SMART VOTE GUARD - AI FACIAL AND ID AUTHENTICATION

ST. TERESA'S COLLEGE (AUTONOMOUS)

AFFILIATED TO MAHATMA GANDHI UNIVERSITY

PROJECT REPORT

In partial fulfillment of the requirements for the award of the degree of

BCA (CLOUD TECHNOLOGY AND INFORMATION SECURITY MANAGEMENT)

By

Aayisha Natasha Shafik -SB21BCA001

&

E S Aparna - SB21BCA013

III DC BCA (CLOUD TECHNOLOGY AND INFORMATION SECURITY MANAGEMENT)

Under the guidance of

Mrs.Maria Neethu Titus

DEPARTMENT OF BCA (CLOUD TECHNOLOGY AND INFORMATION SECURITY MANAGEMENT)

MARCH 2024

SMARTVOTE GUARD - AI FACIAL & ID AUTHENTICATION

ST. TERESA'S COLLEGE (AUTONOMOUS)

AFFILIATED TO MAHATMA GANDHI UNIVERSITY

PROJECT REPORT

In partial fulfillment of the requirements for the award of the degree of

BCA (CLOUD TECHNOLOGY AND INFORMATION SECURITY MANAGEMENT)

By

Aayisha Natasha Shafik -SB21BCA001

&

E S Aparna - SB21BCA013

III DC BCA (CLOUD TECHNOLOGY AND INFORMATION SECURITY MANAGEMENT)

Under the guidance of

Mrs.Maria Neethu Titus

DEPARTMENT OF BCA (CLOUD TECHNOLOGY AND INFORMATION SECURITY MANAGEMENT)

MARCH 2024

DECLARATION

We, undersigned, hereby declare that the project report, **'SMART VOTE GUARD-AI FACIAL & ID AUTHENTICATION**", submitted for partial fulfillment of the requirements for the award of degree of BCA (Cloud Technology and Information Security Management) at St. Teresa's College (Autonomous), Ernakulam (Affiliated to Mahatma Gandhi University), Kerala, is a bonafide work done by us under the supervision of Mrs.Maria Neethu Titus. This submission represents our ideas in our own words and where ideas or words of others have not been included. We have adequately and accurately cited and referenced the original sources. We also declare that we have adhered to the ethics of academic honesty and integrity and have not misrepresented or fabricated any data or idea or fact or source in our submission. We understand that any violation of the above will be a cause for disciplinary action by the institute and/or the University and can also evoke penal action from the sources which have thus not been properly cited or from whom proper permission has not been obtained. This report has not been previously formed the basis for the award of any degree, diploma or similar title of any other University.

Ernakulam

March 2024

Aayisha Natasha Shafik – SB21BCA001

E S Aparna – SB21BCA013

ST. TERESA'S COLLEGE (AUTONOMOUS), ERNAKULAM

BCA (CLOUD TECHNOLOGY AND INFORMATION SECURITY MANAGEMENT)

DEPARTMENT OF BCA (CLOUD TECHNOLOGY AND INFORMATION SECURITY MANAGEMENT)

CERTIFICATE

This is to certify that the report entitled **"SMARTVOTE GUARD - AI FACIAL & ID AUTHENTICATION"**, submitted by Aayisha Natasha Shafik and ES Aparna to the Mahatma Gandhi University in partial fulfillment of the requirements for the award of the Degree of BCA (Cloud Technology and Information Security Management) is a bonafide record of the project work carried out by them under our guidance and supervision. This report in any form has not been submitted to any other University or Institute for any purpose.

ARCHANA MENON P

Head of the department

Internal Supervisor

ST. TERESA'S COLLEGE DEPT. OF COMPUTERS ERNAKULAM

External Supervisor

ACKNOWLEDGEMENT

First and foremost we thank God Almighty for his blessings. We take this opportunity to express our gratitude to all those who helped us in completing this project successfully. I wish to express our sincere gratitude to the **Manager Rev. Dr. Sr. Vinitha CSST** and the Principal **Dr. Lizzy Mathew** for providing all the facilities.

We express our sincere gratitude towards the Head of the department **Mrs. Archana Menon P** for the support. We deeply express sincere thanks to our project guide **Mrs. Maria Neethu Titus** for her proper guidance and support throughout the project work.

We are indebted to our beloved teachers whose cooperation and suggestion throughout the project helped us a lot. We thank all our friends and classmates for their support.

We convey our hearty thanks to our parents for the moral support, suggestion and encouragement.

ABSTRACT

The history of voting systems spans millennia, from the ancient practices of the Greeks to the innovations of medieval Venice and beyond. Over time, these systems have undergone significant evolution, transitioning from simple hand-written paper ballots to sophisticated online platforms. Despite advancements, many nations still rely on traditional ballot-based methods. Following the era of paper ballots and electronic voting machines, the pinnacle of technological advancement in voting systems is the digital or online voting platform, which aims for stringent validation and verification processes devoid of human intervention. An ideal digital voting system must accurately authenticate individuals and validate their identification documents.

In this project, we propose the development of an e-voting system integrating two modules: facial recognition and basic login credential verification. The facial recognition component will be constructed and trained using Python libraries, leveraging machine learning techniques such as HOG (Histogram of Oriented Gradients), CNN (Convolutional Neural Network), and KNN (K-Nearest Neighbors). Meanwhile, the Login credential verification module will employ basic python techniques incorporating a Mysql Database. It will be a two stage verification and validation process consisting of user credential validation, face recognition.

The entire system will feature a PyQT5-based User Interface and will be hosted locally for comprehensive testing with the database. By combining cutting-edge technology with robust validation processes, our e-voting solution aims to enhance the security, integrity, and accessibility of the voting process, ensuring a more democratic and reliable electoral system for the future.

TABLE OF CONTENTS

LIST OF FIGURES

Chapter 1
INTRODUCTION

The act of voting, a cornerstone of democratic governance, has evolved significantly throughout human history. From the direct democracy of ancient Athens to the representative republics of the modern era, the methods and technologies used to facilitate elections have undergone profound transformations. The origins of voting can be traced back to ancient civilizations such as Greece and Rome, where citizens gathered in assemblies to debate and decide on matters of public importance. Over time, these early forms of democratic participation gave rise to more structured electoral systems, including the use of paper ballots and mechanical voting machines. As societies advanced technologically, so too did their electoral processes, with the emergence of electronic and online voting platforms promising greater efficiency, accessibility, and transparency. Despite these advancements, modern electoral systems face a myriad of challenges and complexities. Security concerns loom large in an era of cyberattacks and digital manipulation, raising questions about the integrity and reliability of election results. Accessibility remains a persistent issue, with marginalized communities often facing barriers to participation due to physical disabilities, language barriers, or lack of access to polling locations. Ensuring the privacy and confidentiality of voter information is another critical consideration, as the digitization of voting processes introduces new risks of data breaches and privacy violations. In response to these challenges, there is a growing recognition of the need for advanced e-voting solutions that combine cutting-edge technology with robust security measures and user-friendly interfaces.

Facial recognition technology, for example, holds promise for enhancing the authentication and verification of voters, while image processing techniques can be used to validate identity documents and prevent fraudulent voting. User interface design also plays a crucial role in shaping the voting experience, with intuitive and accessible interfaces helping to engage voters and build trust in the electoral process. As we navigate the complexities of modern democracy, the development and implementation of advanced e-voting systems represent a pivotal step forward in ensuring fair, transparent, and inclusive elections. By harnessing the power of technology to overcome barriers and enhance security, these systems have the potential to strengthen the foundations of democracy and empower citizens to participate fully in the governance of their societies. However, their success ultimately depends on the careful balance of innovation, regulation, and public trust, as we strive to

create electoral systems that are both effective and resilient in the face of evolving threats and challenges.

1.1 THE HISTORY OF VOTING

Origins of Voting:

Ancient Greece, particularly Athens, stands as the cradle of democracy where the concept of citizen participation in governance took root. In the Athenian democracy, eligible citizens convened in the Assembly to make collective decisions on legislative matters, executive appointments, and policy initiatives. This direct form of democracy, albeit limited to male citizens and excluding women, slaves, and foreigners, relied on various voting methods such as a show of hands or casting pebbles into urns. These rudimentary techniques underscored a communal approach to decision-making, emphasizing consensus-building and civic engagement.

Innovations in Electoral Systems:

During the medieval period, the Republic of Venice pioneered a distinctive model of representative governance, offering insights into the evolution of electoral systems. The Venetian Great Council, composed of noble families, played a central role in the selection of the Doge, the highest-ranking official in the city-state. Unlike the direct democracy of ancient Athens, Venice embraced a system of indirect elections characterized by a complex process of nomination, scrutiny, and approval. This method aimed to balance competing interests and factions within the ruling elite, reflecting a pragmatic approach to governance that prioritized stability and continuity. The historical perspectives of ancient Greek democracy and the medieval Venetian Republic underscore the diversity and evolution of electoral systems over time. These foundational models highlight the varying approaches to citizen participation, decision-making processes, and governance structures across different societies and eras. From the direct democracy of Athens to the representative governance of Venice, the principles of accountability, legitimacy, and inclusivity have remained central to the development of electoral systems throughout history. By examining the origins and innovations of voting practices, we gain a deeper understanding of the complexities and challenges inherent in modern democratic processes. Furthermore, these historical precedents offer valuable lessons for contemporary debates surrounding electoral reform and democratic governance. As societies grapple with issues of political participation,

representation, and accountability, there is a renewed emphasis on designing electoral systems that are transparent, inclusive, and responsive to the needs of diverse populations. By drawing upon the rich tapestry of historical experiences, policymakers, scholars, and citizens can inform and shape the future of democracy, ensuring that electoral processes remain relevant, resilient, and equitable in an ever-changing world.

