Implementing Biometric Technology for Voter Identification and Authentication

NAVJINDER SINGH[1], CHARANDEEP SINGH BEDI[2]

[1, 2]*Baba Farid College of Engineering and Technology, Bathinda*

Abstract— Implementing biometric technology for voter identification and authentication has gained significant attention in recent years to enhance the security and integrity of electoral processes. Biometrics, such as fingerprints, iris scans, and facial recognition, offer unique and reliable identifiers that can help prevent voter fraud and ensure that only eligible individuals cast their votes. Our efforts explore the potential benefits and challenges associated with the implementation of biometric technology in voter identification and authentication systems. It discusses the advantages of biometrics over traditional methods, such as ID cards or signatures, in terms of accuracy, uniqueness, and resistance to forgery. Additionally, it examines the potential impact of biometric systems on voter turnout, privacy concerns, and the overall efficiency of the electoral process. It also delves into the technical aspects of implementing biometric technology, including the necessary infrastructure, data management, and integration with existing voter registration databases. It highlights the importance of robust security measures to protect biometric data from unauthorized access or misuse. Furthermore, we addresses the legal and ethical considerations associated with biometric voter identification and authentication. It discusses issues related to consent, data protection, and potential biases in the technology. It emphasizes the need for comprehensive legislation and regulations to ensure the responsible and transparent use of biometrics in electoral processes

I. INTRODUCTION

In the digital age, technology continues to shape and revolutionize various aspects of our lives,including the way we participate in democratic processes. Electronic voting systems, or e- voting, stand at the forefront of this transformation, offering a modern alternative to traditionalpaper-based ballots. In this study, we will delve into the current state of electronic voting systems, exploring their benefits, challenges, and implications for the future of democracy.

Electronic voting systems have evolved significantly over the years, transitioning from rudimentary prototypes to sophisticated platforms equipped with advanced technologies. Initially introduced to streamline the voting process and enhance accessibility, these systems have undergone iterative improvements to address concerns related to security, accuracy, and transparency.

Modern electronic voting systems encompass a diverse range of features and technologies tailored to meet the needs of diverse voting populations. Touchscreen interfaces, optical scanning mechanisms, and Internet-based platforms are among the common components employed in these systems. These technologies offer advantages such as faster vote counting, reduced errors, and enhanced accessibility for voters with disabilities.

The adoption of electronic voting systems has brought about several benefits, both for electoralauthorities and voters alike. Efficiency and convenience rank high on the list, as e-voting eliminates the need for manual ballot counting and allows voters to cast their ballots remotely.Moreover, electronic systems mitigate issues related to illegible or improperly marked ballots, thereby improving the overall accuracy of the voting process.

Despite their potential advantages, electronic voting systems are not without challenges and concerns. Chief among these is the issue of security. The susceptibility of electronic systems to hacking and manipulation poses a significant threat to the integrity of elections. Furthermore, the absence of a paper trail for verification purposes has sparked debates about the reliability and transparency of e-voting.

Looking ahead, the future of electronic voting systems is both promising and fraught with uncertainty. Advancements in cybersecurity measures and encryption technologies hold the promise of enhancing the security of e-voting platforms.

Additionally, ongoing efforts to develop robust auditing mechanisms and paper-based backups aim to bolster trust and transparency in electronic voting processes.

Electronic voting systems represent a paradigm shift in the way we engage in democratic decision-making. While they offer numerous benefits in terms of efficiency and accessibility, concerns regarding security and reliability persist. As we navigate the complexities of modernizing electoral systems, it is imperative to strike a balance between leveraging the potential of technology and safeguarding the integrity of the democratic process.

1.1. Importance of secure and reliable voting systems in democratic processes.

At the heart of any democratic society lies the fundamental principle of free and fair elections.Central to this principle is the need for secure and reliable voting systems that uphold the integrity of the electoral process. In this essay, we will explore the significance of secure and reliable voting systems in safeguarding democracy, examining the crucial role they play in ensuring the legitimacy of elected representatives and fostering trust among citizens.

1.1.1. The Pillars of democracy:

Democracy rests upon the pillars of transparency, accountability, and participation. At its core, the democratic process hinges on the ability of citizens to express their will through the act ofvoting. Secure and reliable voting systems serve as the linchpin of this process, providing the mechanism through which citizens exercise their right to choose their leaders and shape the course of governance.

