WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Dual-Factor Biometric Authentication for Secure Voting: Integration of Smart Cards and Iris Recognition

Prof. Prabhu Kichadi[1], Saraswati S Ullegaddi[2], Rakshita S Hagaragi[3], Balakhushan S Madhale[4], Guruvishnu Kajgar[5]

[1] Asst. Professor, Dept of Computer Science & Engineering, VSM's Somashekhar R. Kothiwale Institute of Technology, Nipani, Karnataka, India, 591237.

[2]Dept of Computer Science & Engineering, VSM's Somashekhar R. Kothiwale Institute of Technology, Nipani, Karnataka, India, 591237

[3] Dept of Computer Science & Engineering, VSM's Somashekhar R. Kothiwale Institute of Technology, Nipani, Karnataka, India, 591237

[4] Dept of Computer Science & Engineering, VSM's Somashekhar R. Kothiwale Institute of Technology, Nipani, Karnataka, India, 591237

[5] Dept of Computer Science & Engineering, VSM's Somashekhar R. Kothiwale Institute of Technology, Nipani, Karnataka, India, 591237

A B S T R A C T

Phishing websites are a major threat to cybersecurity, as they imitate legitimate websites to trick users into sharing sensitive information like passwords and credit card details. This project presents a system to detect phishing websites using machine learning and deep learning techniques. Multiple models, including Decision Tree, Random Forest, Support Vector Machine (SVM), and Artificial Neural Networks (ANN), were trained and tested to find the most accurate and reliable method.

In light of the growing need for secure, transparent, and efficient electoral systems, this research introduces a dual-authentication voting framework that combines smart card technology with iris recognition. Traditional voting mechanisms often face critical issues such as voter fraud, identity theft, multiple voting, and result manipulation. To mitigate these concerns, the proposed system leverages two robust security layers: encrypted smart cards for initial identity verification and iris recognition for biometric authentication. During the registration phase, a voter's personal details, biometric data, and smart card credentials are securely captured and stored in an encrypted central database. On election day, access to the voting interface is granted only after successful verification of both the smart card and the voter's iris scan.

This approach not only strengthens voter authentication but also ensures that the voting process remains tamper-proof and accessible. The system is designed with inclusivity in mind, supporting usability across all voter demographics, including individuals with disabilities. Overall, the integration of these technologies aims to reinforce trust, prevent electoral fraud, and streamline the democratic process.

Keywords: Secure voting system, smart card authentication, iris recognition, biometric verification, electronic voting, dual-factor authentication, electoral integrity, voter identification, tamper-proof voting, inclusive voting interface, biometric security, fraud prevention, secure database, e-governance, transparent elections.

1. Introduction

Elections play a fundamental role in democratic societies, empowering citizens to influence government policies and leadership through their vote. While technological advancements have introduced electronic voting systems, both traditional and modern methods continue to face significant challenges. Common concerns such as voter impersonation, ballot tampering, fraudulent voting, and unauthorized system access threaten the credibility of election outcomes and weaken public trust in democratic institutions. In an era where digital transformation is rapidly reshaping various sectors, the adoption of secure and intelligent technologies is essential to safeguard electoral integrity. To address these issues, this paper presents a Secure Voting System that combines Smart Card technology with Iris Recognition to deliver a dual-layered authentication process. This system is designed to enhance security, ensure voter legitimacy, and improve transparency in the voting process. By integrating smart cards—which securely store encrypted voter data—and iris biometrics—renowned for their uniqueness and permanence—the system provides a reliable defense against identity fraud and unauthorized voting attempts. The process begins with a robust registration phase, where voter details, iris scans, and smart card credentials are securely captured and stored in an encrypted centralized database. On election day, voters must first present their smart cards for validation. Once the card's data is confirmed, the voter undergoes iris scanning to verify their biometric identity. Only after successful dual authentication does the system permit access to the voting interface, which is carefully designed to be intuitive and inclusive, accommodating individuals of all ages and abilities. Votes are then cast and securely transmitted to a central server using encrypted communication channels, ensuring both data privacy and result integrity. By minimizing risks such as vote duplication or manipulation, the system guarantees a fair and tamper-proof electoral process. Additionally, it supports real-time identity verification, reduces queue