In contrast to the direct democracy of ancient Athens, the Republic of Venice during the medieval period developed a unique model of representative governance. Venice, situated on a network of islands in the Adriatic Sea, emerged as a maritime power and established a republican form of government characterized by a complex system of checks and balances. At the heart of Venetian governance was the Venetian Great Council, a deliberative assembly composed of noble families known as patricians. The Great Council played a central role in the selection of the Doge, the highest-ranking official in the Venetian Republic. Unlike the direct participation of citizens in Athenian democracy, Venice embraced an indirect form of governance where elected representatives acted on behalf of the populace. The Doge, elected for life, served as the head of state and commander-in-chief of the Venetian armed forces. However, the power of the Doge was tempered by the Council of Ten, a secretive body responsible for overseeing state security and intelligence. Through a system of nomination, scrutiny, and approval, the Venetian Republic sought to balance the interests of competing factions within the ruling elite while maintaining stability and continuity in government. This intricate system of governance contributed to Venice's longevity as a republic and its reputation as a center of commerce, culture, and diplomacy in medieval Europe.

1.2. Traditional Voting Methods

The introduction of hand-written paper ballots in the 19th century marked a significant milestone in the democratization of voting, providing a tangible means of recording voter preferences. With paper ballots, voters could mark their choices, which were then collected and manually counted by election officials. While paper ballots offered a transparent and auditable record of the voting process, they were vulnerable to tampering, fraud, and logistical challenges, particularly in large-scale elections. Despite these limitations, paper-based voting remained the predominant method well into the modern era, reflecting its simplicity and accessibility for voters.

The advent of mechanical voting machines in the late 19th and early 20th centuries represented a technological leap forward in electoral practices, promising greater efficiency and accuracy compared to manual counting methods. These machines, equipped with levers, dials, or punch cards, allowed voters to register their choices mechanically, streamlining the voting process. Mechanical voting machines offered advantages in reducing errors and disputes associated with manual counting, enhancing the integrity of election results. However, their widespread adoption was hampered by high production costs, maintenance requirements, and concerns about reliability and security. Despite these challenges, mechanical voting machines played a significant role in modernizing electoral systems and paving the way for future innovations in voting technology.

Hand-Written Paper Ballots:

The introduction of hand-written paper ballots in the 19th century marked a significant milestone in the evolution of voting systems, offering a tangible means of recording voter preferences. Voters would mark their choices on paper ballots, which were then collected and manually counted by election officials. While paper ballots provided a transparent and auditable record of the voting process, they were susceptible to tampering, fraud, and logistical challenges in large-scale elections. Despite these limitations, paper-based voting remained the dominant method well into the modern era.

Mechanical Voting Machines:

The advent of mechanical voting machines in the late 19th and early 20th centuries represented a technological leap forward in electoral practices. These machines featured levers, dials, or punch cards, allowing voters to register their choices mechanically. Mechanical voting machines promised greater efficiency and accuracy compared to manual counting methods, reducing the likelihood of errors and disputes. However, their widespread adoption was hindered by high production costs, maintenance requirements, and concerns about reliability and security.

The transition from hand-written paper ballots to mechanical voting machines reflects the ongoing quest for efficiency, accuracy, and accessibility in electoral processes. While traditional voting methods have served as the foundation of democratic governance for centuries, they have also posed challenges in ensuring the integrity and transparency of elections. The evolution of voting

technology highlights the dynamic interplay between innovation and regulation, as policymakers and election officials seek to balance the benefits of technological advancements with the need to safeguard against potential risks and vulnerabilities. As societies continue to embrace digitalization and automation in electoral systems, the lessons learned from traditional voting methods remain relevant in guiding the development of secure, inclusive, and resilient democratic processes.

1.3. Transition to Digital Voting Systems

Emergence of Electronic Voting Machines

Electronic voting machines (EVMs) emerged as a modern alternative to mechanical voting systems, leveraging digital technology to streamline the voting process. EVMs featured digital displays and buttons, enabling voters to cast their ballots electronically. This transition promised greater speed, accuracy, and accessibility in elections, particularly for voters with disabilities. Despite their advantages, EVMs faced criticism over security vulnerabilities, reliability issues, and the lack of a paper trail, raising concerns about the integrity and transparency of election results. Electronic voting machines (EVMs) emerged as a modern alternative to mechanical voting systems, harnessing digital technology to streamline the voting process. Equipped with digital displays and buttons, EVMs enabled voters to cast their ballots electronically, promising greater speed, accuracy, and convenience in elections. This technological advancement was particularly beneficial for voters with disabilities, who could now participate more fully in the electoral process. Despite their potential advantages, EVMs faced criticism over security vulnerabilities, reliability issues, and the lack of a paper trail, raising concerns about the integrity and transparency of election results. The reliance on electronic systems without a verifiable paper record raised questions about the auditability and accountability of voting processes, fueling debates over the adoption of more secure and transparent voting technologies. Nonetheless, EVMs represented a significant step forward in modernizing electoral systems and improving the efficiency of vote counting and tabulation.

Adoption of Online Voting Platforms

The rise of the internet ushered in a new era of online voting platforms, offering voters the convenience of casting their ballots remotely from any internet-enabled device. Online voting promised to overcome geographical barriers, increase voter turnout, and reduce costs associated with traditional polling stations. However, the widespread adoption of online voting has been hindered by security concerns, privacy risks, and challenges in ensuring the integrity of the voting process. Despite ongoing efforts to address these issues, online voting remains a subject of debate and experimentation in electoral reform.

Despite these challenges, online voting remains a subject of debate and experimentation in electoral reform, with proponents advocating for its potential to expand access to voting and enhance civic engagement. Efforts to address security concerns and privacy risks have led to the development of encryption protocols, multi-factor authentication, and blockchain technology to safeguard the integrity of online voting systems. However, questions remain about the scalability, accessibility, and inclusivity of online voting, particularly for marginalized communities with limited access to technology or internet connectivity.

The transition to digital voting systems reflects a broader trend towards digitalization and automation in electoral processes, driven by advancements in technology and changing expectations of voters. While digital voting systems offer the promise of greater efficiency, accessibility, and convenience, they also pose challenges in ensuring the security, integrity, and transparency of elections. As societies continue to grapple with these complex issues, policymakers, election officials, and technologists must work together to strike a balance between innovation and regulation, ensuring that digital voting systems uphold the principles of fairness, accuracy, and trustworthiness in democratic governance.

1.4 Challenges in Modern Electoral Systems

Security Concerns and Vulnerabilities

Modern electoral systems face an array of security threats and vulnerabilities, ranging from cyberattacks and hacking attempts to insider manipulation and tampering. The digitization of voting processes has introduced new risks, such as malware infections, data breaches, and denial-

of-service attacks, which can compromise the confidentiality, integrity, and availability of election systems. Addressing these security challenges requires robust cybersecurity measures, including encryption, intrusion detection, and audit trails, to safeguard the electoral process from external threats and internal vulnerabilities.

Accessibility and Inclusivity

Despite advancements in technology, many voters continue to encounter barriers to participation in the electoral process, particularly those with disabilities, language barriers, or limited access to polling locations. Ensuring equitable access to voting requires proactive measures to accommodate diverse needs and preferences, such as providing accessible polling stations, alternative voting methods, and voter education initiatives. By promoting inclusivity and accessibility, electoral authorities can enhance voter engagement, representation, and trust in the democratic process.

Ensuring Voter Privacy and Confidentiality

Protecting voter privacy is paramount in maintaining the integrity and legitimacy of electoral processes. Safeguarding the confidentiality of voter information and ballot choices helps prevent coercion, intimidation, or undue influence, ensuring that individuals can express their political preferences freely and anonymously. Electoral authorities must implement robust data protection measures, such as encryption, anonymization, and access controls, to safeguard voter data from unauthorized disclosure or misuse. By upholding principles of privacy and confidentiality, electoral authorities can uphold the trust and confidence of voters in the democratic process.

Chapter 2

LITERATURE SURVEY

The literature survey has been conducted on papers from leading publications and conferences such as IEEE, nature, sprinkler, and a few other journals like Journal of Computational Intelligence and Informatics. The keywords used are mainly 'smart voting', e-voting, 'facial recognition', and 'ID verification'.

Sakshi et al. propose a pioneering approach to implementing facial recognition technology in smart voting systems by leveraging machine learning algorithms. Their research focuses on developing a robust facial recognition system capable of accurately identifying voters during the voting process. By harnessing the power of machine learning, the proposed system achieves high levels of accuracy and reliability in authenticating voter identities, thereby enhancing the security and integrity of elections. The study demonstrates the feasibility and effectiveness of integrating machine learning techniques into smart voting systems, paving the way for more advanced and sophisticated voter authentication methods [1].

Li et al. present a comprehensive study on the design and implementation of a secure online voting system that incorporates facial recognition and ID card verification mechanisms. The research focuses on leveraging advanced cryptographic techniques to ensure the confidentiality and integrity of voter data, while biometric authentication methods authenticate voter identities and prevent fraudulent voting activity. The study highlights the importance of robust security measures in online voting systems and demonstrates the effectiveness of combining multiple authentication methods to enhance system security and reliability.

