CHAPTER 1
INTRODUCTION

1.1. OVERVIEW

India is the largest democratic and Republic country in the world. In any democratic and republican country elections are necessary and also a heart to the democracy. In a democracy people have the privilege of being ruled by a government of their own choice. People choose their representatives through elections which are the normal features of democracies all over the world. But these elections should be held freely, fairly, transparently and impartially. For this purpose, the constitution of India provides an Election Commission with autonomous (Art 324-329), consisting a Chief Election Commissioner and other Election Commissioners (at present two other election commissioners).

1.1.1. Indian Electoral System:

The Constitution of India has vested in the Election Commission of India the Superintendence, direction and control of the entire process for conduct of elections to Parliament and Legislature of every State and to the offices of President and Vice-President of India. The Indian Electoral system has been broadly divided into two, they are direct election based on territorial constituencies and proportional representation by means of a single transferable vote.

The first system is followed for the election of the members of Lok Sabha, State Assemblies and Union territories ‘assemblies. The second, election held on the basis of proportional representation by means of a single transferable vote for the President and the Vice-President of India, members of Rajya Sabha and members of Legislative councils.

THE MAIN FEATURES OF INDIAN ELECTORAL SYSTEM:

- Elections are held on the basis of Universal adult franchise, who is a citizen of India and not less than 18 years of age can register as a voter in electoral roll of India. There is no discrimination on the ground of religion, race, caste, sex or any of them.
- There is a provision for reservation of seats for Scheduled Castes (84 Seats) and Scheduled Tribes (47 Seats) in Lok Sabha and Assemblies of State and Union Territories, but there is no such provision of reservations in Rajya Sabha at the Union level and Legislative councils at the State level.
- For the general seats representation is accorded on territorial basis through common electoral roll. Constituencies are delimited with the help of a delimitation commissions (1952, 1963, 1973 and 2002) which is appointed after the census that takes place after every ten years. The result of the revision of constituencies is that that the areas/boundaries change from election to election, but the number of constituencies will not be changed up to the year 2026.
- Voting takes place through secret ballot for the Lok Sabha and State assemblies. It is most important and prerequisite to the public to express their will freely and fairly. For the Rajya Sabha and Council of States through the open ballot system is introduced to stop the corruption in those elections.
- Political parties are an indispensable part of the electoral process. In India multi-party system is functioning.
- Elections are determined on the basis of relative majority of valid votes polled.

1.1.2. Evolution of electoral system in India

After India attained Independence in August 1947, there was a need to hold General Elections to elect a truly representative Government on the basis of universal adult suffrage. Article 324, which provides for the setting up of Election Commission as an independent constitutional authority, was therefore brought into force from November 26th, 1949.

To provide a legal framework for the conduct of elections, Parliament passed the first Acton May 12th, 1950 (Representation of the People Act, 1950) providing mainly for the preparation of electoral rolls and second Act on July 17th, 1951 (Representation of the People Act, 1951) laying down the procedure for the conduct of elections to both Houses of Parliament and Vidhana Sabha's for each State.

After the constitution of the two Houses of Parliament and the State Legislative Assemblies, the first Presidential election was held in May, 1952 and the first duly elected President assumed the charge of office on May 13th, 1952.

For the first and second General Elections in 1951-52, and 1957, the Election Commission adopted the 'Balloting System' of voting. From the 3rd General Elections in 1962 onwards, the Commission switched over to 'marking system' of voting.

The Electronic Voting Machines (EVMs) were used for the first time in part of Parur Assembly Constituency in Kerala in 1982, on experimental basis. Later, the extensive use of EVMs started in 1998. The EVMs were used at all polling stations in the country in the14th General Elections to the Lok Sabha in 2004 for the first time. Since then, all elections to Lok Sabha and Legislative Assemblies have been held using EVMs.

1.2. PROBLEMS IDENTIFIED

India’s current voting system is still fairly traditional and follows the age-old processes. Electoral frauds such as false voter registration, voter intimidation, and irregularities in tallying procedures are clandestine and illegal efforts to shape election results (Lehoucq 2003). Due to their illicit nature, it's hard to study the effects of these practices as political agents are careful not to leave trails. One of the reasons behind controversies associated with the choice of voting technology is that there is little systematic empirical evidence on the relationship between voting technology and election outcomes. Electoral fraud undermines public trust in democratic institutions creating political instability, and may affect long-term growth. In India, many voters do not cast their votes. The voting percentage generally is almost 50 to 60 percent.

Therefore, the representative bodies are not truly representative. One of the main issues India is facing at present is the declining voter turnout. The government attributes this to the fact that people have to vote from the constituencies where they have registered. Voters need to assemble at a centre allotted by the local authority to cast their votes. The process followed to collect and then count the votes has many irregularities that allow cheating and errors. Apart from the actual process, the counting of votes is a time-consuming activity.

If any of the parties challenge the results, the recounting of votes, becomes cumbersome and consumes significant resource. The rigging of poll booths. Some big political parties have an obvious advantage where they can use an excess of money power to ‘buy’ votes with bribery. Other important two kinds of attacks against a real Indian EVM. One attack involves replacing a small part of the machine with a look-alike component that can be silently instructed to steal a percentage of the votes in favour of a chosen candidate. These instructions can be sent wirelessly from a mobile phone. Another attack uses a pocket-sized device to change the votes stored in the EVM between the election and the public counting session, which in India can be weeks later. The current FEC Standards requires that the voting system count ballots, and for each office or measure, that it count votes overvotes and undervotes.

1.3. AI, ELECTORAL BIOMETRICS, BLOCKCHAIN AND IOT

Artificial Intelligence

Artificial Intelligence (AI) is increasingly changing the way we live. AI systems are also being used in democratic elections. The emergence of artificial intelligence (AI), machine learning (ML), and big data have fundamentally changed how politicians engage the Indian electorate and will continue to challenge centuries of political and intrapersonal norms surrounding voter enfranchisement.

Electoral Biometrics

In electoral law, the ballot is considered fair if it meets the requirements of equality and liberty, and the secrecy of voting is respected. The usage of biometric systems in electoral processes makes it possible to meet challenges involved in implementing the principle of "one voter, one vote," which is necessary for the holding of democratic, free and transparent elections.

Blockchain and IoT

The Internet of things (IoT) is transforming the way enterprises operate through the use of sensors and other edge devices and infrastructure. This presents a major challenge for enterprises, which must protect information at all levels of the IoT ecosystem. With the number of connected devices growing multifold every year, data security has become increasingly complex.

Blockchain is helping combat security breaches in an IoT system. Blockchain is a distributed ledger technology that combines with IoT to make machine-to-machine transactions possible. It uses a set of transactions that are recorded in a database, verified by multiple sources and entered in a common ledger distributed across every node.

The combination of IoT and blockchain offers various potential benefits and allows a smart device to function autonomously without the need for a centralized authority. It can also track how devices communicate with each other. While the decentralized nature of blockchain is an architectural benefit, it can be a potential problem for IoT. IoT platforms rely on client-server or hub-and-spoke architecture, which is a centralized authority.

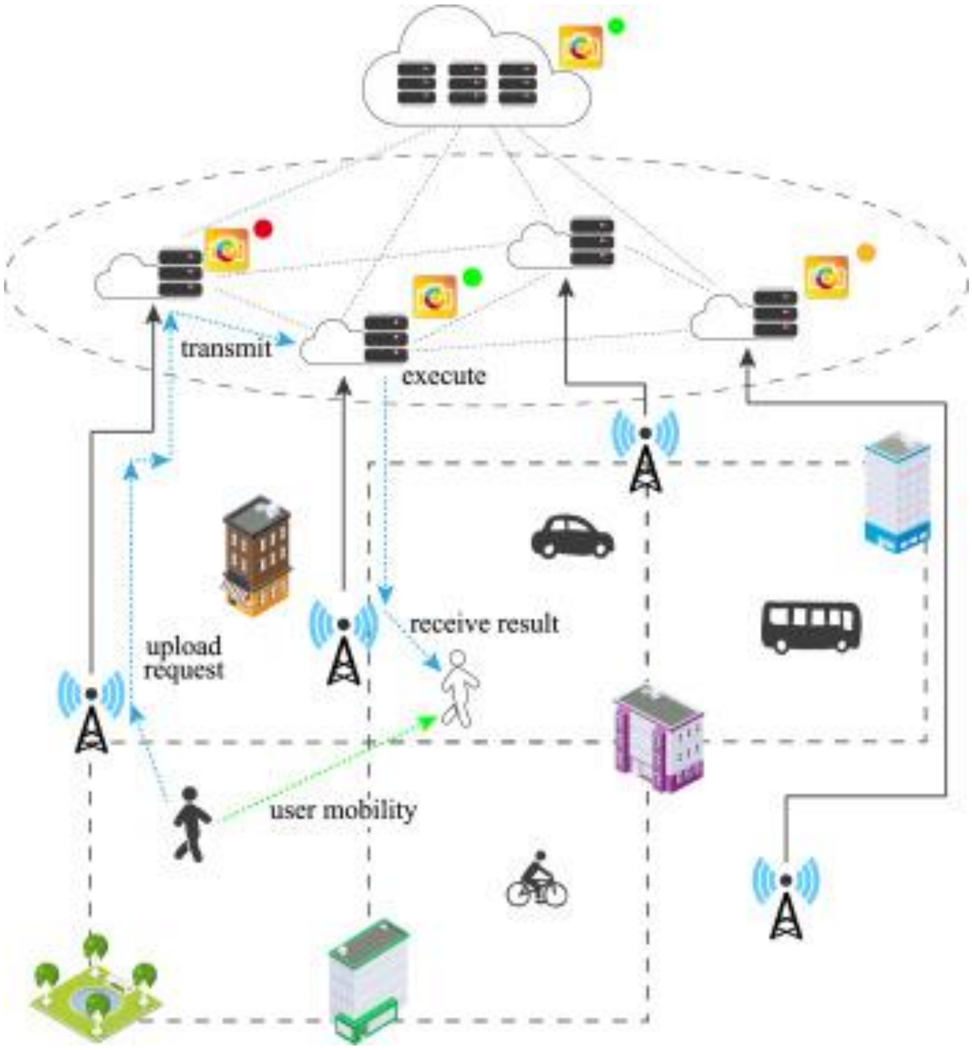

Figure 1.1. Blockchain and IoT

Building an IoT platform that is decentralized in nature will help ensure compatibility with a blockchain network, but it can be a challenge to configure IoT sensors to handle their own computer and data storage, since they rely on central compute and storage resources. This application of blockchain technology allows enterprises to manage data on edge devices in an IoT system, reducing costs associated with IoT device maintenance and data transfer.