* *Corresponding author*. Tel.:+91-9880437187
E-mail address: prabhuk47@gmail.com

times, and enables detailed post-election auditing to maintain accountability and transparency. With its emphasis on security, accessibility, and efficiency, this system represents a significant advancement in the modernization of electoral technologies. This paper introduces a secure voting solution that integrates Smart Card technology with Iris Recognition for dual-factor authentication. By employing encrypted smart cards to store voter credentials and leveraging the precision of iris biometrics, the system ensures that only legitimate voters can participate. The voting process, from registration to ballot casting, is protected through encryption, secure communication protocols, and real-time verification. The approach not only enhances the integrity of elections but also offers transparency, accessibility, and scalability. Elections form the bedrock of democracy, enabling citizens to express their collective will. Yet, electoral systems worldwide are vulnerable to manipulation and security breaches, raising concerns over fairness and accuracy. These risks, if unaddressed, can erode trust in democratic processes and institutions. To mitigate such risks, this paper proposes a technologically enhanced voting system based on smart card authentication and iris recognition. Smart cards serve as secure carriers of voter identity, while iris biometrics ensure one-to-one voter verification. The integration of these technologies provides a reliable and tamper-resistant framework that safeguards both the voting process and the data it generates. Furthermore, the system is designed with user-friendly features to accommodate voters across diverse populations, including the elderly and persons with disabilities.

Nomenclature

This paper uses several key terms integral to understanding the proposed secure voting system. E-Voting refers to the use of electronic systems for casting and counting votes, enhancing speed and efficiency. A Smart Card is a tamper-resistant physical card embedded with a microchip that securely stores a voter's encrypted credentials and personal information. Iris Recognition is a biometric authentication technique that identifies individuals based on the unique and stable patterns in their irises, offering high accuracy in identity verification. Dual-Factor Authentication combines two layers of security—typically something the user possesses (like a smart card) and something inherent to the user (such as biometric data)—to ensure only authorized voters gain access to the voting system. Biometric Verification refers to the use of physiological characteristics, such as iris patterns, to authenticate individuals securely.Encryption is the process of converting sensitive data into a coded format to protect it during storage and transmission. The system employs Secure Communication Protocols to ensure data privacy and integrity during the voting process. A Polling Station is the location—physical or digital—where the authentication and voting occur, while Voter Registration is the initial process where the voter's demographic and biometric data are collected and securely recorded. Other relevant terms include Authentication, the process of validating a voter's identity; Vote Tampering, which refers to any unauthorized modification of votes; and Impersonation, an act of fraudulent voting using another individual's identity. The User Interface (UI) is the platform through which voters interact with the system to cast their votes, designed for accessibility and ease of use. Real-Time Verification ensures instant confirmation of voter credentials, reducing delays. Structure/ DFD

2. Literature survey

Phishing attacks generally follow a structured and deceptive sequence designed to manipulate users into revealing sensitive information. The diagram above illustrates the complete flow of a typical phishing attempt from initiation to exploitation. The process begins when a cyber attacker initiates contact by sending a fraudulent email to the target. This email is often disguised to appear as if it originated from a trusted organization, using familiar logos, language, and sender details to reduce suspicion. The embedded message typically urges the user to act swiftly—such as updating an account, verifying details, or responding to a security alert.

