IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, December 2024

A Review on Online Voting System using Face Recognition and Blockchain

Nandan S[1], Mr. Pradeep Nayak[2], Amar B M[3], Manikanta[4], Karthik Madakari T P[5]
Students, Department of Information Science & Engineering[1,2,3,4]
Assistant Professor, Department of Information Science & Engineering[5]
Alva's Institute of Engineering and Technology, Mijar, Karnataka, India

Abstract: *Online voting systems represent a transformative approach to modernizing electoral processes, offering benefits such as increased accessibility, security, and efficiency. This paper explores the design, implementation, and challenges of online voting systems, with a particular focus on the integration of biometric authentication, encryption, and blockchain technology. These systems aim to address the critical issues of voter identity verification, fraud prevention, and the integrity of election results. The methodology for creating an online voting system involves a multi-stage process, including requirement analysis, system design, development, security implementation, testing, deployment, and post-election auditing. Despite the numerous advantages, challenges such as cybersecurity threats, privacy concerns, and digital accessibility remain. This paper discusses the importance of addressing these challenges to ensure the security, transparency, and inclusivity of online voting. By adopting robust security measures and considering the legal and technological landscape, online voting systems can enhance voter participation and transform electoral practices, providing a reliable and efficient alternative to traditional voting methods*

Keywords: election integrity, digital accessibility, biometric authentication

I. INTRODUCTION

The ease of remote voting is combined with cutting-edge security and authentication features made possible by technology in an online voting system that uses image processing. In order to verify voter identity using biometric features like fingerprint analysis, facial recognition, or signature verification, image processing a subfield of artificial intelligence and computer visionis essential.

Voters register using this technology by supplying biometric information and personal details, which are safely saved for future verification. Voters' photos or their credentials are taken throughout the voting process, and sophisticated algorithms are used to extract distinctive traits for identification matching. This strategy guarantees that only eligible voters can cast ballots and stops fraudulent acts like document fabrication and impersonation.Additionally, image processing makes voting easier for people with disabilities or those living in distant areas by allowing them to use cameras on their devices.

The system must handle issues including privacy concerns, system reliability, and the digital divide despite its many benefits, which include improved security, efficiency, and transparency. By overcoming these obstacles, image processing-based online voting systems have the potential to transform the democratic process and make it safer, inclusive, and reliable for the digital era. Rapid technological development has changed how societies engage with essential processes, like voting, making them more accessible, effective, and safe. By using digital platforms, online voting methods allow voters to cast their ballots from a distance, doing away with the necessity of physically visiting polling places. By solving important issues like voter verification, security, and fraud prevention, image processing is included into such systems to further improve their functionality. Analyzing and modifying visual data is the focus of the artificial intelligence (AI) and computer vision branch of image processing.

By using facial recognition, fingerprint analysis, or signature verification, it ensures safe voter identification and authentication in online voting systems. The system can process voter photos or their documentation to: An image-processing-powered online voting system is a futuristic approach to elections that combines ease, efficiency, and

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, December 2024

security. Such solutions have the potential to revolutionize electoral procedures and fortify democratic norms globally by tackling ethical and technical issue.

Access Control

To guarantee that only eligible and authorized users can access the platform and take part in the voting process, access control is crucial in online voting systems. To preserve election integrity, protect voter data, and guarantee vote confidentiality, it uses several tiers of security procedures. A crucial component is user authentication, which uses biometric verification methods like fingerprint, iris, or facial recognition in addition to two-factor authentication (2FA) systems that combine passwords or PINs with one-time passwords (OTPs) delivered to registered devices.

Furthermore, voter legitimacy is guaranteed by document verification using official identification. To restrict access to sensitive functions, Role-Based Access Control (RBAC) allocates rights based on user roles, including administrators, auditors, and voters. Time-limited sessions and encrypted communication protocols, including HTTPS and SSL/TLS, are enforced by secure session management to safeguard data while it is being transmitted. Database security, which frequently encrypts this data to prevent unwanted access, makes sure that only authorized users may access private voter information and ballots. Sophisticated fraud detection systems keep an eye out for questionable activity, such as repeated login attempts or access from unfamiliar devices, and flag any irregularities for additional examination. By storing votes as unchangeable entries, guaranteeing transparency, thwarting tampering, and protecting voter anonymity, blockchain technology improves access control.