It reduces the risks of managing data, because there is no centralized data repository and the ledger is not vulnerable to cyberattacks. It eliminates the IoT gateway or any other intermediate device for data exchange and reduces the time required to process the data. Blockchain imposes high-level security by authenticating and authorizing encrypted device-generated data with the help of decentralized, distributed ledgers. In a distributed ledger, data computation and storage are spread across millions of devices.

1.3.1. Applications of IoT and blockchain

- LOG OPERATIONAL MAINTENANCE DATA - IoT devices track the state of safety for critical machines and their maintenance. From engines to elevators, blockchain provides for a tamper-free ledger of operational data and the resulting maintenance. Third-party repair partners can monitor the blockchain for preventive maintenance and record their work back on the blockchain. Operational records can also be shared with government entities to verify compliance.
- AUTOMOTIVE SECTOR - The impact of digitalization has resulted in the prolific growth of its competitive demand. Automotive industries have been successfully utilizing IoT-enabled sensors for the development of completely automated vehicles. One of the most prolific uses of blockchain IoT can be identified in the automotive sector for connecting blockchain with industrial IoT solutions. As a result, it can empower multiple users for easier and faster exchange of crucial information.

- SMART HOMES/BIOMETRICS - Following on from smart cities, smart homes are gaining protagonist as well, as IoT devices are increasingly used in our everyday lives. Yet, biometrics alone cannot remove the issue of centralized infrastructure or the possibility of hackers tampering with the data captured by smart devices. Blockchain provides a much safer way of securing the multitude of biometric data, ensuring that it is only accessible to the right parties. This not only keeps consumers safe but saves businesses from the threat of costly cyber-attacks, data breaches, and even litigation.
- MACHINE-LED MAINTENANCE - IoT devices are already helping manufacturers around the world to eliminate inefficiencies and boost their bottom lines. By using smart sensors on their equipment, businesses can reduce expensive downtime through machine-led maintenance. The sensors transmit real-time data on machinery and send reports or error messages allowing business owners to schedule preventive maintenance, essentially fixing a problem before it arises. However, with the attack vector of IoT devices still an easy target for hackers, human intervention and checks are still widely used to ensure that error reports are not altered, tampered with, or overwritten, blockchain can help eliminate this. Plus, with the data distributed across multiple servers, blockchain eliminates the threat of attack and single point of failure of centralized systems, greatly increasing IoT's reliability while removing the need for manual processes and eliminating human error. This risk mitigation translates into significant cost savings for businesses that they can pass on to consumers.

1.4. SCOPE OF THE PROJECT

This project has introduced a secure and transparent e-voting mechanism through trusted IoT devices using Blockchain technology with the aim of detecting and resolving the various threats caused by an intruder at various levels. The trust of IoT devices is computed through a social optimizer that identifies their trust values by analysing their communication behaviours.

In order to prevent a prospective change of stored record of votes in databases, Blockchain is maintained at various levels that keeps track of all the recorded information handled by the election conducting bodies.

Therefore, the potential contribution of the proposed framework is detailed as follows:

- The security of IoT devices is ensured by analysing their communication behaviours through social optimizer by ensuring their trust values.
- The proposed mechanism is a two-end system, i.e., both the National election bodies and every entity may ensure the security upon compromise of IoT devices through blockchain mechanism.
- The proposed mechanism of voting using Blockchain not only serves the election conducting bodies but also the voters who get notified in case of any meddling with their votes before the scheduled counting day.

1.5. OBJECTIVE OF THE PROJECT

The objective of this project is to provide a secure hybrid voting architectural framework using Blockchain technology. The goal of this project has proposed a transparent mechanism in order to overcome the existing issues such as cost, time, delay, computational storage, key management overhead etc.

In the proposed solution, all the activities are managed using a Blockchain based mechanism. It has proposed a two-end mechanism in which all the activities are coordinated by the national and state bodies at various levels and voters play an equal part in it.

1.6. BENEFITS OF THE PROJECT

- REDUCING COST: a blockchain-based scheme is proposed to satisfy the basic e-voting properties offering a degree of decentralisation and putting as much power of the mechanism in the voters' hands. Large-scale conventional elections, especially when there are hundreds of geographically distributed voting centres with millions of voters and are very expensive in the long term.
- INCREASING PERCENTAGE OF TOTAL VOTES (PER BOOTH): Polls were always subject to understatement. Voting has been the subject of voter fraud worldwide in particular. It could leave us wondering how the outcome of elections could vary incredibly if the apt consensus of the people could be reflected. Blockchain may clearly show to be an answer over-looked by governments and their citizens. Increasing transparency: Every nation demands a framework that ensures legitimate voting registration with recognisable proof. They should have a voting platform that optimises the process of looking cast a ballot.
- REDUCING BOGUS/ FRAUDSTERS: The blockchain functionality such as encryption and immutability make it nearly impossible for someone to cast an unlawful or fraudulent vote, or to make adjustments once registered. Distributed and globally recognized: Compared to polling via a blockchain system, conventional voting is costlier, vulnerable to manipulation, less reliable and easily corruptible. Blockchain technology offers a reliable and safe way to store data. It maintains security while

remaining open to public inspection, making it ideal for voting. This is why countries such as Japan are now introducing blockchain to their voting system in order to make the voting system more accessible and simpler.

CHAPTER 2
LITERATURE SURVEY

1. ONLINE SMART VOTING SYSTEM USING BIOMETRICS BASED FACIAL AND FINGERPRINT DETECTION ON IMAGE PROCESSING AND CNN

Authors: S.Jehovah Jireh Arputhamoni; A.Gnana Saravanan

Year: 2021

Link: https://ieeexplore.ieee.org/document/9388405

Objective:

The aim of this project is the detection of face and fingerprint images, the number of fake voters can be reduced using Haar Cascade Algorithm.

Methodology:

Web-based system enables voter to cast their votes from anywhere in the world. Online website has a prevented IP address generated by the government of India for election purpose. People should register the name and address in the website. Election commission will collect the fingerprint and face image from the voters. When the images are obtained on the casting day, it will be compared with database and provides a secured voting on the Election Day. System utilizes faces and fingerprints to unlock the voting system, similar to the mobile phone are used.

Merits:

- More secure and efficient.
- Less time-consuming.

Demerits:

- Time consuming job.
- Cost and implementation is high.

2. SMART ONLINE VOTING SYSTEM

Authors: SGanesh Prabhu; A Nizarahammed.; S Prabu.; S Raghul.; R.R. Thirrunavukkarasu; P. Jayarajan

Year: 2021

Link: https://ieeexplore.ieee.org/document/9441818

Objective:

The aim of this project is to allow the user to vote offline as well if he/she feels that is comfortable using radio frequency identification (RFID) tags.

Methodology:

This article proposed online voting system allows the user to vote through either offline or online. If the user decides to vote through offline the user must have an RFID tag which will be issued by the government to him/her. It is scanned by a RFID card reader and then compared based on the details stored in the database. The user if votes through offline must also undergo the traditional use cases of fingerprints and voter id. If the user decides to vote through online he/she must record their face in the system provided.

Merits:

- Avoiding any mistakes to takes place.
- Reduces the time taken to publish the results.
- Reduce labour force, money and time.

Demerits:

- Voter's Id and others details are validated manually and only after confirmation he/she will be allowed to vote.
- Time-consuming processes.
- It requires man-power and security.

3. ONLINE VOTING SYSTEM USING CLOUD

Authors: Ramya Govindaraj, Kumaresan P, K.Sree harshitha.

Year: 2020

Link:

https://www.researchgate.net/publication/340972420_Online_Voting_System_using_Cloud

Objective:

The aim of this project is to implement online voting system with features like the schemes that the specific party has implemented, based on the features are going to vote.

Methodology:

Before days there was voting system with papers. Now, this electronic system has no need of ballot papers etc. All the authorized and eligible persons can register through online and can vote by logging into their own systems. There is no time consuming for the users. The major advantage is that the user has no need of coming to the voting halls, as they can vote from anywhere. It has more features as compared to the normal voting system.