1. **S.P.Sharma,R.K.Gupta(2015)**
   In their work titled "Biometric Authentication for Secure Voting Systems," Sharma and Gupta examine the integration of biometric technologies—specifically fingerprint and iris recognition—as a means to enhance voting security. The authors argue that biometric verification methods offer superior protection compared to conventional security practices like passwords or PINs, which are susceptible to theft or misuse. Their proposed model incorporates iris scanning alongside smart card verification, introducing a dual-authentication system. This layered security approach, according to the authors, can significantly reduce fraudulent activities like impersonation and unauthorized voting, thereby increasing the credibility of the election process.
2. **J.S.Dinesh,M.S.Babu(2017)**
   Dinesh and Babu, in "Smart Card-Based Voting System for Secure Elections," discuss the deployment of smart cards as a mechanism to secure electronic voting. Each voter is issued a personalized smart card containing encrypted data to ensure identity verification at polling stations. The paper emphasizes the smart card's potential to minimize fraudulent voting, enhance security, and prevent vote duplication. Additionally, the authors propose incorporating biometric verification with smart card usage to strengthen the reliability and integrity of the voting system.
3. **M.Kumar,P.K.Agarwal(2019)**
   In "Iris Recognition for Secure Voting and Access Control," Kumar and Agarwal evaluate various biometric identification methods, concluding that iris recognition offers unparalleled accuracy and resistance to forgery. They advocate for a voting system where iris scans are used in tandem with smart card verification to provide dual-layer authentication. This combination, they suggest, offers a highly secure method to confirm voter identity and preserve the confidentiality of the voting process while significantly reducing impersonation risks.
4. **R.P.Mistry,V.A.Patil(2020)**
   Mistry and Patil, in their study titled "E-Voting with Biometric Authentication: A Smart Card Approach," delve into the challenges facing online voting platforms, such as data breaches and unauthorized access. Their solution involves integrating smart card-based identity

verification with biometric methods like fingerprint or iris scans. This dual system ensures that voter credentials are securely stored and that only legitimate voters can participate. The paper highlights the system's potential to prevent fraud and reinforce trust in electronic voting systems.

5. **S.A.Khokhar,M.N.Sharma(2021)**
   Khokhar and Sharma's research, "A Secure and Transparent Voting System Using Biometrics and Smart Cards," proposes a comprehensive approach to electoral security through the fusion of biometric and smart card technologies. They identify common issues in traditional systems, such as ballot manipulation and voter misidentification, and propose iris recognition as a reliable biometric measure. Combined with tamper-proof smart cards, this approach enhances the accuracy of voter verification and prevents unauthorized access, thereby supporting the development of secure and transparent voting systems for future elections.

2.1 Summary of Literature Survey: Secure Voting System Using Smart Card and Iris Recognition

The review of existing literature reveals a strong consensus on the need for secure, efficient, and tamper-proof voting systems. Researchers consistently highlight the vulnerability of traditional and even some electronic voting methods to fraud, identity theft, and data manipulation. Two key technologies—smart cards and iris recognition—have emerged as powerful tools in addressing these concerns.

2.1.1 Smart Card Technology is recognized for its ability to securely store voter credentials and prevent unauthorized access. By embedding encrypted personal information onto a physical card, smart cards reduce the likelihood of identity fraud and eliminate the shortcomings of traditional voter ID methods. They provide a durable and secure medium for voter verification and are widely trusted in sectors like banking and healthcare.

2.1.2 Iris Recognition, on the other hand, is favored for its biometric precision and difficulty to forge. The iris offers a unique and stable pattern for eachindividual, making it an excellent biometric identifier. Studies emphasize the reliability of iris scans in voter authentication, especially when used alongside smart cards. This dual-layer security structure ensures that the person casting the vote is the registered voter, minimizing risks of impersonation or manipulation.

2.1.3 Integrating Smart Cards with Iris Recognition enhances the voting system's integrity. The smart card serves as the initial validation tool, while iris recognition adds a second, more secure level of identity confirmation. Together, they create a robust authentication framework that deters fraudulent activities and strengthens the reliability of electoral outcomes.

2.2.4 Benefits of Dual Authenticationinclude not only improved security but also increased voter trust and system efficiency. The reviewed works point out that dual-authentication systems streamline the voting process by reducing verification time and minimizing errors. Moreover, these systems are designed to be accessible, supporting user-friendly interfaces for voters of all demographics.