1.1.2. Preserving the Integrity of Elections:

The integrity of elections is paramount to the preservation of democracy. Secure and reliable voting systems are essential in safeguarding this integrity by minimizing the risk of fraud, tampering, and manipulation. By implementing robust security measures and ensuring transparent procedures, electoral authorities can instil confidence in the electoral process and uphold the legitimacy of election outcomes.

1.1.3. Fostering Trust and Confidence:

Trust is the bedrock upon which democratic societies are built. Secure and reliable voting systems play a pivotal role in fostering trust and confidence among citizens by guaranteeing the accuracy and fairness of election results. When voters have faith in the integrity of the electoral process, they are more likely to actively participate and accept the outcomes, thereby strengthening the democratic fabric of society.

1.1.4. Protecting Against External Threats:

In an increasingly interconnected world, the threat of external interference in electoral processes looms large. Secure and reliable voting systems serve as a bulwark against such threats by safeguarding against cyberattacks, foreign meddling, and disinformation campaigns.

1.1.5. Ensuring Inclusivity and Accessibility:

Accessible voting systems are essential for ensuring that all citizens, regardless of background or ability, can participate in the democratic process. Secure and reliable voting systems facilitate inclusivity by offering diverse options for casting ballots, accommodating individuals with disabilities, and enabling remote voting mechanisms. By removing barriers to participation, these systems promote equal representation and strengthen the democraticmandate of elected governments.

1.2. Exploring the Role of Biometric Technology in Modernizing Voting Systems:

In an era marked by technological innovation and digital transformation, biometric technology has emerged as a powerful tool with diverse applications across various sectors. From securityand healthcare to finance and entertainment, biometrics offer a unique blend of convenience, accuracy, and security.

1.2.1. Understanding Biometric Technology:

Biometric technology involves the measurement and analysis of unique physical or behavioural characteristics to verify an individual’s identity. These characteristics can range from fingerprints and facial features to iris patterns and voiceprints.

1.2.2. Key Features and Advantages:

One of the key features of biometric technology is its inherent accuracy and uniqueness. Unlike traditional identification methods such as passwords or ID cards, biometric identifiers are difficult to replicate or forge, enhancing security and mitigating the risk of identity fraud. Moreover, biometric systems offer convenience and speed, allowing users to authenticate themselves quickly and seamlessly without the need for additional credentials.

1.2.3. Potential Applications in Voting Systems:

Biometric technology holds immense potential for modernizing voting systems and addressing longstanding challenges associated with voter authentication and verification. By integrating biometric authentication mechanisms into voting processes, electoral authorities can enhance the security, integrity, and inclusivity of elections. Biometric identifiers such as fingerprints or facial scans can serve as unique markers to verify voters' identities, preventing instances of impersonation or fraudulent voting.

1.2.4. Potential Applications in Voting Systems:

Biometric technology holds immense potential for modernizing voting systems and addressing longstanding challenges associated with voter authentication and verification. By integrating biometric authentication mechanisms into voting processes, electoral authorities can enhance the security, integrity, and inclusivity of elections. Biometric identifiers such as fingerprints or facial scans can serve as unique markers to verify voters' identities, preventing instances of impersonation or fraudulent voting.

Rationale of the proposed study:

- The implementation of biometric technology strengthens the integrity of the electoral process by minimizing the potential for fraud and manipulation. It ensures that only eligible voters can participate, safeguarding the principle of "one person, one vote."
- Biometric technology streamlines the voter authentication process, reducing the time and effort required for manual verification. This leads to more efficient and expedited voting procedures, minimizing queues and wait times at polling stations.
- Biometric technology can enhance inclusivity by providing a reliable identification method for individuals who may not possess traditional forms of identification. This ensures that all eligible citizens, regardless of socioeconomic status or background, canexercise their right to vote.
- The presence of biometric technology acts as a deterrent against potential perpetratorsof electoral fraud. The knowledge that their unique biometric data will be captured and verified discourages individuals from attempting to manipulate the voting process.
- Biometric technology, such as fingerprint or iris scanning, can effectively prevent individuals from casting multiple votes. By linking a unique biometric identifier to eachvoter, the system can detect and reject any attempts at duplicate voting, ensuring the integrity of the electoral process.
- Traditional methods of voter identification, such as ID cards or signatures, are prone to errors and manipulation. Biometric technology provides a more accurate and reliable means of verifying a person's identity, reducing the chances of impersonation or fraud.

