior or sentiment. Remember to consider privacy and security concerns when implementing ML features, especially when handling sensitive voter data.

Feature	On-device	Cloud
Text recognition	✓	✓
Face detection	✓	
Barcode scanning	✓	
Image labeling	✓	✓
Object detection & tracking	✓	
Landmark recognition		✓
Language identification	✓	
Translation	✓	
Smart Reply	✓	
AutoML model inference	✓	
Custom model inference	✓	

Figure 4.14: Features of Firebase Ml-kit

4.2.5   Admin Module

The e-voting system we have created utilizes Firebase as the underlying technology stack. The Realtime Database serves as the backbone for the system's admin module, providing essential functionality for administrators. The administrators of this module may add new users, capturing their phone numbers, election districts, constituencies, and district names. The module also includes a polling division feature, which encompasses candidates, a helpdesk with a helpline number and helpline email, registration locations, and voters' information. The Realtime Database efficiently stores crucial voter details, including names, passwords, village IDs, and voting choices (represented as "yes" or "no").

The e-voting system heavily utilises the Firestore Database in addition to the Realtime Database. With the versatile and scalable data storage provided by this document-oriented database, effective querying and flawless data synchronisation are guaranteed. The Firestore Database is organized into various collections, each serving a specific purpose in the e-voting system's data management.

- The "Answers" collection within Firestore captures responses to questions posed to candidates or voters, facilitating further analysis and evaluation. This collection plays a vital role in gathering insights and opinions from the participants.

- To ensure the integrity of the voting process, the "Ballot Box" collection securely stores submitted votes. This collection guarantees the accuracy and confidentiality of each vote, maintaining the credibility of the electoral system.

- Information about candidates participating in the election is stored in the "Candidates" collection. It includes profiles, credentials, party affiliations, and other relevant details, providing transparency and enabling voters to make informed choices.

- The "Constituencies" collection contains specific details about constituencies, which are important subdivisions within election districts. This collection captures distinct geographic areas or demographic characteristics that influence the election process, aiding in efficient district-level management.

- The "Districts" collection stores essential information about election districts, such as names, boundaries, and administrative details. It serves as a crucial reference for administrators and helps in organizing and overseeing the electoral process effectively.

- The "Registrations" collection captures the registration details of voters, streamlining the process of verifying their eligibility to participate in the election. This collection helps maintain accurate voter records and facilitates authentication during the voting process.

- The "Voters" collection stores comprehensive information about registered voters, including profiles, identification details, and other attributes necessary for authentication and verification. This collection serves as a central repository of voter data, ensuring accurate and up-to-date information for the election process.

- The "Votes" collection records individual votes cast by registered voters. It ensures transparent and anonymous storage of each voter's choice, maintaining the privacy and integrity of the voting process.

Using Firebase and its Realtime Database and Firestore Database components offers a robust and scalable solution for modernizing the electoral process. By effectively utilizing these databases, the system streamlines administrative tasks, provides secure and efficient data storage, and ensures a transparent and reliable voting experience for administrators, candidates, and voters. The system's ability to handle user management, store voter information, facilitate candidate management, and enable efficient data querying makes it a valuable tool in revolutionizing the electoral process.

Chapter 5

Results

- Using Firebase database, we monitor the realtime users like how many users logged in to the Application.

- Using Firebase and its Realtime Database and Firestore Database components offers a robust and scalable solution for modernizing the electoral process.

- Increased Voter Engagement: A user-friendly and accessible voting app can attract more voters and encourage participation, especially among tech-savvy demographics. This can lead to increased voter turnout and engagement in the democratic process.

- Streamlined Voting Process: the app can simplify the voting process, allowing users to cast their votes conveniently and quickly. This can lead to a more efficient voting experience and reduce long queues or waiting times at polling stations.

- Real-time Results and Analysis: With real-time data synchronization and analytics capabilities, the app can provide instant and accurate vote counts, enabling the quick generation and publication of results. This allows stakeholders and the public to access up-to-date information on the voting outcome.

- Cost and Time Savings: Digital voting systems can reduce the costs associated with traditional paper-based voting methods, such as printing ballots and manual vote counting. Moreover, automated processes and efficient data management can save time for election administrators.