2.1.5 E-Voting Security Enhancementsare another area of focus. Several researchers advocate for using biometric-smart card combinations to safeguard digital voting platforms. These systems provide end-to-end encryption, secure data transmission, and detailed audit logs, which contribute to a transparent and verifiable election process. Ultimately, the integration of smart cards and iris recognition presents a promising solution for modern, fraud-resistant voting systems.

3. Objective

The main aim of this project is to develop a highly secure and reliable voting system that leverages the combined power of smart card technology and iris recognition for voter authentication. This dual-authentication strategy is designed to overcome the typical security flaws found in both conventional and existing electronic voting methods. The specific goals of the system are outlined below:

3.1 To implement a robust authentication mechanism:

The system will integrate smart cards and iris biometrics to ensure that only verified and authorized voters can access the voting platform, effectively eliminating impersonation and fake voting attempts.

3.2 To secure sensitive voter information:

Smart cards will be used to store encrypted voter data, offering a secure method to safeguard personal credentials from tampering, theft, or unauthorized access.

3.3 To minimize election fraud:

By incorporating iris recognition, a unique and non-replicable biometric identifier, the system adds a strong second layer of security to confirm that the individual casting the vote is the rightful registrant.

3.4 To establish a transparent and verifiable system:

The inclusion of both biometric and smart card verification allows for clear audit trails, helping election officials trace voting activity without compromising voter privacy, thereby promoting accountability and transparency.

3.5 To create an intuitive and accessible user experience:

Designed with ease-of-use in mind, the system ensures that both the smart card reader and iris scanning process are quick and straightforward, accommodating users of all age groups and backgrounds.

3.6 To maintain voter confidentiality:

Although each voter's identity is confirmed before accessing the ballot, the system is structured to ensure that the vote itself remains anonymous and cannot be linked back to the individual, thereby protecting voter privacy.

3.7 To seamlessly combine card-based and biometric technologies:

A key goal is to achieve smooth integration between iris recognition and smart card modules within existing electoral frameworks, making the solution viable for both on-site and remote (online) voting environments.

3.8 To build public trust in elections:

By eliminating common vulnerabilities such as multiple voting, vote rigging, and unauthorized access, the system is designed to reinforce the integrity of the election process and increase public faith in democratic outcomes.

3.9 To enhance efficiency and ensure scalability:

The system aims to streamline the voting process by automating verification steps, reducing delays, and minimizing manual work. It will also be scalable to handle elections of varying sizes—from small community polls to nationwide contests—ensuring consistent performance under different workloads.