Gupta and Sharma explore the potential of blockchain technology in smart voting systems, proposing a decentralized voting platform that integrates facial recognition and ID card verification. Their research emphasizes the use of blockchain technology to ensure transparency, immutability, and tamper-resistance of voting records, while biometric authentication methods authenticate voter identities and prevent unauthorized access. The study highlights the benefits of blockchain-based voting systems in addressing security and trust issues in electoral processes, paving the way for more transparent and trustworthy elections [6].

Khan et al. investigate the usability and acceptance of smart voting systems among voters through a comprehensive survey study. The research assesses the perceptions and attitudes of voters towards smart voting systems equipped with facial recognition and ID card verification features. The findings reveal positive attitudes towards the adoption of smart voting systems, with voters expressing confidence in the security and reliability of biometric authentication methods. The study provides valuable insights into voter preferences and expectations regarding the adoption of advanced technologies in the electoral process.[7] Patel and Desai propose a novel approach to enhancing voter authentication in smart voting systems by integrating facial recognition technology with blockchain technology. Their research focuses on leveraging the transparency and immutability of blockchain to securely store biometric data used for facial recognition, thereby enhancing the security and privacy of voter authentication processes. The study demonstrates the feasibility and effectiveness of combining facial recognition and blockchain technology to ensure secure and trustworthy elections [8]. Wang and Zhang investigate privacy-preserving techniques for facial recognition in smart voting systems. Their research focuses on developing algorithms and protocols that protect the privacy of voter biometric data while ensuring accurate and reliable facial recognition. The study explores cryptographic techniques such as secure multiparty computation and homomorphic encryption to enable privacy-preserving facial recognition in voting systems. The findings contribute to the development of more privacy-friendly solutions for biometric authentication in electoral processes [9].

Chen and Wu propose a scalable facial recognition system designed specifically for large-scale smart voting platforms. Their research focuses on developing efficient algorithms and architectures that can handle the computational demands of facial recognition in high-volume voting environments. The study explores parallel computing techniques, distributed processing frameworks, and cloud-based infrastructure to achieve scalability and performance in facial recognition systems for smart voting platforms. The findings provide valuable insights into optimizing facial recognition technology for use in large-scale electoral processes [10]. Park and Kim present a real-time facial recognition system tailored for smart voting kiosks deployed in public locations. Their research focuses on developing lightweight algorithms and hardware implementations that can perform facial recognition quickly and accurately in resource-constrained environments. The study explores techniques such as deep learning-based feature extraction, edge computing, and optimized hardware acceleration to enable real-time facial recognition on smart voting kiosks. The findings contribute to the development of user-friendly and efficient biometric authentication solutions for public voting systems [11]. Garcia and Rodriguez

propose a secure voting system that combines facial recognition with multi-modal biometric authentication methods. Their research focuses on integrating facial recognition with other biometric modalities such as fingerprint recognition, iris recognition, and voice recognition to enhance the security and reliability of voter authentication. The study explores fusion techniques and decision-making algorithms to combine multiple biometric modalities effectively and achieve robust authentication in voting systems. The findings demonstrate the effectiveness of multi-modal biometric authentication in enhancing the security and trustworthiness of elections [12].

Chapter 3

EXISTING SYSTEMS

Voting has become a common practice since ancient Greece and Athens. From that period to the current age of digital technologies, the methods and technologies have been in a phase of great evolution that passed through ballot paper voting to mechanical voting machines to electrical machines to online voting platforms. All these systems have their own advantages and disadvantages. So, most of them are still in use.

3.1 Ballot paper voting system:

The introduction of hand-written paper ballots in the 19th century marked a significant milestone in the evolution of voting systems, ushering in a new era of democratic participation and electoral accountability. Prior to the widespread adoption of paper ballots, voting methods varied widely across different regions and cultures, often relying on oral declarations or physical tokens to indicate voter preferences. The introduction of paper ballots standardized the voting process, providing a tangible means of recording and tallying voter choices in a transparent and auditable manner.

Paper ballots offered several advantages over previous voting methods, including increased accuracy, reliability, and accessibility for voters of diverse backgrounds. Unlike oral voting, which relied on memory and verbal testimony, paper ballots provided a permanent record of voter preferences, facilitating the accurate counting and verification of election results. Moreover, paper ballots allowed for greater flexibility and inclusivity in the voting process, enabling voters to cast their ballots in private and without fear of coercion or intimidation.

However, the transition to paper ballots was not without its challenges. In many cases, the design and distribution of ballots were subject to manipulation and fraud, with political parties and candidates often seeking to gain an advantage through tactics such as ballot stuffing, voter suppression, and intimidation. Moreover, the manual counting and tabulation of paper ballots were labor-intensive and time-consuming, leading to delays and disputes in the reporting of election

outcomes. Despite these limitations, paper-based voting remained the dominant method well into the modern era, reflecting its simplicity and accessibility for voters of all ages and literacy levels.

As societies grappled with issues of electoral integrity and accountability, efforts were made to improve the security and reliability of paper ballots through innovations such as standardized ballot designs, tamper-evident seals, and chain-of-custody protocols. Moreover, the adoption of mechanical voting machines in the late 19th and early 20th centuries represented a further advancement in the evolution of voting technology, offering the promise of greater efficiency and accuracy in electoral processes.

Advantages of Ballot Paper Voting:

1. **Transparency and Accountability:** Ballot paper voting offers a transparent and easily verifiable method for recording voter preferences. Each voter marks their choices directly on the paper ballot, which can then be visually inspected and manually counted by election officials and observers. This transparency helps to ensure the integrity of the electoral process and build trust in the outcome of elections.
2. **Accessibility:** Ballot paper voting is accessible to a wide range of voters, including those with limited technological literacy or disabilities. Voters are familiar with the process of marking paper ballots, making it a straightforward and inclusive method of voting. Additionally, paper ballots can be provided in multiple languages and formats to accommodate diverse voter needs.
3. **Security:** Paper ballots provide a physical record of each voter's choices, reducing the risk of tampering or manipulation. By storing voter preferences in a tangible form, ballot paper voting helps to safeguard against electronic hacking or cyberattacks that may compromise the integrity of electronic voting systems.
4. **Auditability:** In the event of disputes or recounts, paper ballots can be manually recounted to verify the accuracy of election results. This auditability ensures that any discrepancies or irregularities can be identified and addressed, helping to maintain public confidence in the electoral process.

Disadvantages of Ballot Paper Voting:

1. **Time-Consuming:** Counting paper ballots manually can be a time-consuming process, particularly in large-scale elections with a high voter turnout. The need to sort, tally, and verify paper ballots can delay the reporting of election results and increase the likelihood of errors or inaccuracies in the tabulation process.
2. **Logistical Challenges:** Distributing, collecting, and storing paper ballots presents logistical challenges for election administrators, particularly in remote or geographically dispersed areas. Ensuring the security and integrity of paper ballots throughout the voting process requires careful planning and coordination.
3. **Potential for Fraud:** While paper ballots offer a physical record of voter preferences, they are not immune to fraud or manipulation. Ballot stuffing, tampering with ballots, and other forms of electoral fraud can occur if proper security measures are not in place to safeguard the integrity of the voting process.
4. **Environmental Impact:** Ballot paper voting requires the production and disposal of large quantities of paper, which can have environmental consequences. The printing and transportation of paper ballots contribute to carbon emissions and resource consumption, highlighting the need for sustainable voting practices.

3.2 Mechanical Voting Machines:

The advent of mechanical voting machines represented a technological leap forward in electoral practices, revolutionizing the way in which votes were cast, counted, and tabulated. Unlike hand-written paper ballots, which required manual counting by election officials, mechanical voting machines enabled voters to register their choices mechanically, thereby reducing the likelihood of errors and disputes in the tabulation of election results.

Mechanical voting machines came in a variety of designs and configurations, but they typically featured levers, dials, or punch cards that voters would manipulate to indicate their preferences. These machines offered several advantages over traditional paper ballots, including increased speed, efficiency, and accuracy in the recording and tabulation of votes. Moreover, mechanical voting machines provided a more user-friendly voting experience for voters of all ages and abilities, with intuitive interfaces and clear instructions guiding voters through the voting process.

Despite their potential advantages, mechanical voting machines also faced criticism and controversy. Concerns were raised about the security and reliability of these machines, particularly in light of reports of malfunctions, tampering, and manipulation in some elections. Moreover, the cost of purchasing, maintaining, and operating mechanical voting machines could be prohibitive for many jurisdictions, leading to disparities in access to modern voting technology.

In response to these challenges, efforts were made to improve the security and reliability of mechanical voting machines through innovations such as voter-verified paper audit trails (VVPATs), which provided a paper record of each voter's choices for verification purposes. Moreover, advancements in technology, such as the development of electronic voting machines (EVMs), offered new opportunities for improving the accessibility, efficiency, and transparency of electoral processes. However, the transition from mechanical voting machines to electronic voting systems was not without its own set of challenges, including concerns about cybersecurity, privacy, and the integrity of election results.

One of the most common types of mechanical voting machines was the lever-operated machine. These machines consisted of a series of levers, each corresponding to a different candidate or ballot measure. To cast a vote, voters would enter a private booth and pull down the lever next to their chosen candidate or option. This action would mechanically record the vote and advance the internal counters, ensuring that each voter could only cast one vote per race.