Merits:

- They can vote from anywhere.
- People can cast their votes without missing.
- It gives graphical and easy to understand portrayal of the votes acquired by every applicant.

Demerits:

- Time devouring.
- Consumes extensive volume of pare work.

4. INTEGRATION OF AN ONLINE VOTING SOLUTION WITH THE SMESEC SECURITY FRAMEWORK

Authors: Jordi Cucurull; Christos Tselios; Carolina Rueda; Noemi Folch; Fady Copty; Reda Igbaria; Manos Athanatos; Antonios Krithinakis; Sotiris Ioannidis; Jose Francisco Ruiz; Pablo Barrientos

Year: 2020

Link: https://ieeexplore.ieee.org/document/9275838

Objective:

The aim of this project is to integration with the SMESEC framework and how exactly this was beneficial for the specific online voting solution.

Methodology:

SMESEC is an H2020 project that designed and implemented a lightweight cybersecurity framework for protecting small and medium-sized enterprises against cyber threats. The framework integrates a large variety of contemporary cybersecurity tools but also provides additional features aiming to facilitate novice users to get an overview of existing threats through simple tutorials, extensive explanatory material and a complete lesson learned section. One of the possible areas in which the project can demonstrate its potential is in the protection of online voting solutions for small companies or governmental institutions.

Merits:

- Security layer for hardening, monitoring, attack detection and prevention.
- Malformed requests can be redirected away from the server.

Demerits:

- Security is low.
- Time consuming processes.

5. AVOIDING PHISHING ATTACK ON ONLINE VOTIG SYSTEM USING VISUAL CRYPTOGRAPHY

Authors: Saloni Sunil Rane; Ketaki Adwait Phansalkar; Mayuri Yashvant Shinde; Atiya Kazi

Year: 2020

Link: https://ieeexplore.ieee.org/document/9104071

Objective:

The aim of this project is to maintain the security in online voting system using CAPTCHA code and Image Share technology.

Methodology:

Elections are conducted everywhere, but voters must go to polling booth to caste vote. Election process is very complex and requires a lot of things to be done prior to voting. There are a lot of arrangements to be done. It includes a lot of manual work. In organization voter must be present at voting centre to caste vote. So, the plan is to make the voting process secure and effective one. This article proposes Visual cryptography, it adds security in voting. Consider an online voting system to elect president or any other authority of the carrom association.

Merits:

- It provides two-way securities to the voting system.
- Voting easy to use and efficient.

Demerits:

- It requires more manpower.
- Security is very low.
- Heavy and repetitive task of vote management.

6. THE NEXT GEN ELECTION: DESIGN AND DEVELOPMENT OF E-VOTING WEB APPLICATION

Authors: Raghav Chhabra; Uday Vohra; Vishrant Khanna;

Year: 2020

Link: https://ieeexplore.ieee.org/document/9138050

Objective:

The aim of this project is to come up with a new solution, does come with a small learning curve, citizens will have to be trained on how to exercise their right to vote online.

Methodology:

New internet-based voting system manages the voter's information, which makes the life of the voter easier, they can just simply login and exercise their right to vote. This new voting system is built on the backbone principles of free and fair elections and hence tries to incorporate all the benefits of traditional voting solutions.

Merits:

- Database is stored in an undisclosed location, only top officials of the Election Commission of India know the exact location.
- The system's intelligent design does not allow any person to vote more than once.

Demerits:

- High cost.
- Time involvement is high.

7. DEVELOPMENT OF A FINGERPRINT BIOMETRIC AUTHENTICATION SYSTEM FOR SECURE ELECTRONIC VOTING MACHINES

Authors: B. U Umar, O. M Olaniyi , L. A Ajao , D. Maliki , I. C Okeke

Year: 2019

Link:

https://www.researchgate.net/publication/331511027_Development_of_A_Fingerprint_Biometric_Authentication_System_For_Secure_Electronic_Voting_Machines

Objective

The aim of this project is to combat the current challenges through the development of a fingerprint biometric authentication system for secure electronic voting machines.

Methodology:

Democracy is a system of governance of the people, by the people and for the people. The backbone of this governance system is the existence of elections, the right of governing citizens to choose their leaders. Voting is the process through which elections are carried out. The outcome of voting is the expression of the electorate, opinion and decision that is accepted by everybody. It means that the integrity of elections is the most important factor in the success of the democratic process.

Merits:

- Security is high.
- Easy to use for the electorate.

Demerits:

- Slower speed and High cost.
- Reliability is low.

8. COERCION-RESISTANT E-VOTING SCHEME WITH BLIND SIGNATURES

Authors: Ahsan Aziz

Year: 2019

Link: https://ieeexplore.ieee.org/document/8854547

Objective:

The aim of this project is an e-voting scheme based on blind signatures which fulfils important security requirements and is efficient too.

Methodology:

An ideal e-voting system would allow users to go online, using web-browser or a phone application, enter their credentials and vote; it would also allow voters to verify their votes after election. The properties that make e-voting such a promising technology also raise potential privacy and efficiency problems. In literature, researchers have listed the requirements which an e-voting scheme must have. Many e-voting schemes have been proposed which are based on combination of cryptographic tools, however some schemes have efficiency problems, voter or election authority does a lot of processing at their end, and some do not fulfil all security requirements e.g., most lack coercion-resistance and receipt free-ness.

Merits:

- Fake votes can be minimized.
- It verifies votes – individually and universally.

Demerits:

- Do not provide complete verifiability to voters after election.
- More Fake votes.
- Security is low.

9. E2E VERIFIABLE ELECTRONIC VOTING SYSTEM FOR SHAREHOLDERS

Authors: Samiran Bag; Feng Hao

Year: 2019

Link: https://ieeexplore.ieee.org/document/8937711

Objective:

The aim of this project is an end-to-end (E2E) verifiable online shareholder voting system using personal computing device, say a smart-phone.

Methodology:

In a publicly traded company, shareholders have certain rights pertaining to their equity investment. These include the right to vote on certain corporate matters related to the functioning of that company. For example, shareholders may vote to elect the board of directors or approve proposed motions, such as making tie-ups with external organizations or making a new acquisition. Thus, shareholders play a crucial role in the management of a company and execution of certain policies. This article proposes SHE, an e-voting scheme that allows shareholders of a company to vote remotely (or onsite) on certain corporate matters.

Merits:

- It provides strong guarantees of the voter privacy.
- It incurs reasonable computational and communication load on the election management system.

Demerits:

- Attacks pose a serious threat to the security of any e-voting system.

10. REMOTE ONLINE VOTING SYSTEM USING ANEKA PLATFORM

Authors: Karishma Varshney, Rahul Johari, R. L. Ujjwal

Year: 2018

Link: https://ieeexplore.ieee.org/document/8748809

Objective:

The aim of this project is to initiate the development of a windows application named 'Remote Online Voting System (ROVS)' which is developed for casting of votes remotely using Aneka platform.

Methodology:

At present, during the time of elections people have to visit the polling booths to cast their vote. The right of franchise in democracy is done through Electronic Voting Machine (EVM) which is made available on various polling booths by the government. The process of voting requires the physical presence of a person on the booth. The flaw is that some people like defence officials, migrants working in abroad, physically challenged and officers on duty are unable to cast their votes in their constituencies so their vote are wasted or misused. ROVS is a windows desktop application developed for the purpose of electronic voting remotely on the voting day irrespective of the user physical presence. The ROVS is in the early days of its development.

Merits:

- It resisting the ballot modification by the attacker.
- It avoids the vote alteration, clash attack by harmful assailant.

Demerits:

- It does not provide better security.
- Malicious hackers tamper the original ballots.
- Effectiveness is low.

CHAPTER 3

SYSTEM ANALYSIS

3.1. EXISTING SYSTEM

- KIOSK VOTING - Voting machines would be located away from traditional polling places, in such convenient locations as malls, libraries, or schools.
- REMOTE INTERNET VOTING - It seeks to maximize the convenience and access of the voters by enabling them to cast ballots from virtually any location that is Internet accessible. While this concept is attractive and offers significant benefits, it also poses substantial security risks and other concerns relative to civic culture. Current and near-term technologies are inadequate to address these risks.
- DESIGN OF SECURED E-VOTING SYSTEMS - It is able to desire with the widespread use of computers and embedded systems. Security is the essential problem should be considered in such systems. This method proposes a new e-voting system that fulfils the security requirements of e-voting. It is based on homomorphic property and blind signature plan.
- A HYBRID MOBILE BIOMETRIC- BASED E- VOTING SYSTEM - Information technology changes and gives shape to networked society all over the world today & its solutions are becoming main drivers in almost all field of human life activity. Although the acceptance rate of government applications is increasing e-voting is hardly accepted as main tool in its field because its shortages in offering good solutions to common problems like fraud, bribery, anonymous character of the vote and absence of good independent monitoring.

- TECHNIQUES FOR FEATURE EXTRACTION IN SPEECH RECOGNITION SYSTEM - The time domain waveform of a speech signal carries all of the auditory information. From the phonological point of view, very little can be said on the basis of the waveform itself. However, past research in mathematics, acoustics, and speech technology have provided many methods for converting data that can be considered as information if interpreted correctly.