4. Designing System

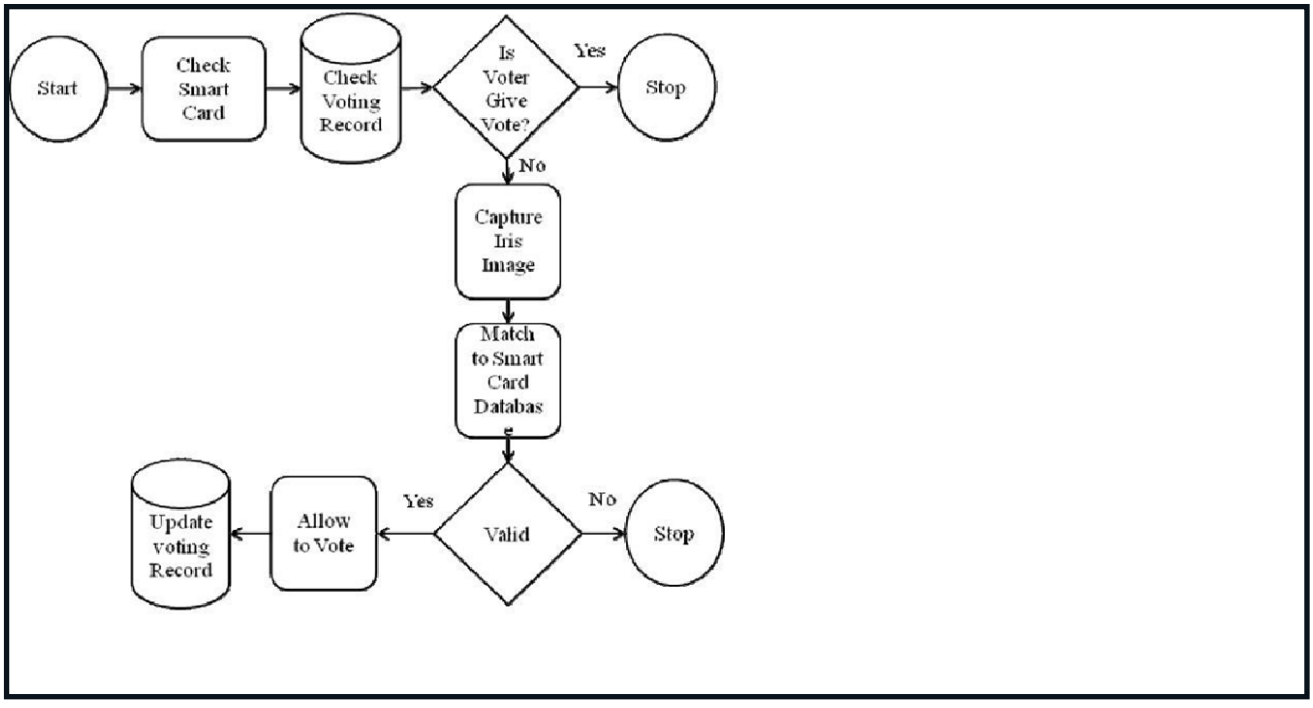

Fig Data flow diagram

The architecture of the proposed Secure Voting System is designed to ensure a safe, reliable, and user-friendly electoral process by integrating smart card and iris recognition technologies. It consists of multiple interdependent components working together to authenticate voters, preserve privacy, and protect the integrity of the election. The entire system is organized into several functional phases, as outlined below:

4.1 Voter Registration Phase

During the registration stage, voters provide their personal information—including name, address, contact details, and official identification—along with a high-resolution iris scan. This biometric data is collected using advanced iris scanning equipment.

Voter credentials and biometric information are encrypted and embedded into a secure smart card, which includes a unique identifier such as a digital certificate or voter ID. The same encrypted data is also stored in a central voter database, forming the foundation for future authentication during elections.

4.2 Voter Authentication Phase

On election day, the authentication begins with the voter inserting their smart card into a verification terminal. The system first checks the integrity of the smart card and validates the unique voter identifier. Following smart card validation, the system prompts the user to complete a biometric scan using an iris scanner. The newly captured iris image is then compared with the pre-stored iris data encrypted within the smart card. If the biometric match is successful, the voter is allowed to proceed; if not, re-authentication is requested or access is denied based on the result.

4.3 Voting Process

After both identity checks are successful, the system confirms the voter's eligibility, ensuring they have not previously voted. Eligible voters are then presented with a digital ballot on a touchscreen interface. Voters select their candidates or choices and are given an opportunity to review their selections before submitting. Once confirmed, the vote is finalized and recorded in an encrypted format that preserves anonymity while allowing validation.

4.4 Secure Vote Transmission

Each vote is protected through strong encryption algorithms such as RSA or ECC to prevent tampering and unauthorized access. The encrypted vote is transmitted over a secure network (utilizing protocols like TLS/SSL) to a centralized election server, where results are securely collected and stored.

4.5 Vote Counting and Results Management

The central server stores all incoming encrypted votes until the election ends. After voting concludes, the system decrypts votes using secure, authorized decryption keys to perform vote tallying. Election administrators can monitor the process in real-time using administrative tools, which provide insights into voting activity, turnout, and system performance without compromising individual privacy.

4.6 Logging and Auditing

The system maintains detailed audit logs of all activities, including voter authentication events, successful and failed attempts, vote submissions, and system-level actions. These logs support transparency and accountability. While voter identity is verified before voting, the actual vote remains completely anonymous to ensure privacy and prevent traceability.