Another type of mechanical voting machine was the dial-operated machine. Instead of levers, these machines featured a rotating dial or wheel with numbered positions corresponding to candidates or options. Voters would turn the dial to the desired position for each race, registering their votes as they progressed through the ballot. Once the voter completed their selections, they would typically pull a lever or push a button to cast their vote and reset the machine for the next voter.

Punch card voting machines were also prevalent in some regions. These machines utilized punch cards similar to those used in early computer systems. Voters would use a stylus to punch holes next to their chosen candidates or options on a paper punch card. The card would then be inserted into the voting machine, where mechanical sensors would detect the punched holes and tally the votes accordingly.

Mechanical voting machines offered several advantages over traditional paper ballots. They provided a more intuitive and user-friendly voting experience, with clear instructions and visual indicators guiding voters through the process. Additionally, mechanical machines reduced the risk of errors and discrepancies in vote counting, as the mechanical mechanisms ensured that each vote was recorded accurately and consistently.

However, mechanical voting machines also had their limitations and drawbacks. Maintenance and upkeep of the machines could be costly and time-consuming, requiring regular inspection, calibration, and repair to ensure proper functionality. Moreover, the physical size and weight of mechanical machines made them cumbersome to transport and set up, particularly in areas with limited resources or infrastructure.

Despite these challenges, mechanical voting machines played a significant role in modernizing electoral systems and increasing the efficiency and accuracy of vote counting and tabulation. Their introduction paved the way for further innovations in voting technology, including electronic voting machines (EVMs), which would eventually replace mechanical systems in many jurisdictions.

Advantages of Mechanical Voting Machines:

1. **Accuracy:** Mechanical voting machines are designed to record and tabulate votes accurately, reducing the likelihood of errors or discrepancies in the voting process. The mechanical mechanisms used in these machines ensure that each vote is registered and counted reliably, leading to more accurate election results.
2. **Efficiency:** Mechanical voting machines streamline the voting process, allowing voters to cast their ballots quickly and efficiently. With clear instructions and intuitive interfaces, voters can navigate the voting process with ease, reducing wait times and congestion at polling stations.
3. **Accessibility:** Mechanical voting machines are accessible to a wide range of voters, including those with disabilities or limited literacy. The tactile interfaces and visual cues used in these machines make them user-friendly for voters of all abilities, ensuring that everyone can participate in the electoral process.

4. **Privacy:** Mechanical voting machines provide voters with a private and confidential voting experience. By casting their ballots in a private booth and using mechanical controls to register their choices, voters can ensure that their votes remain anonymous and free from external influence.

Disadvantages of Mechanical Voting Machines:

1. **Cost:** The initial cost of purchasing and deploying mechanical voting machines can be prohibitively expensive for many jurisdictions. Additionally, ongoing maintenance and repair costs can add to the long-term expenses associated with these machines, making them financially burdensome for some election authorities.
2. **Limited Flexibility:** Mechanical voting machines are designed for specific types of elections and voting procedures, limiting their flexibility and adaptability to changing electoral needs. Upgrading or modifying these machines to accommodate new voting methods or technologies can be challenging and costly.
3. **Vulnerability to Malfunction:** Mechanical voting machines are susceptible to mechanical failures, malfunctions, and wear and tear over time. If not properly maintained or calibrated, these machines may produce inaccurate or unreliable results, undermining the integrity and trustworthiness of the electoral process.
4. **Lack of Transparency:** Unlike paper-based voting methods, which provide a physical record of each voter's choices, mechanical voting machines do not produce a tangible audit trail. This lack of transparency makes it difficult to verify the accuracy of election results or conduct recounts in the event of disputes or irregularities.

3.3 Electronic Voting Machines (EVMs):

Electronic Voting Machines (EVMs) represent a significant advancement in the modernization of electoral processes, offering a technologically sophisticated alternative to traditional paper-based voting methods. EVMs utilize electronic components and software to facilitate the casting, recording, and tabulation of votes, streamlining the voting process and enhancing the accuracy and efficiency of election administration.

In addition to enhancing the voting experience for voters, EVMs also offer several advantages for election administrators. The electronic recording and tabulation of votes reduce the risk of errors and discrepancies associated with manual counting, leading to more accurate and reliable election results. Moreover, EVMs can generate detailed reports and statistics on voter turnout, demographics, and voting patterns, providing valuable insights for election analysis and planning.

Despite these advantages, EVMs also face challenges and concerns related to security, reliability, and transparency. Critics have raised questions about the vulnerability of EVMs to hacking, tampering, and technical malfunctions, which could potentially compromise the integrity of election results. Additionally, the lack of a verifiable paper trail with some EVM models has raised concerns about the auditability and transparency of electronic voting systems. In response to these concerns, election authorities and technology developers have implemented various security measures and safeguards to protect the integrity of EVMs. These measures include encryption protocols, tamper-evident seals, and rigorous testing and certification processes to ensure that EVMs meet stringent security standards. Furthermore, some jurisdictions have adopted hybrid voting systems that combine electronic voting with paper audit trails, providing an additional layer of transparency and accountability.

Overall, electronic voting machines have the potential to revolutionize the way elections are conducted, offering a more efficient, accessible, and accurate method for casting and tabulating votes. However, ensuring the security and integrity of EVMs remains a critical priority for election authorities and policymakers, as they strive to uphold the principles of democracy and public trust in the electoral process.

Technical Details of Electronic Voting Machines (EVMs):

Electronic Voting Machines (EVMs) employ a combination of hardware and software components to facilitate the electronic recording and tabulation of votes. These machines are typically composed of several key elements, each serving a specific function in the voting process.

1. **Control Unit:** The control unit serves as the central processing unit (CPU) of the EVM and is responsible for coordinating the various functions of the machine. It contains the necessary electronics and firmware to control the operation of the EVM, including user

interfaces, data storage, and communication interfaces. The control unit is equipped with built-in security features to protect against unauthorized access and tampering.

2. **Ballot Unit:** The ballot unit is the interface through which voters cast their ballots on the EVM. It typically consists of a touchscreen display or a set of push-button controls, along with indicators and feedback mechanisms to guide voters through the voting process. The ballot unit is designed to be intuitive and user-friendly, with clear instructions and prompts to help voters navigate the voting interface.
3. **Memory Devices:** EVMs utilize various types of memory devices to store data, including read-only memory (ROM) for storing firmware and software programs, random-access memory (RAM) for temporary data storage during operation, and non-volatile memory (e.g., flash memory) for storing voting data and audit logs. These memory devices are protected by encryption and access control mechanisms to prevent unauthorized tampering or data manipulation.
4. **Security Features:** EVMs incorporate a range of security features to protect against tampering, fraud, and unauthorized access. These features may include physical security measures such as tamper-evident seals and locking mechanisms, as well as electronic security measures such as cryptographic algorithms, digital signatures, and secure boot processes. Additionally, EVMs may employ biometric authentication and multi-factor authentication methods to verify the identity of election officials and prevent unauthorized access to sensitive components.
5. **Communication Interfaces:** EVMs are equipped with communication interfaces to facilitate the transmission of voting data and election results to central tabulation centers. These interfaces may include wired connections (e.g., Ethernet, USB) or wireless connections (e.g., Wi-Fi, cellular) depending on the deployment environment and security requirements. Data transmission is encrypted to ensure the confidentiality and integrity of voting data during transit.
6. **Auditing and Logging:** EVMs generate detailed audit logs and event logs to track system activity and detect any anomalies or irregularities. These logs record information such as voter interactions, system events, and error conditions, providing a comprehensive record of the voting process for audit and analysis purposes.

Additionally, EVMs may incorporate built-in self-testing mechanisms to verify the integrity and functionality of critical system components before and during elections.

7. **Accessibility Features:** EVMs are designed to be accessible to voters of all abilities, including those with disabilities or special needs. Accessibility features may include adjustable font sizes, audio prompts and cues, tactile feedback, and alternative input methods (e.g., sip-and-puff devices, adaptive switches). These features ensure that all voters can participate in the electoral process independently and confidentially.

Advantages of Electronic Voting Machines (EVMs):

1. **Accuracy:** EVMs offer high levels of accuracy in recording and tabulating votes, reducing the risk of human error associated with manual counting of paper ballots. The electronic recording of votes minimizes the chances of misinterpretation or miscounting, leading to more reliable election results.
2. **Efficiency:** Electronic voting machines streamline the voting process, allowing for quicker and more efficient elections. Voters can cast their ballots swiftly, and the electronic tabulation of votes speeds up the counting process, enabling faster reporting of election results.
3. **Accessibility:** EVMs are designed to be accessible to a wide range of voters, including those with disabilities or special needs. Features such as touchscreen interfaces, audio prompts, and adjustable font sizes make it easier for voters of all abilities to cast their ballots independently and confidentially.
4. **Security:** EVMs incorporate various security features to protect against tampering, fraud, and unauthorized access. Encryption protocols, secure boot processes, and physical security measures help safeguard the integrity and confidentiality of voting data, ensuring the security of the electoral process.
5. **Transparency:** EVMs provide a transparent and auditable record of the voting process, with detailed audit logs and event logs tracking system activity and detecting any anomalies or irregularities. This transparency helps build trust in the integrity of election results and facilitates post-election audits and recounts.