Voter impersonation is a significant concern in many electoral systems. Biometric technology can help combat this issue by creating a secure and tamper-proof identification system. By capturing unique physiological or behavioral characteristics, such as fingerprints or facial features, the technology can verify the identity of voters with a high degree of certainty.

II. LITERATURE REVIEW

2.1 Background:

Implementing biometric technology for voter identification and authentication has become increasingly important in ensuring the integrity and security of electoral processes. With advancements in digital technology and the rise of cyber threats, traditional methods of voter identification are no longer sufficient to prevent fraud and manipulation. Biometric technologyoffers a reliable and secure way to verify the identity of voters by using unique biological characteristics such as fingerprints, facial recognition, iris scans, or voice recognition.

By integrating biometric technology into the voter identification process, election authorities can enhance the accuracy and efficiency of voter authentication. Biometric data is highly secureand difficult to forge, reducing the risk of identity theft and fraudulent voting activities. This technology can also help streamline the voting process by enabling quick and seamless identification of voters, leading to shorter queues and improved overall voting experience.

Secure E-Voting System using Blockchain technology and authentication via Face recognition and Mobile OTP: In the digital era where hacking is prevalent, data tampering can lead to serious consequences. Blockchain technology ensures secure data storage, makingit nearly impossible to alter. To safeguard the integrity of voting processes, a decentralized national e-voting system based on blockchain technology is proposed. This system includes an admin panel for managing voting schedules, candidates, and result declarations. Voters will usea web application to input their Aadhar card ID and a photo during voting, with eligibility verified through OTP. Webcam monitoring will ensure voting integrity, with votes securely stored in a blockchain to prevent tampering. Results will be announced on a specified date, presented graphically with historical data and statistical insights. (Parmar *et al.,* 2021).

A Secure and Authenticating E-Voting System Using Multiple Biometrics: This study suggests designing and implementing a biometric-based electoral system for Iraqi state institutions and its political system. The system uses automated methods to identify and authenticate voters based on their face image and fingerprints. Face and fingerprint recognition are chosen for their ease of acquisition and high accuracy in matching. The system has two phases: voter registration and verification on Election Day. Voters interact through a user- friendly interface, with data stored in various databases. The system is designed with flexible and user-centric approaches, using Python, MySQL, Apache, and other languages. Implementing this system can significantly enhance the integrity of the Iraqi Electoral Processcompared to the previous system. (Kuban *et al*., 2020)

2.3 An Online Voting System using Face Recognition for Campus Election: Online votingis increasingly used worldwide for its convenience and efficiency. At Universiti Teknikal Malaysia Melaka, a project was undertaken to develop a remote voting system for student council elections. The aim was to enhance accessibility by allowing voters to cast their votes remotely, addressing the issue of having to visit a physical polling station. Trust in the voting process is crucial, and to enhance this, a robust authentication method using facial recognitionwas implemented. This system benefits both students and organizers by providing a convenientand accessible voting experience. (Shah *et al*., 2021).