- Transparency and Trust: The use of blockchain technology can enhance transparency and trust in the voting process. By providing a decentralized and verifiable record of votes, the app can increase confidence among voters and stakeholders in the fairness and reliability of the results.
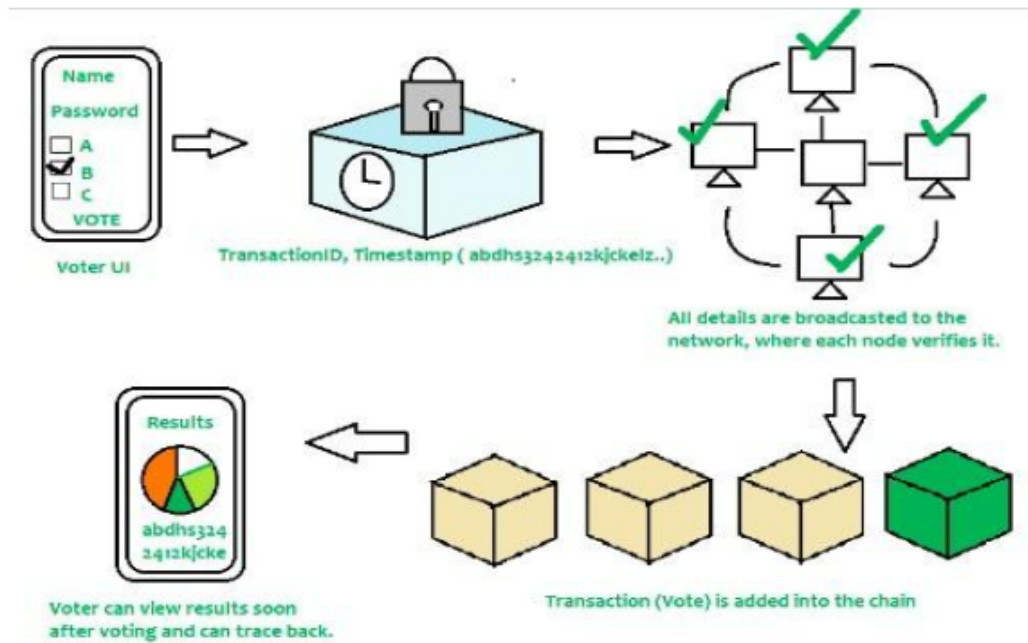
Figure 5.1: model of storing vote with blockchain

The Blockchain utilised to store the votes in the application is seen in the diagram up top. When a voter casts a ballot, the vote is time-stamped and broadcast to all nodes (systems) in the network, informing them that the voter in question is prohibited from casting another ballot for the specific election period. the transaction is subsequently recorded in the blockchain and added to the chain. Utilising blockchain in the application will assist us in removing the network's single point of failure.

Chapter 6

Conclusion and Future Work

6.1 Conclusion

The Android Voting Application developed with Android Studio, Firebase, and Blockchain integration offers a secure and efficient solution for the voting process. By combining the power of these technologies, the application ensures transparency, data integrity, and user-friendly experience. The design of a strong and aesthetically pleasing user interface is made possible by the use of Android Studio as the development platform, which improves the usability and accessibility of the voting app for a variety of Android devices.

Firebase Authentication, which ensures that only authorised users may participate, enhances the security and integrity of the voting process in the voting application with Firebase integration. Real-time data synchronisation, made possible by Firebase Realtime Database or Firestore, enabling prompt updates and precise vote tallying across many devices. Additionally, Firebase ML Kit offers machine learning features like face detection, word recognition, and image labelling that can improve the usability and functionality of the application.

The voting application's security and reliability are further increased by the use of blockchain technology. Blockchain stores voting information in a decentralised, tamper-proof ledger, ensuring its immutability and transparency. Each vote is recorded permanently, allowing for verification and the detection of any unauthorised alterations. Blockchain also improves the voting process' auditability and traceability, enabling participants to confirm the accuracy of the results.

However, additional factors like legal and regulatory constraints, user privacy protection, and thorough testing must be taken into account in order to guarantee the application's dependability and compliance with industry standards. Regular upgrades and maintenance are also required to address potential risks and adapt to changing technological advancements.