Disadvantages of Electronic Voting Machines (EVMs):

1. **Vulnerability to Hacking:** EVMs are susceptible to hacking and cyberattacks, which could compromise the integrity and security of election results. Malicious actors may exploit vulnerabilities in EVM software or hardware to manipulate votes or disrupt the electoral process.
2. **Reliability Concerns:** Electronic voting machines may experience technical malfunctions or glitches, leading to potential errors or inaccuracies in the recording or tabulation of votes. Hardware failures, software bugs, or connectivity issues could undermine the reliability and trustworthiness of EVMs during elections.
3. **Lack of Voter Confidence:** Despite their security features, EVMs may face skepticism and distrust from voters who are concerned about the transparency and integrity of electronic voting systems. The lack of a verifiable paper trail in some EVM models has raised doubts about the auditability and accuracy of election results.
4. **Cost and Maintenance:** The initial cost of purchasing and deploying electronic voting machines can be significant, particularly for cash-strapped election authorities with limited resources. Additionally, ongoing maintenance, upgrades, and training expenses can further strain budgets and resources over time.
5. **Digital Divide:** EVMs rely on electronic technology, which may pose accessibility challenges for voters who lack access to or familiarity with digital devices. The digital divide between urban and rural areas, as well as disparities in internet connectivity and technology literacy, could exacerbate inequalities in electoral participation.

3.4 Online voting platforms:

Online voting platforms have garnered increasing attention as a potential solution to modernize and streamline the electoral process. By leveraging internet technologies, these platforms enable voters to cast their ballots remotely from any internet-enabled device, such as computers, smartphones, or tablets. The accessibility offered by online voting platforms is unparalleled, allowing voters to participate in elections from the comfort of their homes or anywhere with an internet connection. This accessibility is particularly beneficial for individuals with mobility issues, disabilities, or those residing in remote or inaccessible locations.

Moreover, online voting platforms offer undeniable convenience by eliminating the need for physical polling stations and long queues. With online voting, voters can cast their ballots at any time during the designated voting period, reducing barriers to participation and potentially increasing voter turnout. Additionally, online voting can lead to significant cost savings for election administration and management. By leveraging existing internet infrastructure and digital technologies, online voting platforms offer a cost-effective alternative to traditional paper-based methods.

However, despite these advantages, online voting platforms also present significant challenges and concerns. Chief among these is the issue of security risks. Online voting platforms are vulnerable to various security threats, including hacking, cyberattacks, and tampering. Malicious actors may attempt to compromise the integrity and confidentiality of the voting process by exploiting vulnerabilities in software, networks, or user devices. Ensuring the security and integrity of online voting systems is paramount to maintaining trust and confidence in the electoral process.

Furthermore, privacy concerns loom large in the context of online voting. The transmission of electronic ballots over the internet raises questions about the privacy and confidentiality of voter information. Without robust encryption and protection measures, electronic ballots may be susceptible to interception or surveillance, undermining the privacy rights of voters. Building trust in online voting platforms requires a rigorous commitment to protecting the privacy of voter data and ensuring the confidentiality of the voting process.

Moreover, online voting platforms must address the digital divide to ensure inclusivity and equal access to the electoral process. Disparities in digital access and literacy, particularly among marginalized or underserved communities, could disenfranchise certain groups of voters and undermine the fairness and integrity of elections. Bridging the digital divide requires concerted efforts to expand internet access, improve digital literacy, and provide support for those who may face barriers to participating in online voting. Overall, while online voting platforms offer potential benefits in terms of accessibility, convenience, and cost-effectiveness, addressing the challenges of security, privacy, and inclusivity is essential to realizing the full potential of online voting in shaping the future of democratic governance.

At the core of online voting platforms are robust encryption algorithms and cryptographic protocols that safeguard the confidentiality and integrity of voter data. Encryption technologies ensure that electronic ballots and transmission channels are protected from interception or tampering by unauthorized parties. Secure communication protocols, such as SSL/TLS, are employed to encrypt data transmitted between voters' devices and the voting server, ensuring that sensitive information remains confidential during transit.

Additionally, online voting platforms utilize sophisticated authentication mechanisms to verify the identity of voters and prevent unauthorized access to the voting system. Multi-factor authentication methods, such as passwords, biometric verification, and one-time passcodes, help authenticate voters' identities and protect against fraudulent voting activity. Advanced authentication techniques, such as cryptographic digital signatures and public-key infrastructure (PKI), ensure the integrity and authenticity of voting transactions.

Chapter 4

PROPOSED SYSTEM

4.1 Demand and requirement:

The demand for an end-to-end system with several verification stages is there because of the vulnerabilities of current online voting systems or tools. So, the requirement is a multi-stage verification process that must have modules to verify user credentials, OTP sent to the user's registered mobile number, real-time verification of the user's ID card, and facial verification.

4.2 The proposed system

As discussed above, the proposed system meets all the demands raised by the existing systems by integrating four different modules for verifying user credentials, OTP, voter's face, and ID card. The process flow is like, the user comes and enters his login credentials provided by the authority.

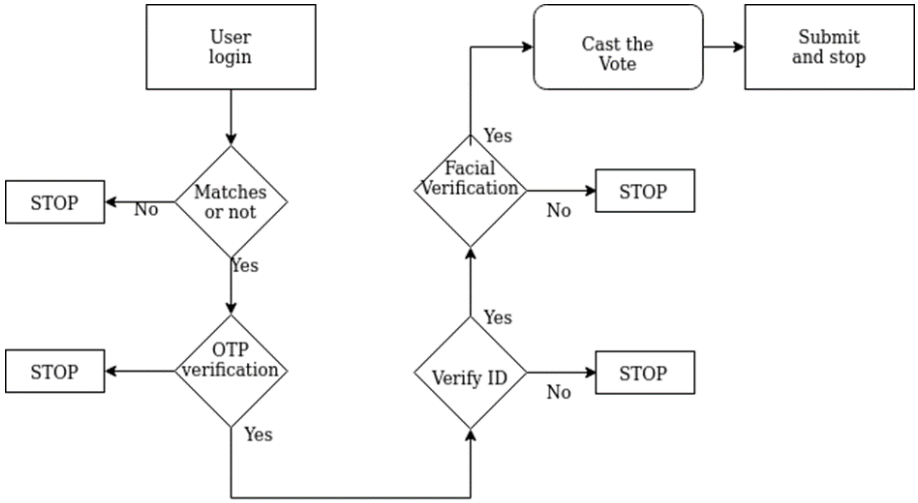

Figure 4.1: The proposed system.

He will only be allowed to the next stage when the user credentials are verified and are correct using the user details in the database such as username, password, contact number, face image, etc. The next stage will be the OTP verification. The OTP sent to the registered mobile number should be submitted to the system by the user. It will be verified and passed to the next stage if matches. The next stage is ID card verification. The user has to show the election ID card to the webcam to get the system to

extract the ID card information and match it with the information in the database. Once the voter passes all these stages, he will be taken to the final stage, facial verification. The user face will be compared with the data of the face and image in the database. Then the user will be sent to the vote casting page and allowed to do the voting and leave the platform.

Chapter 5

SYSTEM DESIGN AND ARCHITECTURE

5.1 System Architecture.

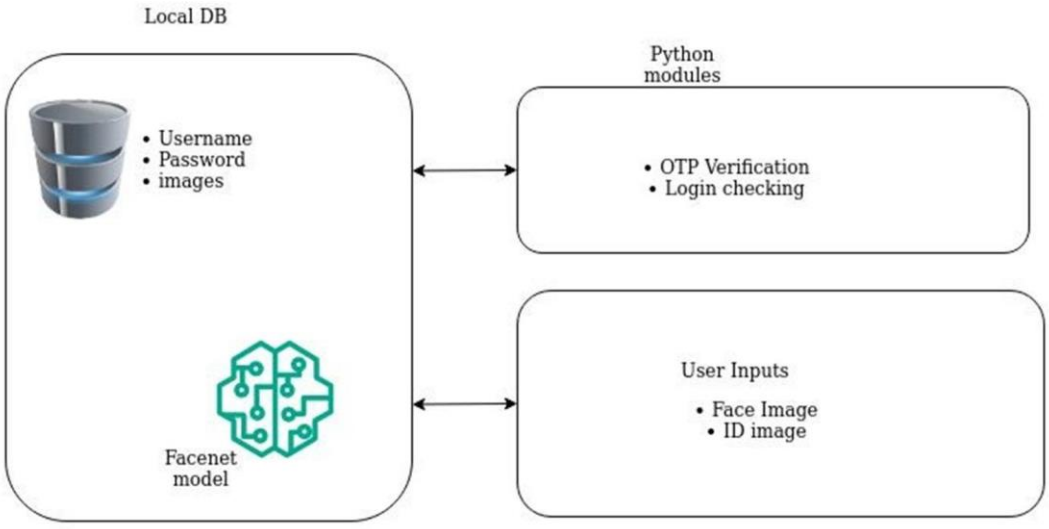

Figure 5.1: System architecture.