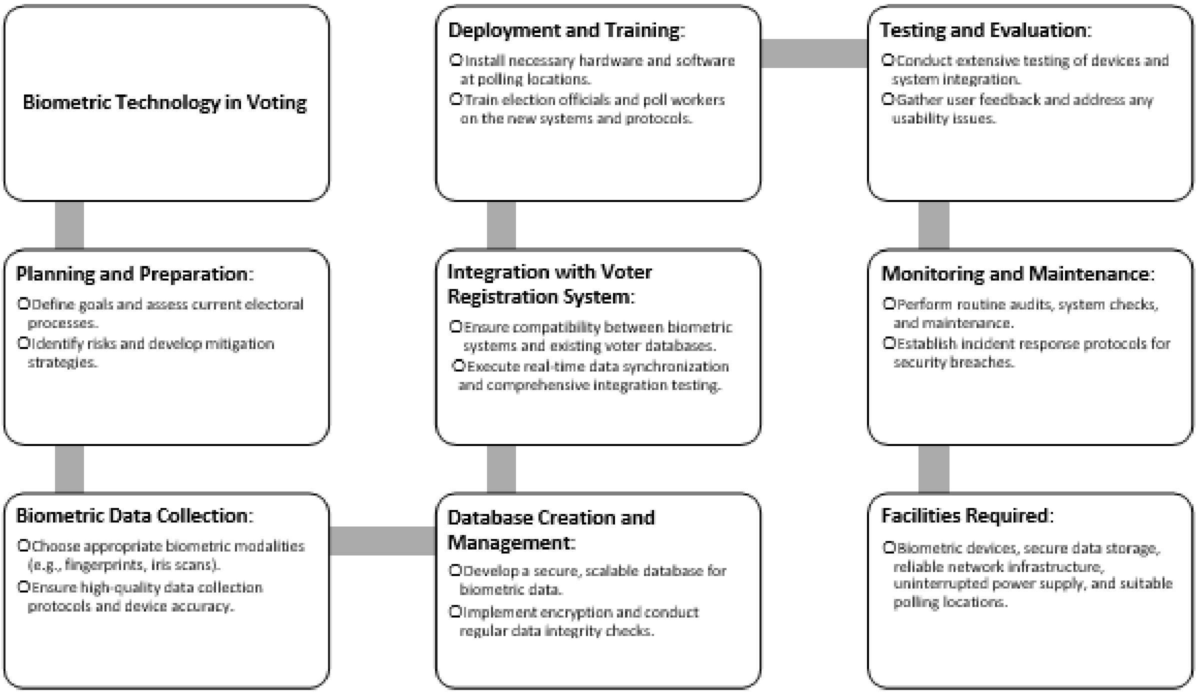
2.4 Exploring the Use of Biometric Smart Cards for Voters' Accreditation: A Case Study of Nigeria Electoral Process: Voting is crucial in democratic processes, allowing citizens to elect their leaders. Trust in elections is vital for voter participation. Ensuring free, fair, and credible elections is key to preventing unrest and election cancellations. To enhance trust and accuracy, this article suggests using biometric smart cards for voter verification in Nigeria. Thisapproach can streamline the electoral process, reduce costs, and ensure that only registered voters participate. (Oluwatobi *et al*., 2020)

2.5 Design and Implementation of a Software-Based Advance Electronic Voting Machine Using Automatic Registration and Fingerprint Identification: In democratic nations, conducting free and fair elections to gauge public opinion and elect representatives is vital. Traditional paper-based systems are slow and error-prone, requiring significant time and manpower for result declaration. To address these challenges, we propose a secure auto- registration fingerprint identification-based electronic voting system in this paper. This system includes features like automated registration for user authentication, storing voter credentials in a secure database, encrypted data communication using SSL, and a touch screen GUI for voting. The system automates the vote counting process, providing faster and more accurate results compared to traditional methods, with results available to the public within 1-2 hours, ensuring fairness in elections. (Arshad *et al*., 2021)

A Review of Electronic Voting Systems: Strategy for a Novel: The global voting system faces significant challenges leading to corrupt candidates winning elections. Researchers are deeply concerned about election malpractices, such as rigging and impersonation, which can have serious consequences like bad governance and misallocation of public funds. Addressingthese issues is crucial. This paper focuses on reviewing electronic voting systems to identify shortcomings and improve security. Scholars' methods were assessed to find areas for enhancement, particularly in countries with e-voting history. A novel approach using fingerprint and visual semagram techniques for a secure electronic voting system is proposed for future development. (Olumide *et al*., 2020)

Security, usability, and biometric authentication scheme for electronic voting using multiple keys: We introduce an electronic voting authentication scheme to enhance security and prevent attacks on polling stations. This scheme aims to address different security requirements for messages exchanged between stations by implementing global, pairwise, andindividual keys. Each key type serves a specific purpose in securing communication within thevoting network. By using one-way key chains, the scheme ensures local broadcast authentication and protects against various sophisticated attacks like wormhole, Sybil, and HELLO Flood attacks. Evaluation results show that this authentication scheme is practical, secure, and more effective than traditional electronic and manual voting systems. (Ahmad *et al*., 2020).