Disadvantages

- Individuals may cast their single vote twice.
- Voting of non-candidates.
- Tampered data and excessive authorities
- Observing remote voting solutions may be more complex/difficult to organise than in person voting.
- There may be information asymmetry between voters who vote in advance and those who vote on Election Day.
- Remote voting solutions which take place in an uncontrolled environment may present a higher risk of fraud, coercion, family voting, impersonation, violation of ballot secrecy or other compromises to the integrity of the vote.
- They may have financial and administrative consequences for Member States or for particular hosting institutions (such as hospitals or prisons), depending on whether they are introduced in addition to - or instead of - existing methods.
- There may be political disagreement over the method and extent of voting by a diaspora, particularly if this is seen to be politically advantageous to a particular party.

3.2. PROPOSED SYSTEM

In the proposed solution, all the activities are managed using a Blockchain based mechanism. We have proposed a two-end mechanism in which all the activities are coordinated by the national and state bodies at various levels and voters play an equal part in it. The integration of Blockchain mechanism and voting system may reduce the risks with transparent and decentralized feature of Blockchain technology.

- POLL-SITE INTERNET VOTING - It offers the promise of greater convenience and efficiency in that voters could cast their ballots from any poll site using their Aadhar card, and the tallying process would be both fast and certain.
- QR AND FINGERPRINT BASED VOTER VERIFICATION SYSTEM - The proposed method uses the QR code and fingerprint biometric authentication provided by the Aadhaar card in India.
- AADHAR QR VERIFICATION - Aadhaar card contains a citizen information, Aadhaar number, QR code. In that, Aadhaar QR code contains a valid Aadhaar number. By decoding the QR code, the Aadhaar number is obtained. The citizen information can be accessed by using the Aadhaar number. The citizen information contains an iris data, fingerprint data, address, etc. Based on the Aadhaar QR code, a virtual voting System using diary technique is developed. The AVS allows the citizen Aadhaar QR code. The Aadhaar number is extracted by the decoding of QR code. Extract the citizen information and fingerprint from the database based on the Aadhaar number.
- FINGERPRINT BIOMETRIC - In order to prevent identity theft and multiple voting, biometric technology can be used at polling stations to confirm the identity and eligibility of voters. Biometrics is the best technology to identify and authenticate individuals reliably and

quickly based on their unique physical characteristics, such as fingerprints, to cite just the most well-known example.

- DCNN BASED BIOMETRIC VERIFICATION - The individual's biometric features are captured and compared to previously captured and confirmed biometric features of that individual. All biometric data is first captured by a sensor as an image. This image is then further processed into a biometric template. DCNN Algorithm used for verification and de-duplication are based on comparing these biometric templates.
- BALLOT CHAIN - Cast as intended: The recorded vote must be the same as the one the voter intended to cast. The fundamental idea of the Ballotchain solution is to match a Bitcoin transaction to a vote cast by an elector in support of the candidate selected by the voter. Every vote therefore benefits from the characteristics of a Blockchain transaction.
- COUNTED AS CAST - The tally must be the same as the sum of the recorded votes. Satisfying this crucial requirement without tallying authorities is the main Contribution. This is because the last voter to cast a ballot is able to compute the election result before choosing his/her vote and casting the final ballot.
- ENDCORE COUNTING - Artificial Intelligence applied to the electoral count using Counting Sort Decision Algorithm. It is the most vital and robust module that has been developed to run on the Election Day for counting of votes, monitoring of end-to-end process and declaration of Results by the System. The Application is designed in a way that the series of work to be done by the Returning Officer in the System will automatically be popped up one after another.

Advantages

- Ballotchain allows for an online process with the same guarantees of a public election.
- The proposed trusted approach enhances the metrics by reducing cryptographic key management and storage overhead needed during communication process.
- Blockchain network for use as a voting platform with the integration of biometrics for the purpose of enhanced user security.
- Data immutability while providing the user with security and control over their ballot.
- Secure and anonymous votes, which can be verified at any moment
- The fingerprint biometric authentication exhibits better security against the vote modification malware, re-voting malware, and self-voting malware.