35

Overall, the Android Voting Application developed with Android Studio, Firebase, and Blockchain integration presents a promising solution for modernizing and digitizing the voting process, promoting inclusivity, transparency, and trust in democratic practices.

6.2   Future Work

- In the future, we will improve our system by integrating AADHAAR Card information so that we can match the user's actual biometrics with what they input, and we'll also incorporate facial recognition and face detection so that our system is more reliable.

- Adding support for local languages to the Android Voting Application can significantly enhance its accessibility and user reach.

- Integration with External Systems: Consider integrating the voting application with other systems or platforms, such as government databases or voter registration systems, to streamline the overall voting process. This integration can automate voter registration, validate voter eligibility, and ensure seamless data exchange.

References

[1] Cosmas Krisna Adiputra, Rikard Hjort, and Hiroyuki Sato. A proposal of blockchain-based electronic voting system. In *2018 second world conference on smart trends in systems, security and sustainability (WorldS4)*, pages 22–27. IEEE, 2018.

[2] Mohammad Kamel Alomari. Digital divide impact on e-voting adoption in middle eastern country. In *2016 11th International Conference for Internet Technology and Secured Transactions (ICITST)*, pages 409–412. IEEE, 2016.

[3] Hamoud Alshammari, Khaled Elleithy, Khaled Almgren, and Saleh Albelwi. Group signature entanglement in e-voting system. In *IEEE Long Island Systems, Applications and Technology (LISAT) Conference 2014*, pages 1–4. IEEE, 2014.

[4] Syada Tasmia Alvi, Mohammed Nasir Uddin, and Linta Islam. Digital voting: A blockchain-based e-voting system using biohash and smart contract. In *2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT)*, pages 228–233. IEEE, 2020.

[5] Ahmed Ben Ayed. A conceptual secure blockchain-based electronic voting system. *International Journal of Network Security & Its Applications*, 9(3):01–09, 2017.

[6] Supeno Djanali, Baskoro Adi Pratomo, Karsono Puguh Nindyo Cipto, Astandro Koesriputranto, and Hudan Studiawan. Design and development of voting data security for electronic voting (e-voting). In *2016 4th International Conference on Information and Communication Technology (ICoICT)*, pages 1–4. IEEE, 2016.

[7] Kanika Garg, Pavi Saraswat, Sachin Bisht, Sahil Kr Aggarwal, Sai Krishna Kothuri, and Sahil Gupta. A comparitive analysis on e-voting system using blockchain. In *2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU)*, pages 1–4. IEEE, 2019.

[8] Ramya Govindaraj, P Kumaresan, et al. Online voting system using cloud. In *2020 International Conference on Emerging Trends in Information Technology and Engineering (ic-ETITE)*, pages 1–4. IEEE, 2020.

[9] Fririk Hjálmarsson, Gunnlaugur K Hreiarsson, Mohammad Hamdaqa, and Gísli Hjálmtỳsson. Blockchain-based e-voting system. In *2018 IEEE 11th international conference on cloud computing (CLOUD)*, pages 983–986. IEEE, 2018.

[10] SM Jambhulkar, Jagdish B Chakole, and Praful R Pardhi. A secure approach for web based internet voting system using multiple encryption. In *2014 International Conference on Electronic Systems, Signal Processing and Computing Technologies*, pages 371–375. IEEE, 2014.

[11] Baoyuan Kang. Cryptanalysis on an e-voting scheme over computer network. In *2008 International Conference on Computer Science and Software Engineering*, volume 3, pages 826–829. IEEE, 2008.

[12] Nir Kshetri and Jeffrey Voas. Blockchain-enabled e-voting. *Ieee Software*, 35(4):95–99, 2018.

[13] Mahender Kumar, Satish Chand, and Chittaranjan Padmanabha Katti. A secure end-to-end verifiable internet-voting system using identity-based blind signature. *IEEE Systems Journal*, 14(2):2032–2041, 2020.