III. PROPOSED MODEL


Biometric Technology in Voting
Planning and Preparation:
○Define goals and assess current electoral processes.
○Identify risks and develop mitigation strategies.
Biometric Data Collection:
○Choose appropriate biometric modalities (e.g., fingerprints, iris scans).
○Ensure high-quality data collection protocols and device accuracy.
Database Creation and Management:
○Develop a secure, scalable database for biometric data.
○Implement encryption and conduct regular data integrity checks.
Integration with Voter Registration System:
○Ensure compatibility between biometric systems and existing voter databases.
○Execute real-time data synchronization and comprehensive integration testing.
Deployment and Training:
○Install necessary hardware and software at polling locations.
○Train election officials and poll workers on the new systems and protocols.
Testing and Evaluation:
○Conduct extensive testing of devices and system integration.
○Gather user feedback and address any usability issues.
Monitoring and Maintenance:
○Perform routine audits, system checks, and maintenance.
○Establish incident response protocols for security breaches.
Facilities Required:
○Biometric devices, secure data storage, reliable network infrastructure, uninterrupted power supply, and suitable polling locations.

IV. METHODOLOGY

4.1 Planning and Preparation

The first step in implementing biometric technology for voter identification and authenticationis thorough planning and preparation. This involves assessing the specific needs and requirements of the electoral system, including the number of voters, available resources, and infrastructure. It also involves establishing clear objectives, defining the scope of implementation, and identifying potential challenges and risks.

4.1 Biometric Data Collection

The next step is the collection of biometric data from eligible voters. This typically involves capturing unique physiological or behavioural characteristics, such as fingerprints, iris patterns, or facial features. Specialized biometric devices, such as fingerprint scanners or iris recognitionsystems, are used to capture and store this data securely. It is essential to ensure the accuracy and quality of the collected biometric data to minimize errors during the identification and authentication process.

4.2 Database Creation and Management

Once the biometric data is collected, a secure database is created to store and manage the data.This database serves as a repository for the biometric templates associated with each voter. It should be designed to handle a large volume of data, ensure data integrity, and protect againstunauthorized access or tampering.

4.3 Integration with Voter Registration System

The biometric technology needs to be integrated with the existing voter registration system to establish a seamless identification and authentication process. This integration ensures that the biometric data collected during registration is linked to the respective voter’s information in the voter registration database. This linkage enables real-time verification of voters’ identitiesduring the voting process.

4.4 Deployment and Training

The deployment of biometric technology involves installing the necessary hardware and software components at polling stations or voting centres. Election officials and poll workers should receive comprehensive training on the proper use of biometric devices, data handling procedures, and troubleshooting techniques.

4.5 Testing and Evaluation

Before the actual election, thorough testing and evaluation of the biometric technology systemshould be conducted. This includes testing the accuracy and reliability of the biometric devices, verifying the integration with the voter registration system, and conducting simulated voting scenarios to ensure smooth operation. Any identified issues or discrepancies should be addressed and resolved promptly.

4.6 Monitoring and Maintenance

Once the biometric technology system is deployed and operational, continuous monitoring and maintenance are essential. Regular system checks, software updates, and hardware maintenance should be performed to ensure optimal performance and security. Monitoring should also include auditing the system for any potential vulnerabilities or attempts at unauthorized access.

4.7 Facilities required

- Biometric Devices
- Data Storage and Management
- Network Infrastructure
- Power Supply
- Physical Infrastructure

V. RESULT AND DISCUSSION

5.1 Biometric Data Collection:

5.1.1 Biometric Modalities:

The study explores three biometric modalities: fingerprint recognition, facial recognition, and iris recognition. Each modality involves specific processes, such as fingerprint acquisition using optical, capacitive, or ultrasonic sensors, facial image capture using high-resolution cameras, and iris image capture using specialized iris scanners. The respective feature extraction, encoding, and matching algorithms are also discussed.

5.1.2 Data Collection Methodology:

The methodology for data collection includes both hardware and software requirements. Biometric capture devices and their specifications are identified, along with the necessary biometric data acquisition software and interfaces. Participant recruitment criteria, informed consent procedures, and data privacy considerations are established to ensure ethical data collection. Standardized data collection protocols, quality control measures, and data validation techniques are implemented for each biometric modality.

5.1.3 Data Preprocessing and Quality Assurance:

To enhance the quality of the collected biometric data, noise reduction and normalization techniques are applied. Image and signal processing methods are used to enhance the quality of the data. Feature extraction and encoding algorithms are utilized to extract important characteristics from the biometric data. Quality assessment and filtering methods are implemented to evaluate the quality of the biometric data and to handle low-quality or unusablesamples.