These measures collectively enhance security, protect data privacy, and maintain election integrity. However, implementing such systems poses challenges, including balancing security with user convenience, addressing emerging cybersecurity threats, and ensuring accessibility for all voters, including those less familiar with technology. By overcoming these challenges, access control mechanisms can make online voting systems secure, efficient, and trustworthy for all stakeholders.

Biometric

By utilizing distinct physiological or behavioral traits, biometric technology in an online voting system improves security, accuracy, and voter authentication. To make sure that only eligible voters may access the platform and cast their ballots, biometric systems include capabilities like voice recognition, iris patterns, fingerprints, and facial identification. Voters submit their biometric information during the registration process, and it is safely kept in an encrypted database for later validation. In order to verify the voter's identification, the system records their biometric input when voting and compares it with the data that has been saved.For example, fingerprint algorithms identify distinct ridge patterns, while face recognition examines facial landmarks. Known for its great accuracy, iris recognition analyzes the complex eye textures. By limiting the possibility of voter impersonation or identity theft, these techniques guarantee that each person can only cast one ballot. Additionally, biometric solutions increase accessibility by providing a simple and rapid verification process, which lessens the need for physical documents or passwords.

Nevertheless, there are difficulties in integrating biometrics into online voting systems. The safe processing and preservation of private biometric information raises privacy issues. Reliable software and top-notch equipment are necessary to avoid mistakes like false positives or negatives. It's also critical to make sure the system is accessible to those with impairments or who have trouble supplying biometric information, such as worn fingerprints or facial obstructions. Notwithstanding these difficulties, biometric integration offers a safe and convenient means of maintaining election integrity while also greatly improving the dependability and openness of online voting systems.

Authentication

In order to confirm voters' identities and guarantee that only those with permission can access the platform and cast their ballots, authentication is a crucial step in online voting systems. The integrity of the voting process is maintained, voter data is safeguarded, and unwanted access is avoided via a strong authentication system. Multiple layers of authentication are usually used by the system to improve security while preserving user comfort. Biometric authentication, which makes use of distinctive physiological characteristics like fingerprints, facial recognition, or iris scans, is among the most successful techniques. By ensuring that each voter is individually identifiable, biometric

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, December 2024

solutions lower the possibility of multiple voting attempts or impersonation. Furthermore, two-factor authentication (2FA), which combines a voter's knowledge (like a password or PIN) with their possessions (such a one-time password given to a registered mobile device), is frequently employed to increase security. The system may additionally include document authentication, which involves scanning and validating voter cards or government-issued identification documents using image processing algorithms, for additional verification.

The technology verifies that the voter's credentials match those kept in a secure database during the authentication process. Sensitive information is protected during transmission by encryption protocols like SSL/TLS, which guarantee that it stays private. It is also possible to improve accessibility by implementing alternate techniques like voice-based verification or QR codes, particularly for voters with impairments.

Despite its benefits, authentication in online voting systems faces challenges, such as ensuring privacy, managing false positives or negatives in biometric verification, and safeguarding against cyberattacks. A balance between robust security measures and ease of use is essential to encourage voter participation. When implemented effectively, authentication mechanisms provide a secure and reliable foundation for online voting, ensuring trust in the electoral process.

Face recognition

One cutting-edge biometric technology that guarantees safe and effective voter authentication in an online voting system is face recognition. This technique improves the security and usability of the system by using each person's distinct face traits to confirm their identification. Voters submit their facial information throughout the registration process, and it is photographed and analyzed to extract important characteristics like the distance between eyes, nose shape, or jawline contour. For later use during the voting process, this information is safely kept in an encrypted database.

When a voter casts a ballot, the system records a live video or picture of them and compares it with the recorded information using facial recognition algorithms. High-accuracy matching is frequently achieved using methods such as convolutional neural networks (CNNs), which are based on deep learning, even when there are slight variations in appearance or different lighting conditions. Face recognition speeds up and simplifies the authentication process for users by doing away with the need for passwords, PINs, or paper documents.Because each face is distinct and difficult to duplicate.