3.3. SYSTEM DESIGN

3.3.1. Voter verification module

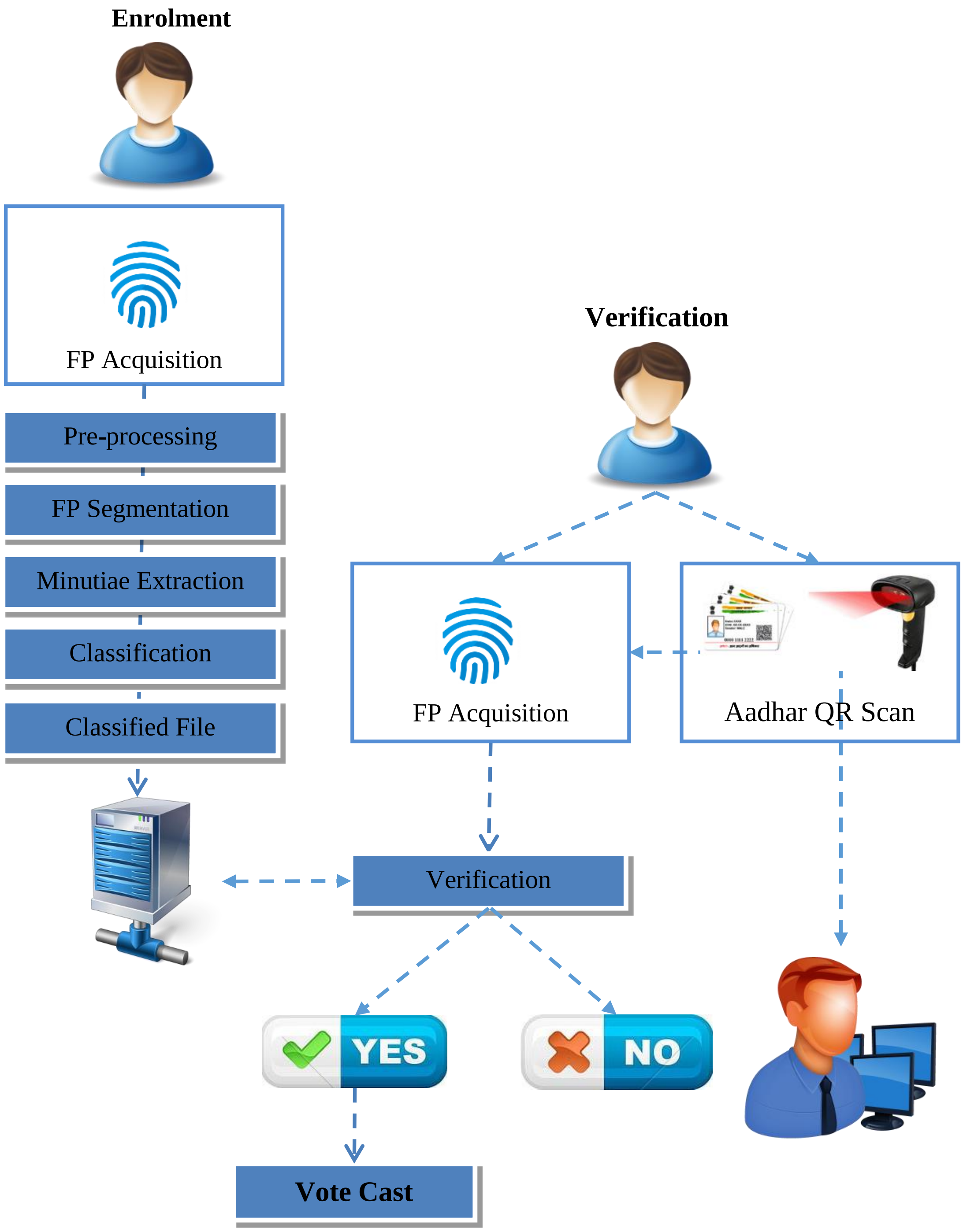

Figure 3.1. Voter Verification Module

3.3.2. System architecture

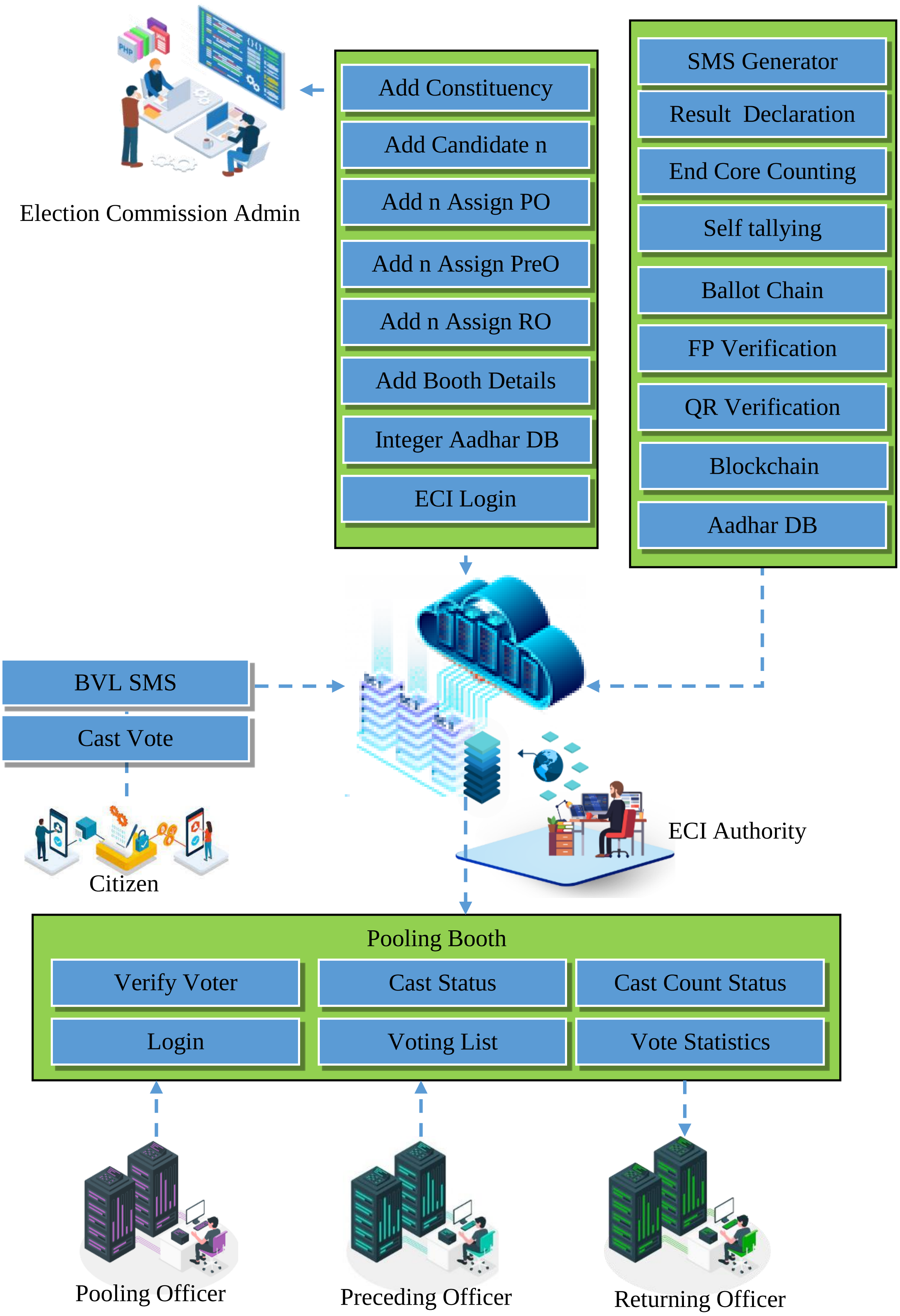

Figure 3.2. System Architecture

CHAPTER 4
SYSTEM IMPLEMENTATION

4.1. MODULES SPLIT UP

1. Ballot Chain Web Dashboard

Initially, the election commission board set under registration process in server. In Under registration process, the Electoral Server is integrated with Aadhar and Blockchain to conduct election securely.

2. End-User Module

2.1. ELECTION COMMISSION ADMIN

Election officer has the authority to add, delete or edit the election district list. Likewise, even the booth details like the reference number, district, and the booth manager in-charge can be seen or edited. In voting process, when election commission checks the voting progress in server.

2.2. ECI AUTHORITY

Once the election commission deselects, the voting progress gets closed in server. The e-voting machine assigned as voting closed at this time voter cannot able to poll their vote. Mainly the ECI authority has the secret key to decrypt Ballotchain votes of each candidate from different booth and announce the winner of election district wise.

2.3. RETURNING OFFICER

Returning Officer In every constituency, one Officer is designated as Returning Officer by the Commission in consultation with the concerned State government. However, an Officer can be nominated as Returning Officer for more than one constituency. All the nomination papers are submitted to the Returning Officer.

2.4. PRESIDING OFFICERS

Every constituency has a large number of polling booths. Each polling booth on an average caters to about a thousand votes. Every such booth is under the charge of an officer who is called the Presiding Officer. He/she supervises the entire process polling in the polling booth and ensures that every voter gets an opportunity to cast vote freely. After the polling is over, he/she seals all the ballot boxes and deliver them to the Returning Officer.

2.5. POOLING OFFICER

Every Presiding Officer is assisted by three to four polling officers. Pooling Officer login to the ballotchain dashboard with given username and password. The Pooling officer receiving the vote may demand that the voter Aadhar identify himself/herself before he or she inserts the ballot in the ballot box.

2.6. CITIZEN

The Citizen can verify ballots on the blockchain to make sure the validity of the voting process.

3. Poll-site Internet voting

The model of an Aadhaar-linked electronic voting system that would enable electors to cast their votes from any part of the country — irrespective of where they are registered to vote to develop a blockchain system that will allow voters registered in any part of the country to exercise their franchise even after they move cities.

4. Blockchain Integration

Smart contract: The role of smart contract includes 1.) Stores the encrypted ballots. 2.) Verify the validity of the ballots. 3.) Count the encrypted ballot. 4.) Verify the correctness of the voting result. 5.) Publish the voting result and provide the platform for the voters to verify the voting process.

5. Voter Verification Module

This module uses the QR code and fingerprint biometric authentication provided by the Aadhaar card in India.

- AADHAR QR VERIFICATION - Aadhaar card contains a citizen information, Aadhaar number, QR code. In that, Aadhaar QR code contains a valid Aadhaar number. By decoding the QR code, the Aadhaar number is obtained. The citizen information can be accessed by using the Aadhaar number.
- DCNN BASED BIOMETRIC VERIFICATION - The individual's biometric features are captured and compared to previously captured and confirmed biometric features of that individual. All biometric data is first captured by a sensor as an image. This image is then further processed into a biometric template.

6. Ballotchain Pooling

Smart Contract:Defining a smart contract includes identifying the roles that are involved in the agreement (the election agreement in our case) and the different components and transactions in the agreement process. The blockchain application layer includes smart contracts, chain code, and Ballot Chain. This layer comprises two sub-layers: 1) presentation layer and 2) execution layer.

The presentation layer includes scripts, APIs, and user interface. These tools are used to connect the application layer with the blockchain network. The execution layer includes smart contracts, chain code and underlying rules. The presentation layer sends instructions to the execution layer, which runs transactions. For example, instructions are sent to chain code in HF and smart contract in EVM.

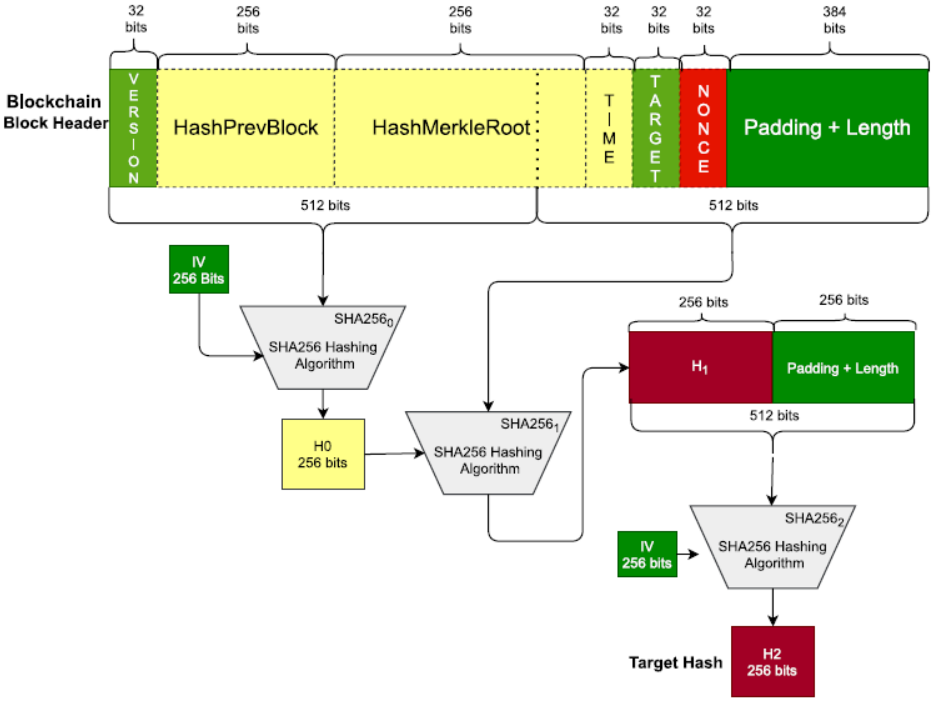

Figure 4.1. Block header hashing algorithm

Each vote is added into each block encrypted by 256-bit SHA hash code, the hashed block cannot be tampered by any individual as more security is added to the system.