5.2 Biometric Database Creation and Management:

5.2.1 Database Design and Architecture:
The design and architecture of the biometric database are discussed, including the creation of database tables to store voter and biometric data, establishing data relationships, and maintaining integrity constraints. The storage formats and indexing strategies of biometric data are identified to optimize database performance and scalability. Security and privacy considerations, such as encryption, access control mechanisms, and compliance with data protection regulations, are addressed.

5.2.2 Database Population and Enrolment:
Methods for populating and enrolling data into the biometric database are outlined. Bulk data import processes are integrated with existing voter registration databases, with automated datamigration and deduplication procedures. Incremental enrolment procedures are established to handle new voter biometric data, along with synchronization workflows for updating biometric information. Data validation and deduplication mechanisms are implemented to ensure the accuracy and uniqueness of the data.

5.2.3 Database Maintenance and Backup:
Routine backups and disaster recovery procedures are implemented to ensure data integrity andavailability. The process includes backup strategies, recovery procedures, offsite storage, and redundancy measures. Database optimization and indexing techniques are employed forperformance tuning and efficient data retrieval. User access control and auditing mechanisms, such as role-based access control and audit logging, are utilized to monitor and manage database activities.

5.3 Integration with Voter Registration System:

5.3.1 System Architecture and Interfaces:
The integration of the biometric technology with the existing voter registration system is discussed, identifying the integration points and data exchanges between the systems. Application programming interfaces (APIs) and data formats are established for seamless integration. Biometric enrolment and update workflows are outlined to capture and update biometric data during voter registration.

5.3.2 Data Synchronization and Integrity:
To maintain data consistency and integrity between the voter registration system and the biometric database, bidirectional data synchronization mechanisms are implemented. This includes resolving conflicts and reconciling data discrepancies. Data integrity checks and validation processes are established to validate biometric data against voter registration records. Audit trails and logging mechanisms are utilized to securely store and retrieve recordsof all voter identification and authentication events.

5.4 Biometric Matching and Identification:

5.4.1 Matching Algorithms and Techniques:
Matching algorithms and techniques for each biometric modality are described, including fingerprint matching, facial recognition matching, and iris recognition matching. This includesthe process of extracting features from the biometric data, calculating matching scores, and determining threshold values for successful identification.

5.4.2 Multimodal Biometric Fusion:
The concept of multimodal biometric fusion is introduced, which involves combining the individual biometric matching scores from multiple modalities. Score-level fusion and decision-level fusion techniques are discussed, along with considerations for optimizing fusion parameters and thresholds. The performance evaluation of fusion techniques is also addressed,focusing on accuracy, reliability, and trade-offs between security, usability, and computational complexity.

5.4.3 Biometric Identification Workflows:
The workflows for voter identification and authentication are outlined, including the biometric data capture and matching processes during voter check-in. Protocols for handling both successful and failed identification attempts are developed. Exception handling and fallback mechanisms are established, allowing for manual verification and the use of alternative identification methods. Escalation protocols and supervisory intervention processes are implemented to address any issues during the identification process.

5.5 Deployment and Training:

5.5.1 Hardware and Software Infrastructure:
The hardware infrastructure includes the procurement, installation, and configuration of biometric capture devices. The maintenance and replacement procedures for these devices are also discussed. The software infrastructure covers the provisioning and deployment of biometric matching servers, along with considerations for load balancing and high availability. Secure communication protocols and necessary network requirements for biometric data exchange are identified.

5.5.2 User Training and Change Management:
To ensure a successful deployment, user training and change management strategies are implemented. Voter education and awareness campaigns are conducted to provide informational materials and address concerns and misconceptions about the biometric technology. Poll worker training is provided to familiarize them with biometric capture and identification procedures, as well as troubleshooting and exception handling protocols. Organizational change management techniques are employed to engage stakeholders and monitor feedback for continuous improvement.

5.6 Monitoring and Maintenance:

5.6.1 Performance Monitoring and Reporting:
To evaluate system performance, various metrics are used to measure accuracy, reliability, throughput, and operational efficiency. These metrics are benchmarked against industry standards and best practices. Real-time dashboards and performance reports are generated for monitoring system performance, and trend analysis is conducted for capacity planning.