4.7 Voter Interaction Interface

The user interface is designed to guide voters' step-by-step—from inserting the smart card and completing the iris scan to casting their vote. It emphasizes ease of use and quick navigation. To support diverse voter populations, the system includes accessibility features such as voice guidance and multilingual support, helping individuals with disabilities or language barriers participate independently.

4.8 Data Security and Privacy Measures

Modern encryption standards (e.g., AES-256) are employed to secure all stored and transmitted data. Voter credentials and biometric records are kept in encrypted databases with stringent access controls, ensuring that only authorized officials can retrieve sensitive information. Importantly, no personally identifiable data is linked to the vote during the tallying process, ensuring privacy while maintaining system integrity.

4.9 Reporting and Result Publication

After the voting process concludes, the system compiles the final results and presents them securely to authorized election bodies. With appropriate safeguards, election results can also be made available to the public. Detailed analytics and system reports are generated, covering aspects such as voter participation, system usage statistics, and operational performance, which are crucial for future audits and evaluations.

4.10 Maintenance and System Updates

The architecture is designed to support regular updates, security patches, and feature enhancements. Smart card firmware and iris recognition software can be upgraded to improve accuracy and resilience.In addition, the system performs regular backups and follows a well-defined disaster recovery plan to ensure quick restoration of services in the event of hardware failure or cyberattack.

5. Methodology

The development of a Secure Voting System that incorporates both Smart Card and Iris Recognition technologies involves a structured, multi-phase approach. This methodology ensures that the final system is secure, efficient, scalable, and user-centric. The key stages of development include system planning, voter registration, authentication, voting, vote handling, security enforcement, and testing.

5.1 System Design and Planning

The first step is to establish a detailed system blueprint. This phase includes:

1. Requirement Analysis: Identifying the core features and constraints of the system, such as secure dual-factor authentication, protection of voter privacy, system scalability, and the need for smart card and biometric integration.
2. Architectural Planning: The architecture comprises modules for voter enrollment, identity verification, vote casting, and result processing. Security protocols like TLS/SSL are defined at this stage to secure data exchanges.
3. Database Structure: A centralized, encrypted database is designed to store voter records, biometric templates, and voting logs. The database is optimized for quick retrieval while maintaining strict access control.

5.2 Voter Enrollment

This phase ensures that only verified individuals are included in the voting system.Smart Card Generation: Each voter is issued a smart card that holds encrypted personal and biometric data, including a unique voter ID and iris scan.

1. Biometric Capture: Using a high-precision iris scanner, each voter's iris pattern is digitized and converted into a biometric template stored on the smart card.
2. Secure Storage: All collected data is encrypted using strong algorithms like AES-256 and stored both locally on the smart card and in a secure central database, with restricted access for authorized personnel only.

5.3 Voter Authentication

This critical stage confirms the identity of each voter before allowing access to the ballot.

1. Smart Card Verification: Voters insert their smart cards into the terminal, where the card's integrity and unique identifier are validated against the central database.
2. Iris Scan Matching: The system captures the voter's iris pattern during login and compares it with the template stored on the card. If the data matches, the voter is allowed to proceed.
3. Data Validation: To prevent tampering, hash verification techniques ensure that smart card data remains unaltered. Only after successful verification is access to the voting screen granted.

5.4 Voting Procedure

Once identity is confirmed, the voter is presented with the interface to make their choices.

1. Ballot Display: The electronic ballot is shown on the screen, listing all candidates and propositions. The interface includes features for accessibility, such as multi-language support and visual enhancements.
2. Vote Selection: The voter marks their choices, reviews them, and confirms. The vote is then encrypted using public-key cryptography to ensure confidentiality.

3. Vote Submission: The finalized vote is securely transmitted to a central server, tagged with a unique—but anonymous—voter ID to prevent multiple votes while preserving voter privacy.

5.5 Vote Transmission and Counting

After the vote is cast, it goes through a secure transmission and tallying process.

1. Secure Vote Transfer: Votes are encrypted using asymmetric algorithms like RSA or ECC and sent through a protected network using TLS/SSL.
2. Decryption and Tallying: Once the election ends, authorized officials use secure private keys to decrypt and count the votes. The results are compiled automatically and accurately.
3. Audit Trails: The system logs every transaction—including timestamps and terminal IDs—to support audits and verify the integrity of the process without exposing voter identities.