Benefits

- **Convenience and Accessibility** Voters can cast their ballots online from any location with a device that can connect to the internet, doing away with the requirement to physically visit polling places. People with disabilities, those living in distant places, and foreign-born citizens especially benefit from this.
- **Increased Voter Turnout** By reducing barriers such as travel, long queues, or time constraints, online voting encourages broader participation, potentially increasing voter turnout and strengthening democratic representation.
- **Enhanced Security** Advanced authentication methods, including biometrics, two-factor authentication, and blockchain technology, ensure that votes are cast only by eligible individuals, reducing the risk of fraud and tampering
- **Cost-Effectiveness** Online voting reduces the costs associated with traditional voting methods, such as printing ballots, staffing polling stations, and transporting materials. This makes elections more economical and environmentally friendly.
- **Faster Results** Digital systems automate vote collection and counting, significantly reducing the time required to tally results and announce outcomes compared to manual counting processes.

Challenges

While online voting systems offer numerous advantages, they also face several challenges that must be addressed to ensure their success and reliability. One of the primary concerns is cybersecurity; online voting systems are vulnerable to hacking, phishing attacks, and data breaches that could compromise voter information or alter election results.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, December 2024

Ensuring the security of sensitive voter data, such as personal details and voting preferences, requires advanced encryption and robust security protocols. Another challenge is voter authentication—ensuring that only eligible voters can cast their ballots.

While methods like biometrics and two-factor authentication are commonly used, there is still a risk of identity theft, impersonation, and false matches, particularly with less accurate biometric systems or when voters' physical appearance changes. Privacy is also a critical issue; safeguarding voter anonymity while preventing tampering with votes is essential, as any breach of privacy could undermine public trust in the system. Furthermore, digital accessibility presents a significant barrier; not all voters have access to the necessary technology or the digital literacy to navigate an online voting platform. For elderly voters, those in rural areas, or people with disabilities, participating in online voting could be difficult.

Additionally, legal and regulatory challenges arise, as many countries have strict laws governing voting processes and the use of electronic systems, requiring updates to accommodate online voting securely and fairly. Finally, there are concerns over system reliability—ensuring that the platform remains stable and responsive under high traffic conditions, particularly during peak voting times, is crucial for preventing outages or delays. Addressing these challenges is necessary for the widespread adoption of online voting systems, making them secure, accessible, and trusted by the public.

II. METHODOLOGY

The methodology for designing and implementing an online voting system involves a series of steps that ensure the system is secure, reliable, user-friendly, and legally compliant. The process typically includes system planning, design, development, testing, and deployment, all guided by security, privacy, and accessibility considerations. Below is an overview of the key stages in the methodology:

The first step involves gathering the requirements for the online voting system. This includes understanding the legal and regulatory framework, determining the needs of voters and election authorities, and identifying the features necessary to support voter registration, authentication, vote casting, and result tallying. Security, scalability, and user accessibility are key considerations at this stage.

Based on the requirements, the system architecture is designed. This involves creating a framework for both the front-end and back-end components. The front-end allows voters to interact with the system through user-friendly interfaces, while the back-end handles vote processing, data storage, and security features. Key design considerations include:

Once the system design is finalized, the development phase begins. This includes coding the system components, integrating necessary technologies (such as biometric authentication, digital signatures, and blockchain for vote integrity), and setting up databases for voter registration and ballot storage. During this stage, developers also focus on ensuring that the system is responsive, accessible, and compatible with different devices (e.g., smartphones, tablets, PCs).A core element of the online voting system is ensuring voter data confidentiality, integrity, and privacy.

After the election is completed, the system generates detailed reports, which can be audited for accuracy and transparency. Blockchain-based systems allow for easy verification of vote integrity, providing voters and election authorities with trust in the system's reliability. Any issues encountered during the election process are documented and analyzed for future improvements.

Ongoing maintenance is essential to address any system bugs, security vulnerabilities, or changes in legal requirements. Periodic upgrades may also be necessary to improve system performance, incorporate new technologies, or address emerging security threats.