4.2. BLOCK DIAGRAM

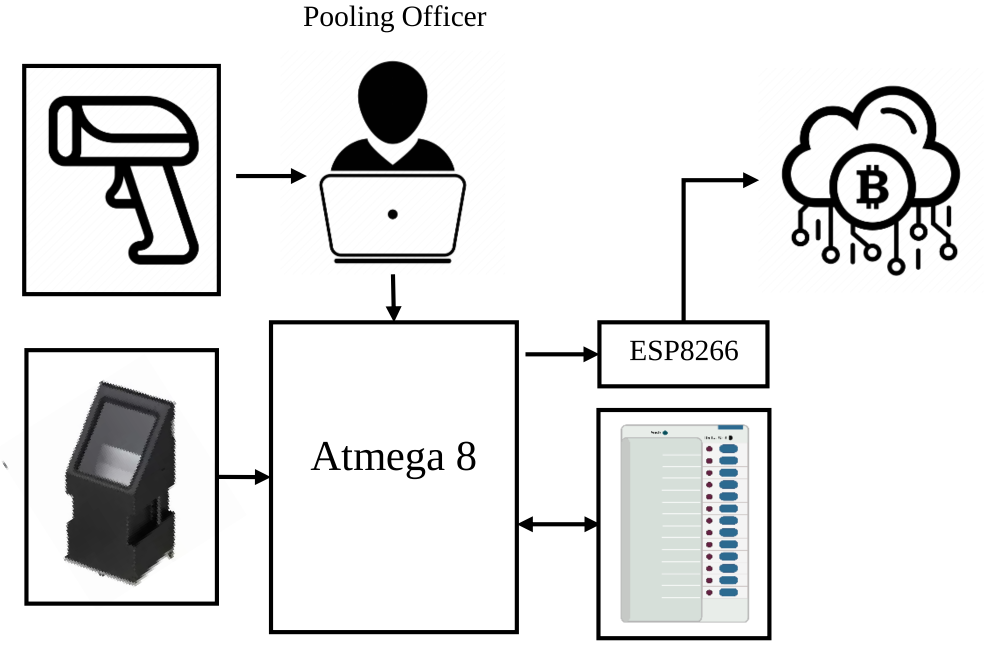

Figure 4.2. Conventional Block Diagram

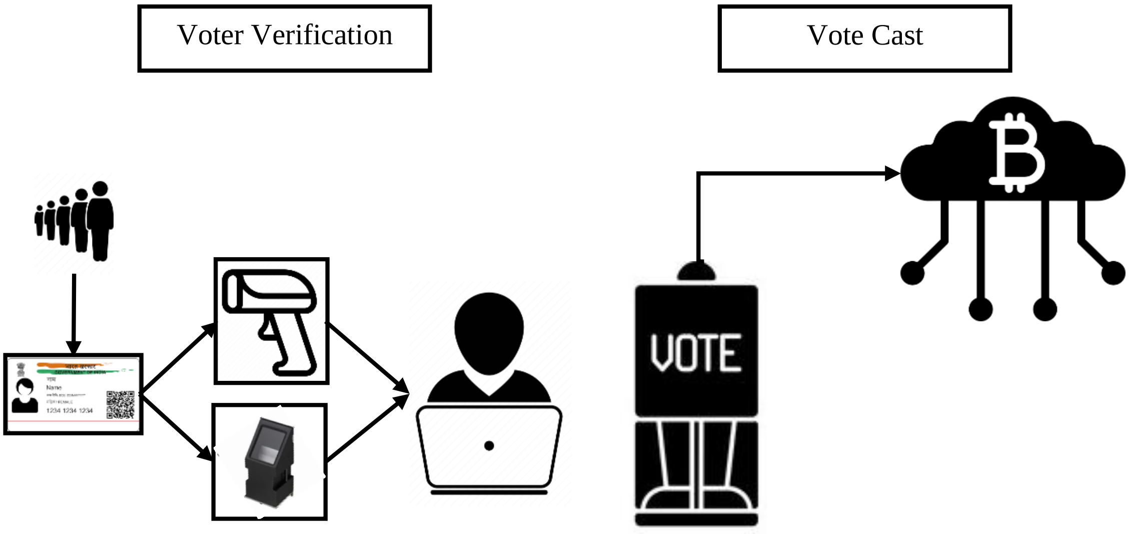

Figure 4.3. Prescribed Block Diagram

Block Description

The activity point to supply a better state of being free from threat or danger in balloting the heavy instrument that get better of the counterfeit referendum. The components with microchips mechanical device are approached by corresponding in pattern the information with the identity info.

In this proposed model, a voter can vote from anywhere and from any constituency of India. Counting will be done automatically and thus reduces the manpower and huge time. So that the Election Commission of India can easily announce the results within a short span of time.

1. REQUESTING TO VOTE: The user has to go the voter booth with his/her Aadhar card, QR is used for verification of the citizen. In this case, the user enters Aadhar number and the next step of verification flows inwards as shown in the Block Diagram Voter Verification. The next step is biometric for verification. This may so eliminate the trail for fake vote, issues in uncertain credentials, use of fake identities, multiple times by the same person for voting at more than one centre.

2. CASTING A VOTE: Voters can need to opt to either vote for one among the candidates or solid a vote. It ensures that the electoral fraud won't happen and therefore the transparency is going to be achieved. While casting, the system ensures that the person is not voted however. If the person has already voted, then the message is going to be displayed because the person is already voted. As an alternative, the person is going to be allowed to vote for his or her desired candidate.

3. ENCRYPTING VOTES: Once an individual vote, a block is instantiated and in real time hash code is calculated for the corresponding block, hash of the current vote in addition because the hash of the previous block is going to be hold on. This fashion every input is going to be unique and make sure that the encrypted outputs are going to be unique in addition. Block header records all the encrypted data of every vote solid. SHA-256 encrypts all the knowledge associated with each vote, and it's inconceivable to search out the encrypted hash function.

Adding the vote to the Block chain: During this step, once an individual completed his vote, his/her vote will be incremented/add to the block chain as shown in the figure 5.1. Every block gets linked to antecedent solid vote. Such a vote cannot be changed. If one block gets changed or tampered the additional blocks from the tampered block will be modified. Hence change of state is not possible in the block chain.

Hardware Components Description

QR HANDHOLD SCANNER DEVICE

UIDAI has introduced new Secure QR Code which contains demographics as well as photograph of the Aadhaar number holder. Information in the QR Code is secure and tamper-proof as it is digitally signed by UIDAI.

Figure 4.4. QR Scanner

R307 OPTICAL FINGERPRINT READER SENSOR MODULE

This is the R307 Optical Fingerprint Reader Sensor Module. R307 fingerprint module is a fingerprint sensor with a TTL UART interface for direct connections to microcontroller UART or to PC through MAX232 / USB-Serial adapter.

Figure 4.5. Finger Print Scanner

The user can store the fingerprint data in the module and can configure it in 1:1 or 1: N mode for identifying the person.

ESP 8266

The "Pitch" is the space between pins on the ESP8266 module, which is important to know if the device will be used on a breadboard. The "Form factor" also describes the module packaging as "2 × 9 DIL", meaning two rows of 9 pins arranged "Dual In Line", like the pins of DIP ICs.

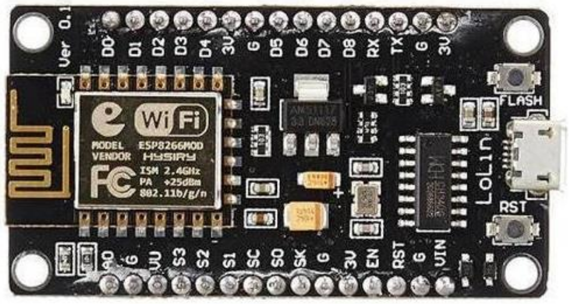

Figure 4.6. ESP 8266

Many ESP-xx modules include a small on-board LED which can be programmed to blink and thereby indicate activity. There are several antenna options for ESP-xx boards including a trace antenna, an on-board ceramic antenna, and an external connector which allows an external Wi-Fi antenna to be attached.

ARDUINO UNO

The Arduino Uno is an open-source microcontroller board based on the Microchip ATmega328P microcontroller and developed by Arduino.cc. The board is equipped with sets of digital and analog input/output (I/O) pins that may be interfaced to various expansion boards (shields) and other circuits.

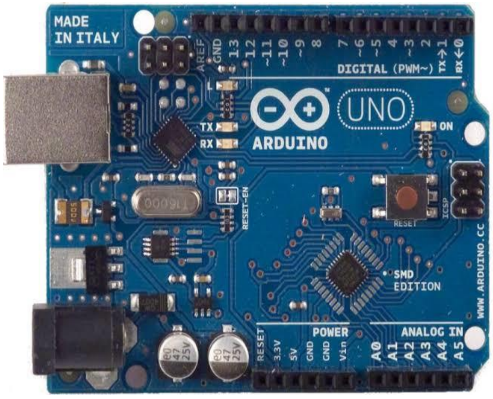

Figure 4.7. Arduino UNO

The Arduino/Genuino Uno has a number of facilities for communicating with a computer, another Arduino/Genuino board, or other microcontrollers. The ATmega328 provides UART TTL (5V) serial communication, which is available on digital pins 0 (RX) and 1 (TX).

OLED

OLED (Organic Light Emitting Diodes) is a flat light emitting technology, made by placing a series of organic thin films between two conductors. When electrical current is applied, a bright light is emitted. OLEDs are emissive displays that do not require a backlight and so are thinner and more efficient than LCD displays (which do require a white backlight).