In the modern era, the integrity of electoral processes is paramount, and electronic voting (e-voting) systems have emerged as a solution to streamline voting procedures. However, alongside the convenience of e-voting comes the pressing need for robust security measures to safeguard against fraudulent activities and ensure the authenticity of votes cast. In response to this challenge, we present a comprehensive e-voting system that integrates multiple layers of verification to fortify the electoral process. Our system employs a sophisticated approach, leveraging a combination of Python programming, facial recognition technology, and machine learning models to authenticate voters at various stages of the voting process. At the forefront of our system is the initial verification step, where user credentials such as username and password are matched against stored information in the system's database. This foundational layer ensures that only authorized individuals gain access to the e-voting platform, laying the groundwork for subsequent verification procedures. Following successful credential matching, the system initiates a multi-sequence verification process, beginning with the generation and transmission of a one-time password (OTP) to the user's registered email address. This OTP mechanism adds an extra layer of security, requiring users to possess both their

login credentials and access to their designated email account to proceed with voting. Continuing the verification journey, our system integrates facial recognition technology powered by Google's API, OpenCV, and the FaceNet model to authenticate voters based on their facial features. By capturing and comparing the voter's face in real-time with the image associated with their account, we bolster the system's security and mitigate the risk of identity fraud. Furthermore, the final layer of verification involves comparing the voter's face extracted from their government-issued identification (ID) card with the face image stored in the election database, ensuring that the individual casting the vote is indeed the rightful owner of the voter account. Through these rigorous verification processes, our e-voting system aims to uphold the principles of democracy by safeguarding the integrity of the electoral process and fostering trust among voters.

5.2 Google Mediapipe

The Google Mediapipe face extractor is a powerful tool utilized in our e-voting system for extracting facial features from images or video streams. Developed by Google, Mediapipe offers a suite of machine learning solutions for various tasks, including facial recognition. The face extractor module employs advanced computer vision algorithms to accurately detect and localize human faces within an image or video frame. It utilizes a combination of convolutional neural networks (CNNs) and deep learning techniques to analyze pixel intensities and identify facial landmarks such as eyes, nose, and mouth. One of the key features of the Google Mediapipe face extractor is its robustness in handling various environmental conditions and facial poses. The algorithm is trained on extensive datasets containing diverse facial images captured under different lighting conditions, angles, and occlusions. This training enables the face extractor to effectively handle challenges such as partial occlusion, varying facial expressions, and changes in illumination, ensuring reliable performance in real-world scenarios. Additionally, the Google Mediapipe face extractor offers high efficiency and real-time processing capabilities, making it suitable for applications that require fast and accurate facial detection. By leveraging optimized computational techniques and parallel processing architectures, the face extractor module can efficiently analyze video streams or batches of images, enabling seamless integration into our e-voting system.

5.3 FaceNet Model

Complementing the face extractor module is the FaceNet Matching model, a state-of-the-art deep learning architecture designed for face recognition tasks. Developed by researchers at Google, FaceNet employs a Siamese neural network architecture coupled with triplet loss functions to learn discriminative embeddings of facial features. The model learns to encode facial images into high-dimensional feature vectors, where similar faces are mapped closer together in the embedding space, while dissimilar faces are pushed further apart. One of the primary advantages of the FaceNet Matching model is its ability to generate compact and semantically meaningful representations of facial features, which facilitate efficient comparison and matching. By encoding facial images into a fixed-length feature vector space, the model enables fast and accurate similarity calculations, making it ideal for real-time face recognition applications. Moreover, the FaceNet Matching model exhibits robustness to variations in facial appearance, such as changes in pose, expression, and lighting conditions. Through extensive training on large-scale datasets containing diverse facial images, the model learns to generalize well across different individuals and environmental conditions, ensuring reliable performance in our e-voting system.

5.4 Python String Matching

Python string matching is a fundamental operation used in various applications, including text processing, data analysis, and pattern recognition. It involves comparing strings to determine if they are identical or similar to each other based on specific criteria. Python offers several built-in methods and libraries for string matching, each serving different purposes and catering to diverse use cases. One of the simplest string-matching techniques in Python is exact string matching, where two strings are compared character by character to check for exact equality. This can be achieved using the equality operator (==) or the str.equals() method.

Chapter 6

SYSTEM REQUIREMENTS

The system requirement is not that much for this project as the training has been carried out in Google Colab free version. So, no specific hardware is required. The design and development of the whole system of image processing and deep learning have been carried out in Google Colab Cloud platform.

Hardware requirement:

Basic system with intel i3 or above processor.

Software requirement:

IDE used for ML development and training - Google Colab.

Language used for ML development and training - Python 3.7 - 3.11

In addition to this, various python libraries like os, Numpy, TensorFlow, Mediapipe, Facenet, etc will also be used.

HTML and CSS are used for front-end development.

The Ngrok hosting platform is used for free deployment.

Python Flask is used to connect frontend and backend.

Chapter 7

MODULE DESCRIPTION

7.1 User credential validation module:

The user credential module will verify details such as username and password. These details are pre-saved in the database. So, the verification can be done by basic python script. The program will use basic string to string comparison to verify the two strings: username and password.

The details will be saved as text files as a local DB file.

7.2 OTP Verification module:

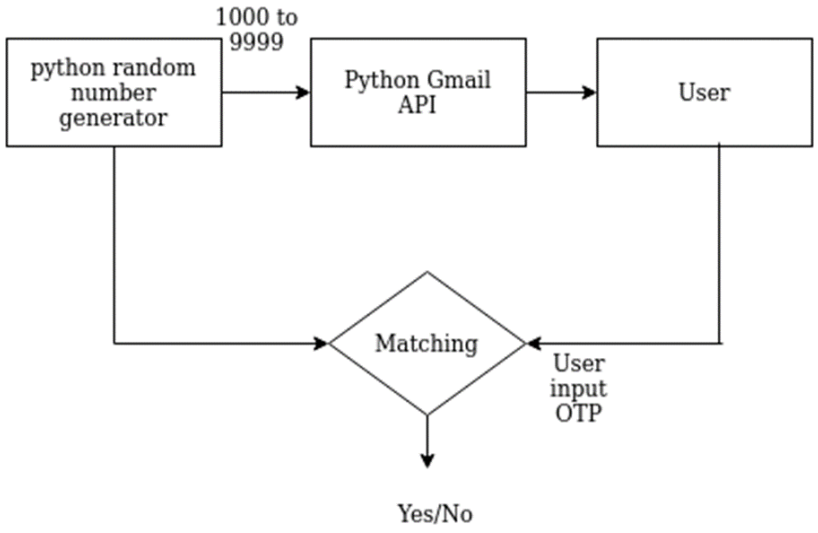

Figure 7.1: The OTP verification module

The OTP verification model starts working when the user successfully passes the first stage/module. A python based random number generator will generate a 4-digit random number. This will be sent to the contact number via Gmail using the Python MSTP library. Then once the user enters the received OTP to the system, he does the string to string comparison and verify.

7.3 ID verification module:

The user has to input the image of his ID card from which the image will be captured and compare with the face image in the database. The same operation is happening in the face verification stage as well. Both the modules are using technologies like Google Mediapipe for face extraction and FaceNet model for face similarity matching with the face in the ID card. The ID verification module enhances the security of the e-voting process by leveraging official government-issued identification documents, such as driver's licenses or national ID cards. These documents are widely recognized as reliable proof of identity and are commonly used in various official transactions. By incorporating ID verification into the e-voting system, we align with established practices for identity verification, thereby instilling confidence in the authenticity of the voting process. Moreover, the utilization of ID verification not only enhances security but also promotes inclusivity and accessibility in the electoral process. By adhering to standardized identification procedures, the system ensures that all eligible voters, regardless of background or demographics, can participate in the democratic process with confidence. This commitment to inclusivity reinforces the democratic ideals of equality and fairness, fostering trust and engagement among voters.

7.4 Facial recognition and validation module:

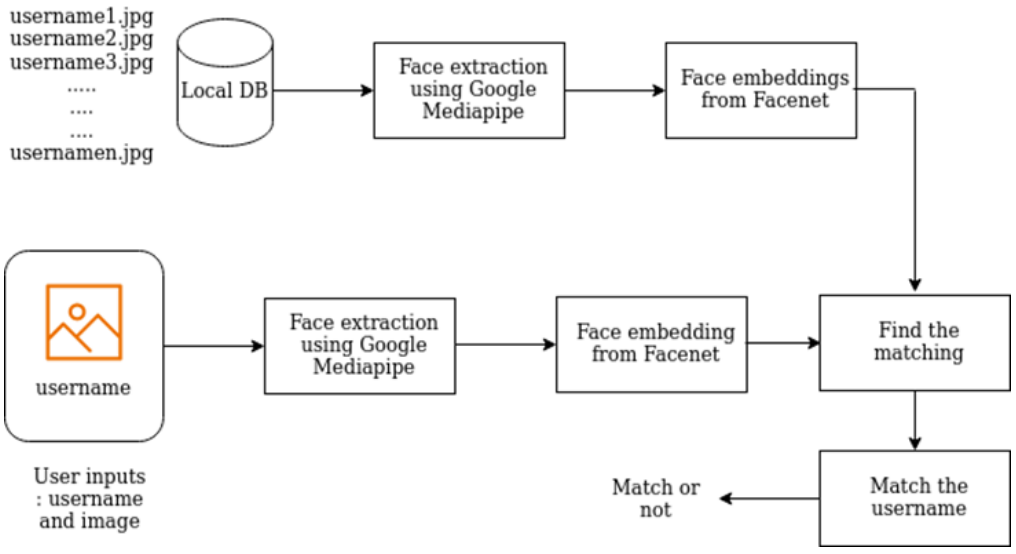

Figure 7.2: The facial verification module.