5.6 Security Framework

Robust security practices are integrated into every component of the system.

1. Data Encryption: All critical data—from smart card credentials to biometric images and vote records—is encrypted to prevent data theft and tampering.
2. Dual Authentication: The combined use of a smart card and iris scan creates a two-layer identity verification process that significantly reduces impersonation risks.
3. Secure Communication: All data sent between system components is transmitted over encrypted channels, ensuring that interception or manipulation is not possible.
4. Role-Based Access: Access to sensitive information is restricted to authorized officials only, with all actions logged and auditable.

5.7 System Testing and Validation

To guarantee the system's reliability, several levels of testing are performed:

1. Module Testing: Each individual component, such as the iris scanner, card reader, and vote submission interface, is tested for proper functionality.
2. System Integration Testing: The interactions between subsystems—like the handshake between smart card authentication and biometric verification—are tested to ensure end-to-end compatibility.
3. Security Testing: Ethical hacking and penetration tests are conducted to identify vulnerabilities and validate the effectiveness of security protocols.
4. Usability Testing: The system is tested with real users to ensure ease of use, with a focus on inclusivity for voters with different levels of digital literacy or physical disabilities.

6. Hardware and Software requirements

Sl. No.	Hardware Component	Description & Functionality	Example Devices
1	Smart Card Reader	Reads encrypted voter data stored on smart cards for identity verification. Supports both contact and contactless modes.	ACR122U, SCR3310v2.0
2	Iris Scanner	Captures high-resolution images of the iris and converts them into biometric templates for verification. Uses infrared technology and is non-contact.	IRIS ID iCAM7000, Crossmatch Verifier 300
3	Voting Terminal	Acts as the main user interface; handles input, displays ballot, processes vote, and interacts with smart card and iris scanner.	Desktop PC, Raspberry Pi, Intel NUC
4	Central Server	Stores voter records, vote logs, and handles encryption/decryption for secure vote tallying.	Dell PowerEdge R740, AWS, Microsoft Azure
5	Network Infrastructure	Facilitates secure communication between terminals and server using encrypted protocols like SSL/TLS.	Cisco Catalyst Switch, Juniper EX Series, Wi-Fi APs
6	Backup Power Supply	Provides uninterrupted power to system components to ensure seamless operation during power failures.	APC Smart-UPS 1500VA, CyberPower CP1500AVRLCD

Sl. No.	Software Tool	Description & Functionality	Technologies/Examples
1	Django Framework	Web application framework for managing voter data, authentication, vote submission, admin controls, and security.	Django (Python), Django Admin Panel
2	Database System	Securely stores encrypted voter data, biometric templates, and voting records. Integrated with Django ORM.	SQLite (for demo), PostgreSQL/MySQL (for production)
3	OpenCV	Used for iris image acquisition, preprocessing, segmentation, enhancement, and feature extraction.	OpenCV (Python/C++)
4	NumPy	Performs numerical computations needed for image processing, feature matching, and biometric comparison.	NumPy Library (Python)
5	Iris Recognition Algorithms	Algorithms to generate iris codes and compare using metrics like Hamming Distance to match biometric patterns.	Daugman's Algorithm, Hamming Distance
6	Security Protocols	Encrypts and decrypts data during storage and transmission using symmetric and asymmetric encryption. Also prevents threats like SQL injection or CSRF.	AES-256, RSA, SSL/TLS
7	Operating System	Platform for deploying server and terminal software securely and efficiently.	Windows/Linux (Ubuntu), Raspbian (for Pi-based UI)

7. Applications and Advantages

The core application of the proposed secure voting system is in conducting official elections at national, state, and local levels. Through the integration of iris recognition and smart card technology, the system ensures that only verified individuals are able to cast their vote, enhancing both the security and accuracy of the electoral process. This system is ideal for implementing online voting platforms, enabling citizens to vote from remote locations while maintaining stringent authentication protocols. The dual-authentication setup—iris and smart card—ensures that remote votes are legitimate and secure from unauthorized access. Organizations and corporate entities can use this system to facilitate secure internal voting, such as board member elections, policy approvals, or shareholder decisions. Only authorized members can access the system and cast a vote, ensuring integrity and transparency.