[14] Oleksandr Kurbatov, Pavel Kravchenko, Nikolay Poluyanenko, Oleksiy Shapoval, and Tetiana Kuznetsova. Using ring signatures for an anonymous e-voting system. In *2019 IEEE International Conference on Advanced Trends in Information Theory (ATIT)*, pages 187–190. IEEE, 2019.

[15] Tulasi Menon and R Sindhuja. Id based signature schemes for electronic voting. In *2009 Second International Conference on Computer and Electrical Engineering*, volume 1, pages 403–406. IEEE, 2009.

[16] Evgeniy V Palekha, Irina S Trubchik, Olga N Manaenkova, Olga A Safaryan, Vitaliy M Porksheyan, Sergey A Morozov, Larissa V Cherckesova, and Boris A Akishin. Cross-platforming web-application of electronic on-line voting system on the elections of any level. In *2019 IEEE East-West Design & Test Symposium (EWDTS)*, pages 1–4. IEEE, 2019.

[17] Harsha V Patil, Kanchan G Rathi, and Malati V Tribhuwan. A study on decentralized e-voting system using blockchain technology. *Int. Res. J. Eng. Technol*, 5(11):48–53, 2018.

[18] Himanshu Vinod Purandare, Akash Ramswaroop Saini, Freddy Donald Pereira, Bibin Mathew, and Pratiksha S Patil. Application for online voting system using android device. In *2018 International Conference on Smart City and Emerging Technology (ICSCET)*, pages 1–5. IEEE, 2018.

[19] Deepali Raikar and Avimanyou Vatsa. Bct–voting: A blockchain technology based voting sys-tem. In *The 27 th International Conference on Parallel and Distributed Processing Techniques and Applications (PDPTA'21), July*, pages 26–29, 2021.

[20] Chang-Hyun Roh and Im-Yeong Lee. A study on electronic voting system using private blockchain. *Journal of Information Processing Systems*, 16(2):421–434, 2020.

[21] TM Roopak and R Sumathi. Electronic voting based on virtual id of aadhar using blockchain technology. In *2020 2nd International Conference on Innovative Mecha-nisms for Industry Applications (ICIMIA)*, pages 71–75. IEEE, 2020.

[22] G Shanmugasundaram, A Kalaimathy, M Johnvee, and S Pavithra. Perspective anal-ysis of digital voting systems. In *2019 IEEE International Conference on System, Computation, Automation and Networking (ICSCAN)*, pages 1–6. IEEE, 2019.

[23] Poman Sharad and GM Bhandari. A step towards digital voting system using bct.

[24] Ashish Singh and Kakali Chatterjee. Secevs: Secure electronic voting system using blockchain technology. In *2018 International Conference on Computing, Power and Communication Technologies (GUCON)*, pages 863–867. IEEE, 2018.

[25] S Srinivas, B Ashwin Kumar, and R Srishylam. Blockchain-based e-voting system using proof of voting (pov) consensus algorithm. *CVR Journal of Science and Tech-nology*, 18(1):110–114, 2020.

[26] B Sudharsan, Nidhish Krishna MP, M Alagappan, et al. Secured electronic voting system using the concepts of blockchain. In *2019 IEEE 10th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, pages 0675–0681. IEEE, 2019.

[27] Mohib Ullah, Arif Iqbal Umar, Noor ul Amin, et al. An efficient and secure mobile phone voting system. In *Eighth International Conference on Digital Information Management (ICDIM 2013)*, pages 332–336. IEEE, 2013.

[28] Emre Yavuz, Ali Kaan Koç, Umut Can Çabuk, and Gökhan Dalkılıç. Towards secure e-voting using ethereum blockchain. In *2018 6th International Symposium on Digital Forensic and Security (ISDFS)*, pages 1–7. IEEE, 2018.

[29] Zhao Yuehua and Fan Lijuan. Research on the voting algorithm and its application in intrusion tolerant system. In *2010 2nd International Conference on Computer Engineering and Technology*, volume 7, pages V7–206. IEEE, 2010.

[1] [2] [3] [4] [5] [6] [7] [8] [9] [10] [11] [12] [13] [14] [15] [16] [17] [18] [19] [20] [21] [22] [23] [24] [25] [26] [27] [28] [29]