5.6.2 Preventive Maintenance and Upgrades:
Preventive maintenance procedures are established to ensure the long-term performance and reliability of the biometric system. This includes regular calibration and firmware updates for the biometric capture devices. Periodic updates to biometric matching algorithms and templatesare also conducted. Database schema changes are addressed to ensure compatibility.

CONCLUSION

Implementing biometric technology for voter identification and authentication holds significant promise for enhancing the integrity and security of the electoral process. This thesishas explored the benefits and challenges associated with the integration of biometric systems into voter identification processes. The findings suggest that biometrics can effectively addressconcerns related to identity fraud and multiple voting, thus ensuring fair and transparent elections.

Biometric technology, such as fingerprint recognition or iris scanning, offers highly accurate and unique identification methods that can effectively deter impersonation and voter fraud. By incorporating biometrics into the voter registration process, authorities can verify the identity of voters with a high degree of certainty, thereby reducing the risk of electoral malpractice.

Furthermore, biometric authentication can streamline the voting process, increasing efficiency and convenience for both voters and election officials. The use of biometric data can expedite the verification process, eliminating the need for manual identity checks and reducing waitingtimes at polling stations. This can lead to increased voter turnout and a more efficient electoralprocess overall.

However, the implementation of biometric technology also presents challenges that must be addressed to ensure its successful utilization. These include data privacy concerns, technological infrastructure requirements, and ensuring accessibility for all voters, regardless of physical disabilities or literacy levels.

Appropriate legal frameworks and safeguards must also be put in place to protect the integrity of biometric databases and prevent their misuse.

In conclusion, the adoption of biometric technology for voter identification and authentication has the potential to significantly enhance the integrity and security of elections. By effectivelyaddressing identity fraud and streamlining the voting process, biometric systems can contributeto fair and transparent electoral processes. It is crucial, however, to address the challenges associated with implementation and to ensure that the technology is accessible, secure, and respects the privacy rights of voters. With proper considerations and safeguards in place, biometric technology can be a valuable tool in safeguarding democracy and upholding the electoral rights of individuals.

REFERENCES

[1] Abayomi-Zannu, T. P., Odun-Ayo, I., Tatama, B. F., & Misra, S. (2020). Implementinga Mobile Voting System Utilizing Blockchain Technology and Two-Factor Authentication in Nigeria. Lecture Notes in Networks and Systems, 121(Ic4s), 857– 872.

[2] Abd Hamid, N., Appunair, C. D. N., Abidin, A. F. A., Mohamed, M. A., Abdul Kadir, M. F., & Mohd Satar, S. D. (2023). a Secure Online Voting System Using Face Recognition Technology. Malaysian Journal of Computing and Applied Mathematics,6(1), 1–9.

[3] Afolabi, O. S. (2020). Biometric Technologies, Electoral Fraud and the Management ofElections in Nigeria and Zimbabwe. Strategic Review for Southern Africa, 42(2).

[4] Ahmad, M., Rehman, A. U. and Ayub, N. (2020) ‘Security, usability, and biometricauthentication scheme for electronic voting using multiple keys’, 16(7).

[5] Amaechi, L. N., & Gerald, E. (2021). The 2015 Biometric Voting System and the Politics of Free, Fair and Sustainable Democracy in Nigeria. Journal of International Politics, 3(1), 9–30.

[6] Annor, E. Y. M. (2020). Development of A Biometric Authentication Voting System for Senior High Schools in Ghana.

[7] Arshad, J. and Farooq-i-azam, M. (2021) *Design and Implementation of a Software- Based Advance Electronic Voting Machine Using Automatic Registration and Fingerprint Identification*.

[8] Based, A., Khan, T. A., & Peash, K. M. (2021). Voter Authentication, Vote Counting & Voter Verifiability in an Electronic Voting Machine Abstract: February.

[9] Bhadoria, R. S., Das, A. P., Bashar, A., & Zikria, M. (2022). Implementing Blockchain- Based Traceable Certificates as Sustainable Technology in Democratic Elections. Electronics (Switzerland), 11(20).

[10] Bharathi, D., Chinnandi, A. M., & Nivedita, A. (2020). Biometric Voting System to Eradicate Illegal Voting. April.

[11] Chakraborty, S., Bej, D., Roy, D., & Mahammad, S. A. (2022). Designing a biometricfingerprint scanner-based, secure, and low-cost electronic voting machine for India. International Journal of System of Systems Engineering, 12(4), 354–370.