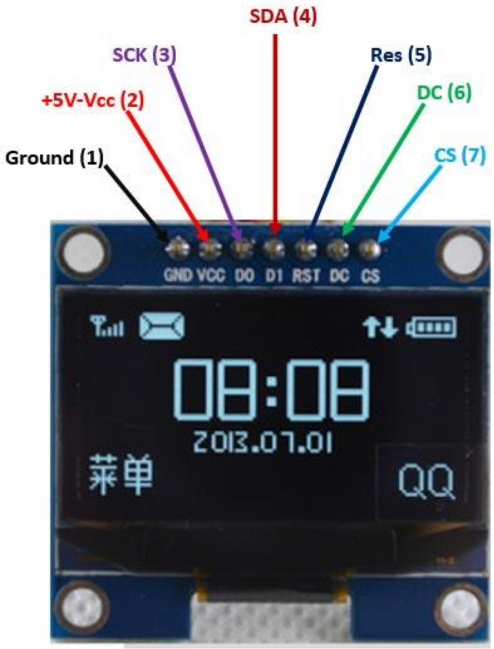

Figure 4.8. OLED

System Specification

HARDWARE SPECIFICATION

- Processors: Intel® Core™ i5 processor 4300M at 2.60 GHz or 2.59 GHz (1 socket, 2 cores, 2 threads per core), 8 GB of DRAM
- Disk space: 320 GB
- Operating systems: Windows® 10, macOS*, and Linux*

SOFTWARE SPECIFICATION

- PHP 5 or Python 3.2
- MySQL
- WAMP Server 2.0
- Macromedia Dream viewer 8 IDE
- Embedded C
- Arduino IDE

SOFTWARE DESCRIPTIONS

ARDUION IDE

Arduino is an open-source electronics platform based on easy-to-use hardware and software. Arduino boards are able to read inputs - light on a sensor, a finger on a button, or a Twitter message - and turn it into an output - activating a motor, turning on an LED, publishing something online. You can tell your board what to do by sending a set of instructions to the microcontroller on the board. To do so you use the Arduino programming language (based on Wiring), and the Arduino Software (IDE), based on Processing.

There are many other microcontrollers and microcontroller platforms available for physical computing. Parallax Basic Stamp, Netmedia's BX-24, Phidgets, MIT's Handyboard, and many others offer similar functionality. All of these tools take the messy details of microcontroller programming and wrap it up in an easy-to-use package. Arduino also simplifies the process of working with microcontrollers, but it offers some advantage for teachers, students, and interested amateurs over other systems:

- INEXPENSIVE - Arduino boards are relatively inexpensive compared to other microcontroller platforms. The least expensive version of the Arduino module can be assembled by hand, and even the pre-assembled Arduino modules cost less than $50.

- CROSS-PLATFORM - The Arduino Software (IDE) runs on Windows, Macintosh OSX, and Linux operating systems. Most microcontroller systems are limited to Windows.
- SIMPLE, CLEAR PROGRAMMING ENVIRONMENT - The Arduino Software (IDE) is easy-to-use for beginners, yet flexible enough for advanced users to take advantage of as well. For teachers, it's conveniently based on the Processing programming environment, so students learning to program in that environment will be familiar with how the Arduino IDE works.
- OPEN SOURCE AND EXTENSIBLE SOFTWARE - The Arduino software is published as open-source tools, available for extension by experienced programmers. The language can be expanded through C++ libraries, and people wanting to understand the technical details can make the leap from Arduino to the AVR C programming language on which it's based. Similarly, you can add AVR-C code directly into your Arduino programs if you want to.
- OPEN SOURCE AND EXTENSIBLE HARDWARE - The plans of the Arduino boards are published under a Creative Commons license, so experienced circuit designers can make their own version of the module, extending it and improving it. Even relatively inexperienced users can build the breadboard version of the module in order to understand how it works and save money.
- ARDUINO INTEGRATED DEVELOPMENT ENVIRONMENT - or Arduino Software (IDE) - contains a text editor for writing code, a message area, a text console, a toolbar with buttons for common functions and a series of menus. It connects to the Arduino and Genuino hardware to upload programs and communicate with them.

EMBEDDED C

In every embedded system-based project, Embedded C programming plays a key role to make the microcontroller run & perform the preferred actions. The controlling of these embedded devices can be done with the help of an embedded C program.

1) Using PHP - With PHP, it's a simple matter to embed dynamic activity in web pages. When you give pages the .php extension, they have instant access to the scripting language. From a developer's point of view, all you have to do is write code such as the following: How are you? The opening command. Outside of this construct, everything is sent to the client as direct HTML.
2) Using MySQL - Of course, there's not a lot of point to being able to change HTML output dynamically unless you also have a means to track the changes that users make as they use your website. In the early days of the Web, many sites used "flat" text files to store data such as usernames and passwords. But this approach could cause problems if the file wasn't correctly locked against corruption from multiple simultaneous accesses. Also, a flat file can get only so big before it becomes unwieldy to manage—not to mention the difficulty of trying to merge files and perform complex searches in any kind of reasonable time.
3) Apache Web Server - In addition to PHP, MySQL, JavaScript, and CSS, there's actually a fifth hero in the dynamic Web: the web server. In the case of this book, that means the Apache web server. We've discussed a little of what a web server does during the HTTP server/client exchange, but it actually does much more behind the scenes. For example, Apache doesn't serve up just HTML files—it handles a wide range of files, from

images and Flash files to MP3 audio files, RSS (Really Simple Syndication) feeds, and more.

4) WAMP, MAMP, or LAMP - abbreviations for “Windows, Apache, MySQL, and PHP,” “Mac, Apache, MySQL, and PHP,” and “Linux, Apache, MySQL, and PHP,” 13 www.it-ebooks.info respectively. These abbreviations describe a fully functioning setup used for developing dynamic Internet web pages.

CHAPTER 5
RESULT AND CONCLUSION

In this section, the performance of our proposed e-voting system is analysed. The prevoting phase has no computation, which only distributes the numbers of the voters and candidates. Thus, we mainly analyse the computation cost of the voting phase and postvoting phase. Moreover, we also, respectively, test the total time cost for the different numbers of voters and candidates by using the 1024-bit session key and the 512-bit shared secret on a laptop.

Performance Analysis of the Voting Phase

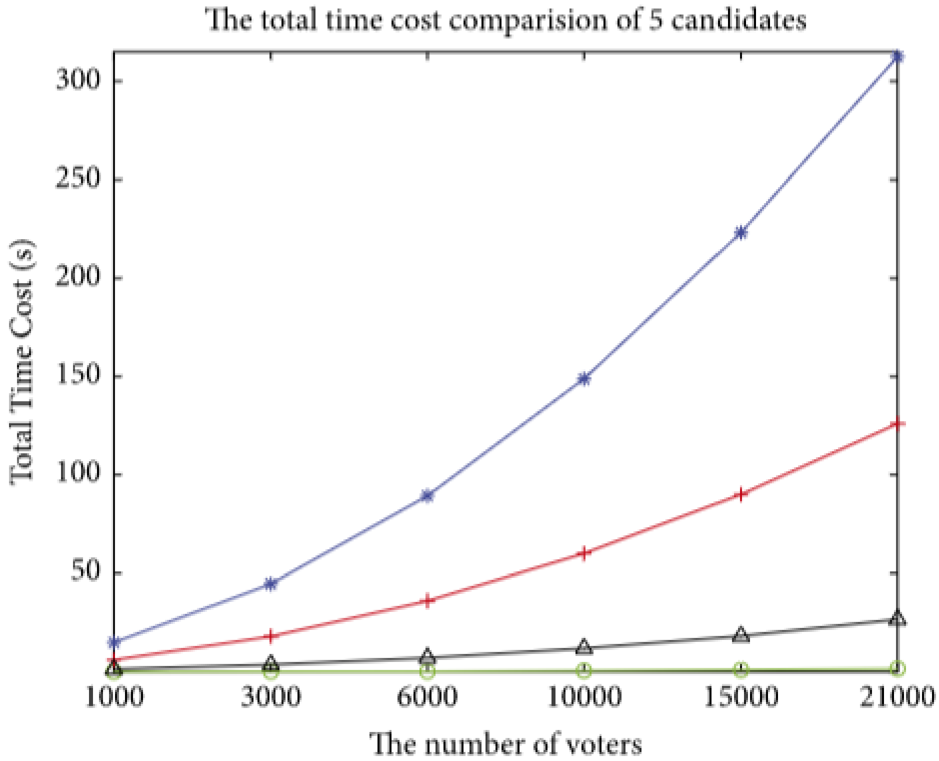

Figure 5.1. Performance Analysis of the Voting Phase

In the voting phase, the five steps are as follows: registering identification for voters, negotiating session keys among voters, generating masked values, constructing shared polynomials, and computing shares. Meanwhile, the computation cost mainly concentrates upon generating masked values and computing shares. Assume that the computation costs of one masked value and one share are separately expressed as costmask and costshare