For surveys that require verified participation—such as public policy feedback or community decision-making—the system ensures each response is genuine, authenticated, and tamper-proof. This is particularly useful in government or private sector polling where data integrity is critical.

Schools, colleges, and universities can apply this system for student council elections, faculty voting, or internal decision-making processes. It ensures that only eligible participants can vote and that votes are securely recorded and counted. Governments can adopt the system for public consultations, referendums, or participatory budgeting processes where identity verification is vital to uphold legitimacy and confidence in citizen feedback. The use of two independent authentication methods—biometric (iris scan) and smart card—provides a strong multi-factor security system, significantly lowering the chances of unauthorized access or manipulation. The dual-layer verification ensures that only the rightful, registered individual can vote, effectively preventing impersonation, duplicate voting, and other forms of electoral fraud. Iris patterns are highly unique and do not degrade with age or usage, unlike fingerprints or facial features. This ensures highly reliable and precise voter identification. The system is designed with usability in mind. Voters can complete the authentication and voting process quickly and intuitively, making it accessible to individuals of all ages and technical backgrounds. Votes are recorded and transmitted in real-time, allowing for immediate tabulation and monitoring by election officials. This ensures fast, efficient result processing and timely election outcomes. The system minimizes reliance on paper ballots, physical security staff, and manual counting—reducing long-term operational costs and improving the sustainability of the election process. Designed to handle elections of varying sizes, the system can scale up from small institutional votes to full-scale national elections, without compromising performance or reliability. Every transaction, from voter authentication to vote casting, is logged in a secure audit trail. These logs can be reviewed to verify the integrity of the election, promoting transparency and accountability.

By automating authentication and vote processing, the system significantly reduces the risk of errors caused by manual entry or handling, ensuring a more accurate and efficient election process.

The system can be enhanced with support for audio guidance, language selection, and screen-readers, ensuring that voters with disabilities or language barriers can participate comfortably and independently.

Advanced encryption protocols protect sensitive data such as voter identity and vote content, both during storage and transmission. This maintains the confidentiality and integrity of every vote cast.

The digital and paperless nature of the system reduces the environmental impact traditionally associated with printed ballots and physical logistics, contributing to a greener voting approach.

REFERENCES

1. S. Sharma, R. Verma, and A. Kumar, "A Secure Voting System Based on Iris Recognition and Smart Cards," International Journal of Computer Science andTechnology, vol. 11, no. 2, pp. 125-130, May 2023.
2. Patel, M. Joshi, and R. S. Yadav, "Biometric Authentication System for Voting Using Iris Recognition," IEEE Transactions on Industrial Informatics, vol. 17, no. 6, pp. 3780-3792, June 2021. DOI: 10.1109/TII.2020.3018554.
3. P. S. Mehta and R. Gupta, "Securing Voting Systems Using Smart Cards and Biometric Authentication," Journal of Cryptography and Information Security, vol. 9, no. 3, pp. 215-227, Oct. 2022.
4. K. D. Kumar and S. Singh, "Smart Card-Based Secure Voting System with Biometric Iris Verification," IEEE Access, vol. 7, pp. 43857-43866, Jan. 2020. DOI: 10.1109/ACCESS.2019.2966071.
5. R. Sharma and P. Gupta, "Design and Implementation of Secure Voting System Using Smart Cards and Biometric Authentication," Computers & Security, vol. 88,
6. zpp. 8598, July 2020. DOI: 10.1016/j.cose.2019.101576.
7. H. Li and T. Zhang, "Advanced Biometric Systems for Secure Voting: A Review of Iris Recognition Technology," International Journal of Computer Applications, vol. 183, no. 4, pp. 45-52, Nov. 2020.