III. CONCLUSION

in conclusion, the development and implementation of an online voting system offer significant advantages, such as increased accessibility, enhanced security, and more efficient election processes. By leveraging advanced technologies like biometric authentication, encryption, and blockchain, online voting systems can ensure secure voter identity verification, prevent fraud, and maintain the integrity of the election results.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, December 2024

The methodology behind such systems involves a structured approach, from requirement analysis and system design to rigorous testing, deployment, and post-election auditing. However, challenges such as cybersecurity threats, privacy concerns, digital accessibility, and legal compliance must be carefully addressed to ensure the system's success.

REFERENCES

[1]. Abd Hamid, Nazirah, Citra Devi Nair Appunair, Ahmad Faisal Amri Abidin, Mohamad Afendee Mohamed, Mohd Fadzil Abdul Kadir, and Siti Dhalila Mohd Satar. "A SECURE ONLINE VOTING SYSTEM USING FACE RECOGNITION TECHNOLOGY." Malaysian Journal of Computing and Applied Mathematics 6, no. 1 (2023): 1-9.

[2]. Rura, Lauretha, Biju Issac, and Manas Kumar Haldar. "Online voting system based on image steganography and visual cryptography." Journal of computing and information technology 25, no. 1 (2017): 47-61.

[3]. Kajal, B., Vala, B. and Patel, W., 2021, May. A Review of Online Voting System Security based on Cryptography. In Proceedings of the International Conference on Smart Data Intelligence (ICSMDI 2021).

[4]. Sulaiman, M.M.K.M.M., Othman, M.F.I., Shah, W.M., Hassan, A., Harum, N. and Alseadoon, I.M., 2021. An Online Voting System using Face Recognition for Campus Election. Journal of Advanced Computing Technology and Application (JACTA), 3(1), pp.37-42.

[5]. Prabhu, S.G., Nizarahammed, A., Prabu, S., Raghul, S., Thirrunavukkarasu, R.R. and Jayarajan, P., 2021, March. Smart online voting system. In 2021 7th International conference on advanced computing and communication systems (ICACCS) (Vol. 1, pp. 632-634). IEEE.

[6]. Mark, Leslie, Vasaki Ponnusamy, Arya Wicaksana, Basilius Bias Christyono, and Moeljono Widjaja. "A secured online voting system by using blockchain as the medium." The Smart Cyber Ecosystem for Sustainable Development (2021): 405-430.

[7]. Purandare, H.V., Saini, A.R., Pereira, F.D., Mathew, B. and Patil, P.S., 2018, January. Application for online voting system using android device. In 2018 International Conference on Smart City and Emerging Technology (ICSCET) (pp. 1-5). IEEE.

[8]. Haroutunian, M.E., Margaryan, A.S. and Mastoyan, K.A., 2024. New Approach for Online Voting Ensuring Privacy and Verifiability. Programming and Computer Software, 50(Suppl 1), pp.S60-S68.

[9]. Hazzaa, F.I., Kadry, S. and Zein, O.K., 2012. Web-based voting system using fingerprint: design and implementation. International Journal of Computer Applications in Engineering Sciences, 2(4), pp.404-409.

[10]. Pawade, D., Sakhapara, A., Badgujar, A., Adepu, D. and Andrade, M., 2020. Secure online voting system using biometric and blockchain. In Data Management, Analytics and Innovation: Proceedings of ICDMAI 2019, Volume 1 (pp. 93-110). Springer Singapore.

[11]. Ipinnimo, O., Ogbemhe, J., Mumuni, Q., Owoeye, S.O. and Olurombi, A., 2024. FACIAL RECOGNITION-BASED ONLINE VOTING SYSTEM WITH TWO-FACTOR SECURITY. JOURNAL OF INNOVATION SCIENCE AND TECHNOLOGY, 3(1).

[12]. Nair, KC Deepika, and I. Mamatha. "Online Voting System Based on Face Recognition and QR Code Authentication." In International Conference on Robotics, Control, Automation and Artificial Intelligence, pp. 619-629. Singapore: Springer Nature Singapore, 2022.