Performance Analysis of the Postvoting Phase

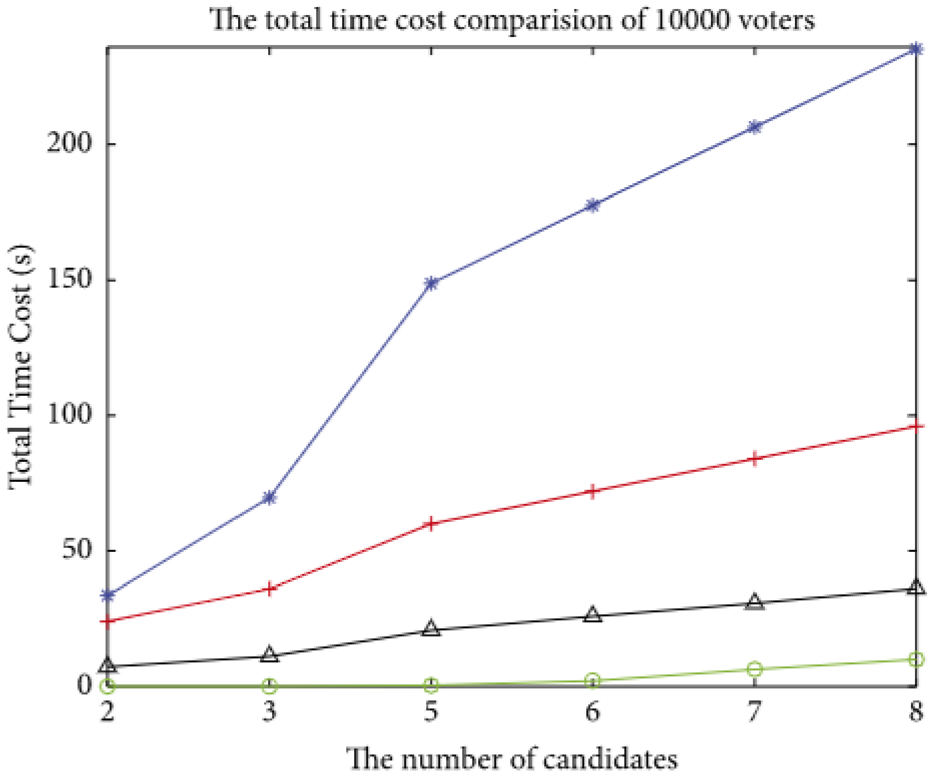

Figure 5.2. Performance Analysis of the Post-voting Phase

In postvoting phase, VS and candidates are responsible for computing the sum of shares and then publish. Each participant reconstructs a polynomial to obtain the tallying result and then verifies it. Meanwhile, computing the sum of shares, recovering polynomial, and verifying the tallying result are the main computation cost in this phase. Assume that they are separately expressed as costmask, costshare and costverify.

Conclusion

The idea of adapting digital voting systems to make the public electoral process cheaper, faster and easier, is a compelling one in modern society. Making the electoral process cheap and quick, normalizes it in the eyes of the voters, removes a certain power barrier between the voter and the elected official and puts a certain amount of pressure on the elected official. It also opens the door for a more direct form of democracy, allowing voters to express their will on individual bills and propositions.

In this project, we introduced a unique, blockchain-based electronic voting system that utilizes smart contracts to enable secure and cost-efficient election while guaranteeing voters privacy. We have outlined the systems architecture, the design, and a security analysis of the system.

Future Enhancement

In the future, it is aimed to simulate with a more realistic system, to operate the system from end to end, and to focus on optimizations for scalability of the system. Another future work is that in the proposed system the end of election is assumed to be depending on the system time. However, the system may be improved to increase the security of the time dimension. In our opinion, transition to the e-voting method should proceed slowly by implementing in small pilot populations first and then widening the scope slowly. The implementation of such voting systems still poses many challenges and risks for developers and governments.

APPENDIX 1

Source Codings

```
<%@ Master Language="C#" AutoEventWireup="true"
CodeFile="Main.master.cs" Inherits="Main" %>
<!DOCTYPE html>
<html xmlns="http://www.w3.org/1999/xhtml">
<head runat="server">
    <link href="Style/main.css" rel="stylesheet" />
    <title>Aadhaar based Voting System</title>
    <asp:ContentPlaceHolder id="head" runat="server">
    </asp:ContentPlaceHolder>
    <style type="text/css">
        .auto-style1 {
            text-align: center;
            text-decoration: underline;
        }
    </style>
</head>
<body>
    <form id="form1" runat="server">
        <div class = "page">
    <div id = "Header">
        <asp:Image ID="Image1" runat="server" Height="180px"
ImageAlign="Top" ImageUrl="~/Images/IndiaFlag.jpg" Width="1000px" />
        </div>
    <div><h2 class="auto-style1">Aadhaar Card Voting System</h2>
        </div>
            <div style = "margin : 0px auto 0px auto; width : 600px;">
    <asp:Menu ID="Menu1" runat="server" Orientation="Horizontal"
Width="800px" StaticSubMenuIndent="16px" StaticDisplayLevels="2"
ForeColor="#FF3300">
      <DynamicHoverStyle BackColor="White" ForeColor="#6600FF" />
      <Items>
        <asp:MenuItem Text="Home" Value="Home"
NavigateUrl="~/Home.aspx"></asp:MenuItem>
        <asp:MenuItem Text="Voter Login" Value="Voter Login"
NavigateUrl="~/VoterLogin.aspx"></asp:MenuItem>
        <asp:MenuItem Text="Voter Registration" Value="Voter
Registration" NavigateUrl="~/VoterRegistration.aspx"></asp:MenuItem>
        <asp:MenuItem Text="Candidate Information" Value="Candidate
Information" NavigateUrl="~/CandidateInfo.aspx"></asp:MenuItem>
        <asp:MenuItem Text="About UIDAI" Value="About UIDAI"
NavigateUrl="~/About.aspx"></asp:MenuItem>
        <asp:MenuItem Text="Results" Value="Results"
NavigateUrl="~/Results.aspx"></asp:MenuItem>
      </Items>
      <StaticMenuItemStyle HorizontalPadding="10px" />
    </asp:Menu></div>
  <div id = "contentpart">
    <asp:ContentPlaceHolder id="ContentPlaceHolder1" runat="server">
    </asp:ContentPlaceHolder>
    </div>
      <br />
      <br />
  <div id = "Footer">
```

```
        <asp:Image ID="Image2" runat="server" Height="138px"
ImageUrl="~/Images/UPES Logo.jpg" Width="143px" />
        <br />
        &copy Aadhaar based E-Voting System (December- 2017)
         </div>
</div>
    </form>
</body>
</html>
using System;
using System.Collections.Generic;
using System.Linq;
using System.Web;
using System.Web.UI;
using System.Web.UI.WebControls;
public partial class Main : System.Web.UI.MasterPage
{
    protected void Page_Load(object sender, EventArgs e)
    {
    }
}
<?xml version="1.0" encoding="utf-8"?>
<!-- For more information on using web.config transformation visit
http://go.microsoft.com/fwlink/?LinkId=125889 -->
<configuration xmlns:xdt="http://schemas.microsoft.com/XML-Document-
Transform">
  <!--
  In the example below, the "SetAttributes" transform will change the value
of
  "connectionString" to use "ReleaseSQLServer" only when the "Match"
locator
  finds an attribute "name" that has a value of "MyDB".
  <connectionStrings>
   <add name="MyDB"
    connectionString="Data Source=ReleaseSQLServer;Initial
Catalog=MyReleaseDB;Integrated Security=True"
    xdt:Transform="SetAttributes" xdt:Locator="Match(name)"/>
  </connectionStrings>
 -->
 <system.web>
  <compilation xdt:Transform="RemoveAttributes(debug)" />
  <!--
   In the example below, the "Replace" transform will replace the entire
   <customErrors> section of your web.config file.
   Note that because there is only one customErrors section under the
   <system.web> node, there is no need to use the "xdt:Locator" attribute.
   <customErrors defaultRedirect="GenericError.htm"
    mode="RemoteOnly" xdt:Transform="Replace">
    <error statusCode="500" redirect="InternalError.htm"/>
   </customErrors>
  -->
 </system.web>
</configuration>
```

REFERENCES

1. A. Ghosh, S. Gupta, A. Dua, and N. Kumar, “Security of Cryptocurrencies in blockchain technology: State-of-art, challenges and future prospects,” Journal of Network and Computer Applications, vol. 163, Article ID 102635, 2020.

2. K. Curran, “E-voting on the blockchain,” =e Journal of British Blockchain Association, vol. 1, no. 22–7, 2018.

3. M. Audi Ghaffari, An E-Voting System Based on Blockchain and Ring Signature, School of Computer Science University of Birmingham, Birmingham, UK, 2017.

4. M. G. Gurubasavanna, S. Ulla Shariff, R. Mamatha, and N. Sathisha, “Multimode authentication based electronic voting kiosk using raspberry pi,” in Proceedings of the International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud), I-SMAC, pp. 528–535, Palladam, India., September 2018.

5. S. Bai, G. Yang, J. Shi, G. Liu, and Z. Min, “Privacy-Preserving oriented floating-point number fully homomorphic encryption scheme,” Security and Communication Networks, vol. 2018, Article ID 2363928, 14 pages, 2018.

6. S. Komatineni and G. Lingala, “Secured E-voting system using two-factor biometric authentication,” in Proceedings of the 2020 Fourth International

Conference on Computing Methodologies and Communication (ICCMC), pp. 245–248, Iccmc, Erode, India, March 2020.

7. S. Shukla, A. N. *asmiya, D. O. Shashank, and H. R. Mamatha, “Online voting application using ethereum blockchain,” in 2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI), pp. 873–880, Bangalore, India, September 2018.

8. X. Yang, X. Yi, S. Nepal, A. Kelarev, and F. Han, “A Secure verifiable ranked choice online voting system based on homomorphic encryption”, IEEE Access, vol. 6, pp. 20506-20519, 2018.

9. Y. Abuidris, A. Hassan, A. Hadabi, and I. Elfadul, “Risks and opportunities of blockchain based on e-voting systems,” in Proceedings of the 2019 16th International Computer Conference on Wavelet Active Media Technology and Information Processing, pp. 365–368, Chengdu, China, December 2019.

10. Y. Mehmood, F. Ahmad, I. Yaqoob, A. Adnane, M. Imran, and S. Guizani, ``Internet-of-Things-based smart cities: Recent advances and challenges," IEEE Commun. Mag., vol. 55, no. 9, pp. 16-24, Sep. 2017.