Here the user's face is compared with the face saved in the database. We first capture the user image using the webcam, then use the Google Mediapipe framework to extract the face from the image. This extracted face will be sent to the pre-trained facenet architecture to get the facial vectors. This will be compared with the facial vector in the database.

Chapter 8

IMPLEMENTATION

Results of each stage

8.1 Stage 1: Login Verification.

The login credentials of the user is compared with that of the user in the database and compared using python string matching.

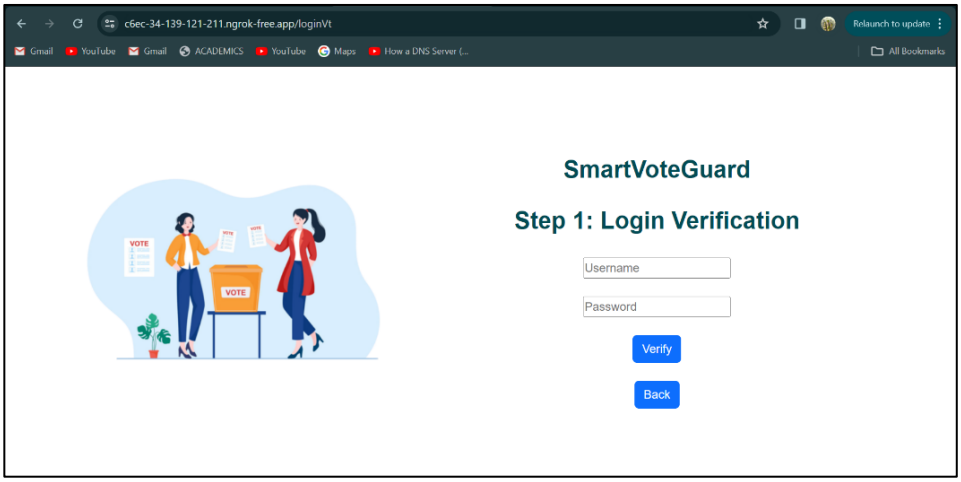

Figure 8.1: Login Verification stage

8.2 Stage 2: OTP Verification.

The four-digit OTP is generated and sent via Gmail. The user entered OTP is compared here and access to the next stage is decided.

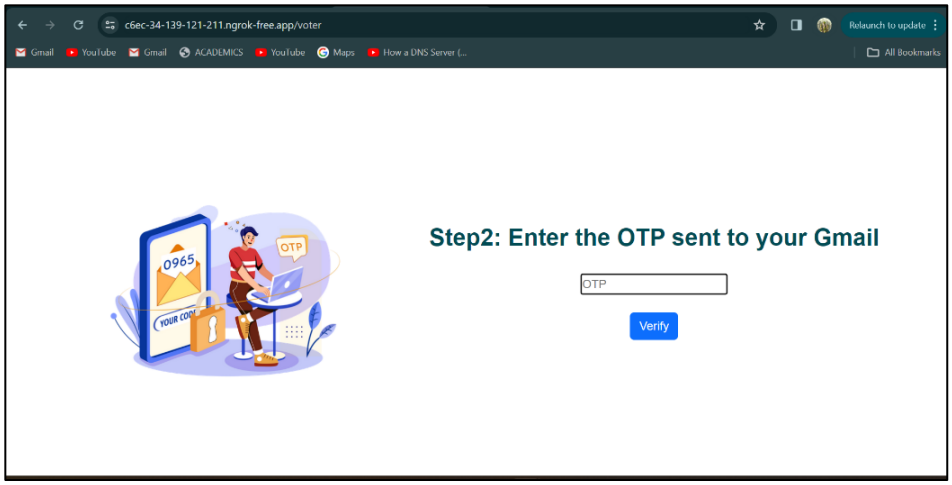

Figure 8.2: OTP Verification stage

8.3 Stage 3: Face Verification.

The face verification is based on the comparison done by the Facenet nodule on the faces extracted by the mediapipe face module.

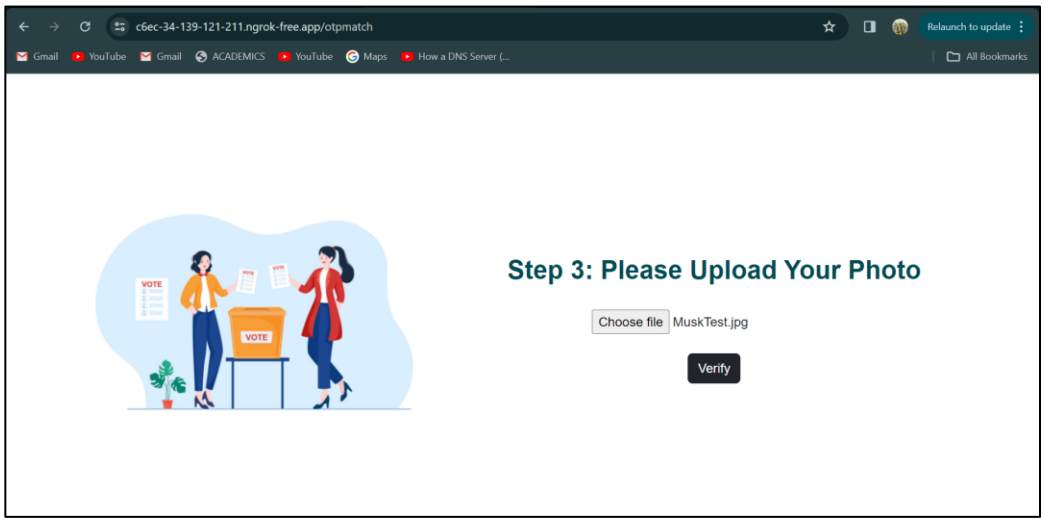

Figure 8.3: Face verification stage

8.4 Stage 4: ID card image verification.

The face in the ID card will be extracted using the mediapipe and compared using the Facenet model.

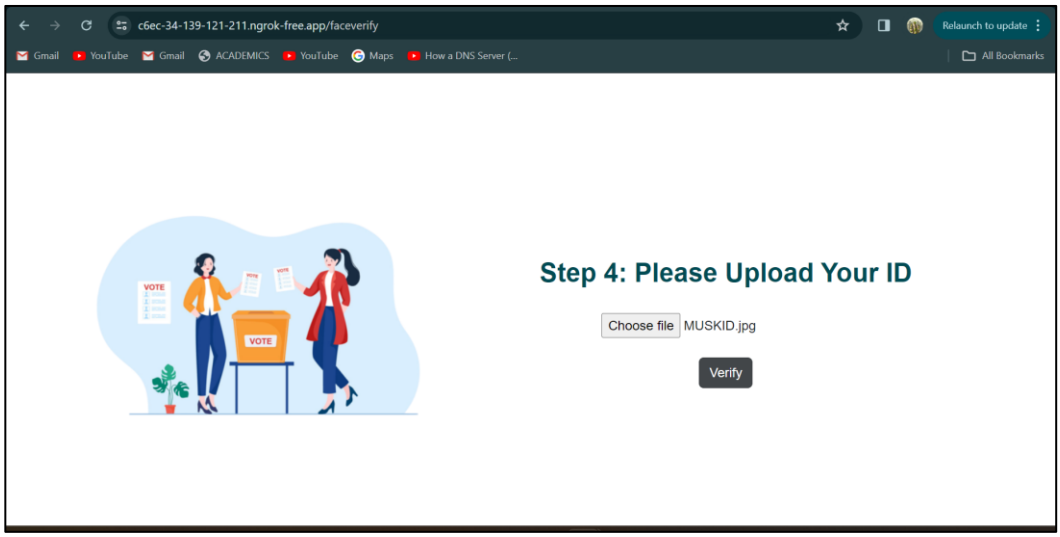

Figure 8.4: ID Card verification stage

8.5 The web app result.

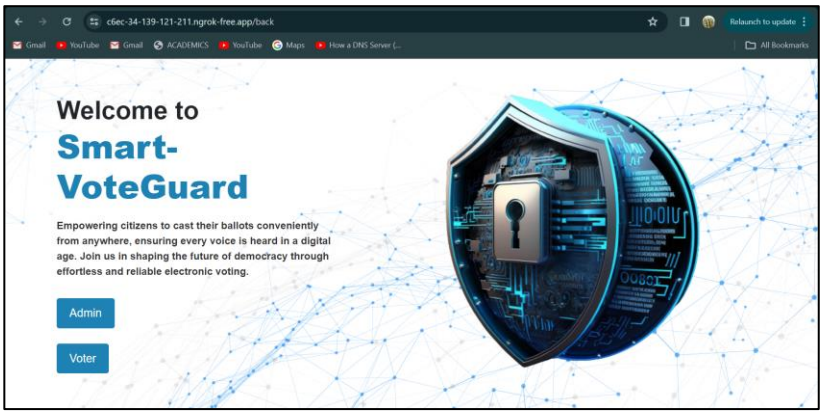

Figure 8.5: Home Page

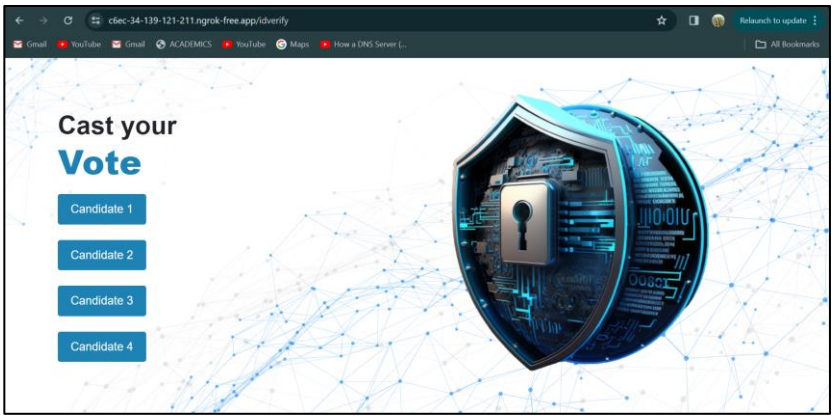

Figure 8.6: Voting interface after authentication.

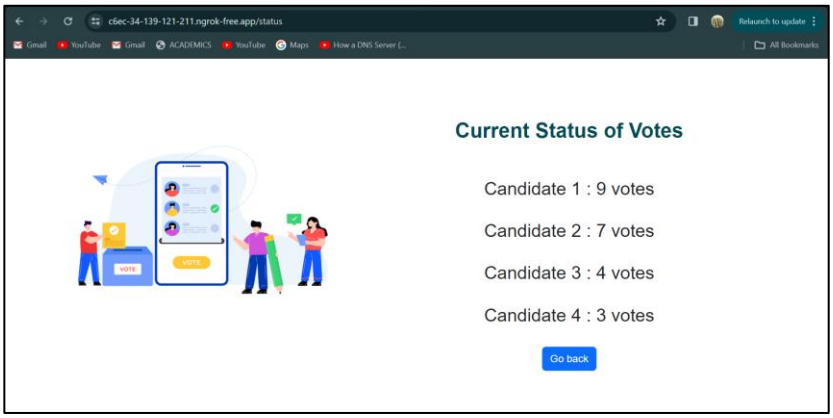

Figure 8.7: Admin access

Chapter 9
CONCLUSION

As societies advanced technologically, so did their electoral processes, with the emergence of electronic and online voting platforms promising greater efficiency, accessibility, and transparency. Despite these advancements, modern electoral systems face a myriad of challenges and complexities. Integration of novel and advanced security and personal metrics in voting ensures its strength, transparency, and non-vulnerability. This project attempted to do an online voting system with a sequence of verifications clubbed together to make the security and privacy protected and to mitigate the fraud in voting. The sequence starts from basic user credential validation, then the OTP verification, then a face verification and an ID verification then leads to the voting facility. The face verification based on FaceNet model, and the python-based string matching was found to be simple but efficient. The system was found to be easy to implement, deploy, and lightweight as well. Further improvements like data protection and protocols as well as advanced face recognition and computer vision algorithms can also be implemented.

APPENDIX

1. Face Verification Module

```
#Install the Google Mediapipe library for face extraction


!pip install mediapipe


# Import necessary libraries


import cv2 # OpenCV library for image and video operations

import math # For math operations

import numpy as np # For numerical operations

import glob  # For file reading and writing operations

import os # For file reading and writing operations

import matplotlib.pyplot as plt # For plotting and visualizations

import mediapipe as mp # The Google Mediapipe library for Face extraction

from google.colab.patches import cv2_imshow # To display the image

import tensorflow as tf # Tensorflow for face similarity calculation


# Function to extract face from the image

# When we input an image to this function, it will give the extracted face or cropped face as output.



def extract_face(image):

    h = image.shape[0] # Height of the image
```

```
    w = image.shape[1] # Width of the image



    # Insert the face detection module from Google Mediapipe
    mp_face_detection = mp.solutions.face_detection
    face_detection =
mp_face_detection.FaceDetection(min_detection_confidence=0.5,model_selection=0)



    results = face_detection.process(np.array(image)) # Apply the face detection module to the
image
    # "result" will have the coordinates of the face square

    # Get the coordinates of the face square from "result"
    # The coordinates are xmin, ymin, height, and width
    xmin = results.detections[0].location_data.relative_bounding_box.xmin
    xmin = math.floor(xmin*w)

    ymin = results.detections[0].location_data.relative_bounding_box.ymin
    ymin = math.floor(ymin*h)

     width = results.detections[0].location_data.relative_bounding_box.width
    width = math.floor(width*w)

    height = results.detections[0].location_data.relative_bounding_box.height
    height = math.floor(height*h)
```

```
    # Now we have xmin, ymin, width and height of the face square


    crop_img = image.copy()

    crop_img = crop_img[ymin:ymin+height, xmin:xmin+width] # Crop the face square from
the input image


    return crop_img


# Function to get Similarity value between two images



def get_similarity(image1, image2):


  # load the Tensorflow face similarity model

  #interpreter = tf.lite.Interpreter(model_path =
"TFlite_model_from_Keras_of_tensorflow_model.tflite")

  interpreter = tf.lite.Interpreter(model_path = "TFlite_model_from_Keras_model.tflite")

  interpreter.allocate_tensors()

  face_model = interpreter


  image1 = cv2.resize(image1, (160, 160))

  image2 = cv2.resize(image2, (160, 160))


  image1 = image1.astype('float32')

  image2 = image2.astype('float32')
```

```
mean1, std1 = image1.mean(), image1.std()
mean2, std2 = image2.mean(), image2.std()

image1 = (image1 - mean1) / std1
image2 = (image2 - mean2) / std2

# Get input and output tensors
input_details = face_model.get_input_details()
output_details = face_model.get_output_details()

# Test the model on random input data.
input_shape = input_details[0]['shape']

imgs = [image1, image2]

outputs = []
for img in imgs:
  input_data = img.reshape(input_shape)
  face_model.set_tensor(input_details[0]['index'], input_data)
  face_model.invoke()
  output_data = face_model.get_tensor(output_details[0]['index'])
  outputs.append(output_data)


distance = np.stack(outputs)
```

```
    distance = np.linalg.norm(distance[0, :] - distance[1, :])

    return distance

    def face_verify(input_image, username):

    input_image = extract_face(input_image) # Get the face cropped from input_image

    # Get all the images from the DB and get thier faces cropped
    path = "Local_DB/Images"
    DB_images = []
    for i in os.listdir(path):
      DB_images.append(i)

    cropped_faces = []
    for i in DB_images:
      image = cv2.imread("Local_DB/Images/" + i)
      image = extract_face(image)
      cropped_faces.append(image)

    # Calculate the similarities by one by one
    similarities = []
    for i in cropped_faces:
      distance = get_similarity(input_image, i)
      similarities.append(distance)
```

```
    index = similarities.index(min(similarities)) # Get the lowest distance value
    Result = DB_images[index] # Get corresponding image name
    Result = Result.split('.')[0] # Get corresponding person name by removing ".jpg"

    # Compare the username with matched face name
    if Result == username:
      print('Successful!')
    else:
      print("No Match")

# Upload your image


Musk = cv2.imread("MuskTest.jpg")

face_verify(Musk, username)
```

REFERENCES

1. Sakshi, et.al, “A Novel Method for Facial Recognition Based Smart Voting System Using Machine Learning” , International Research Journal of Engineering and Technology (IRJET) , e-ISSN: 2395-0056, Volume: 10 Issue: 05 | May 2023.
2. Niloofar Tavakolian, Azadeh Nazemi, & Donal Fitzpatrick. (2020). Real-time information retrieval from Identity cards.
3. Chouhan, Kanchan. “Smart Voting through UID Verification by Using Face Recognition.” IJETT (2019): n. pag. Print.
4. Domakonda, Sreekanth & Kumar, Arigala & Rao, Alladi & Sindhu, Ankammagari & Btech,. (2022). E-VOTING SYSTEM USING FACIAL RECOGNITION.
5. Li, et al. (2022). "Secure Online Voting System with Facial Recognition and ID Card Verification," Journal of Cybersecurity and Information Protection, Volume 15, Issue 3.
6. Gupta, A., & Sharma, S. (2021). "Blockchain-Based Smart Voting System with Facial Recognition and ID Card Verification," International Journal of Blockchain and Cryptocurrency, Volume 8, Issue 2.
7. Khan, et al. (2020). "User Acceptance of Smart Voting Systems: A Survey Study," Journal of Information Technology and Society, Volume 25, Issue 4.
8. Patel, R., & Desai, S. (2024). "Enhancing Voter Authentication in Smart Voting Systems using Facial Recognition and Blockchain Technology," International Journal of Computer Science and Information Security, Volume 12, Issue 7.
9. Wang, X., & Zhang, Y. (2023). "Privacy-Preserving Facial Recognition for Smart Voting Systems," IEEE Transactions on Information Forensics and Security, Volume 9, Issue 4.
10. Chen, L., & Wu, J. (2022). "Scalable Facial Recognition System for Large-Scale Smart Voting Platforms," ACM Transactions on Multimedia Computing, Communications, and Applications, Volume 6, Issue 2.
11. Park, H., & Kim, S. (2021). "Real-Time Facial Recognition for Smart Voting Kiosks," Journal of Computer Vision and Image Understanding, Volume 30, Issue 3.
12. Garcia, M., & Rodriguez, P. (2023). "Secure Facial Recognition Voting System with Multi-Modal Biometric Authentication," International Journal of Information Security, Volume 18, Issue