IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

## IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 5, May 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2024 ||

| DOI: 10.15680/IJIRCCE.2023.1205083 |

# E – Voting System Using A Deep Learning Model

**Advaith Ramana S[1], Jaiguganesh K[2], Keerthana P[3], Kavishree S[4]**

[1,2,3]U.G. Student, Dept. of I.T., Sri Venkateswara College of Engineering, Sriperumbudur, Tamil Nadu, India

[4]Assistant Professor, Dept. of I.T., Sri Venkateswara College of Engineering, Sriperumbudur, Tamil Nadu, India

**ABSTRACT**: The foundation of democracy and organization is the voting system. In recent decades, there have been numerous effective modifications to the electoral system. The largest majority rule nation in the world, India, still conducts its elections using either Electronic Voting Machines (EVM) or Secret Ballet Voting (SBV), both of which are expensive, and require a lot of manual labor. Only identity documentation was validated under the current method, increasing the likelihood of bogus votes. We created a web-based smart voting system and an innovative face detection and recognition technique in order to prevent the aforementioned problems. The Residual Network (ResNet) architecture, which is renowned for its exceptional performance in image recognition tasks, forms the foundation of the electronic voting system. ResNet facilitates the reliable and genuine analysis of voting data by leveraging the hierarchical feature extraction capabilities of deep convolutional neural networks (CNNs). Through extensive testing and validation, we demonstrate how ResNet can reliably identify voters, tabulate ballots with unprecedented precision, and discover abnormalities. People can use the complete internet architecture to safeguard their votes from anywhere in the world. Voter fraud is reduced when the ID of appearances is used, and voters who are recognized by the system and who are enrolled in the political contest are allowed to cast ballots. As a result, the framework is the best way to make the decision thanks to the technique.

**KEYWORDS**: Residual Network (ResNet), Convolutional neural network (CNNs).

## I.INTRODUCTION

The advent of the digital era has indeed brought about a significant transformation, placing a heightened emphasis on the need for secure and efficient electoral processes. As a result, electronic voting systems have emerged as a prominent solution to address these critical aspects. This research seeks to introduce a groundbreaking approach that not only elevates the integrity and accuracy of voting mechanisms but also pioneers the integration of cutting-edge face recognition technology utilizing the ResNet architecture. By proposing this innovative E-voting system, we are taking a substantial step forward in the ongoing quest for elections that are not only robust and secure but also easily accessible to all eligible voters. Through the strategic incorporation of advanced facial recognition algorithms, this system brings forth an additional layer of identity verification, ensuring that registered voters can confidently participate in the electoral process. Leveraging the power of ResNet architecture, meticulously trained on a vast and diverse dataset of facial images, the system achieves instantaneous and precise voter identification and authentication. This sophisticated approach acts as a powerful deterrent against potential threats such as voter fraud and impersonation, reinforcing the system's reliability and trustworthiness. One of the primary advantages of this groundbreaking system lies in its ability to enhance and streamline the voting experience for citizens at large. By eliminating the traditional reliance on physical voter identification documents, it offers a seamless and user-friendly pathway for individuals to exercise their democratic rights securely and conveniently. In summary, the proposed system represents a significant leap forward in modernizing electoral processes by combining technology and security measures to ensure efficient and trustworthy elections.

## II.RELATED WORK

In [1] "DVTChain: A blockchain-based decentralized mechanism to ensure the security of digital voting system" authored by Syada Tasmia Alvi, Mohammed Nasir Uddin, Linta Islam, and Sajib Ahamed presents a novel approach to enhancing the security of digital voting systems using blockchain technology. The authors propose DVTChain, a decentralized system designed to address the vulnerabilities inherent in traditional electronic voting systems. Through a comprehensive literature review, the paper identifies key challenges in existing digital voting mechanisms and demonstrates how blockchain can mitigate these issues. By leveraging the transparency, immutability, and decentralization of blockchain, DVTChain aims to ensure the integrity and trustworthiness of electoral processes. In [2] "Securing e-voting based on blockchain in P2P network" by Haibo Yi presents a comprehensive exploration of leveraging blockchain technology to enhance the security of electronic voting systems within peer-to-peer networks. Yi's paper critically examines existing e-voting vulnerabilities and proposes innovative solutions by integrating

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2024 ||

| DOI: 10.15680/IJIRCCE.2023.1205083 |

blockchain's immutable ledger and decentralized consensus mechanisms. Through a meticulous literature review, Yi highlights the significance of blockchain in mitigating fraud, tampering, and coercion in e-voting processes. The paper delves into technical aspects, elucidating how blockchain ensures transparency, verifiability, and integrity in voting transactions. Yi's research underscores the potential of blockchain to revolutionize e-voting paradigms, fostering trust and confidence among stakeholders. In [3] "A Blockchain-Based Self-Tallying Voting Protocol with Maximum Voter Privacy," authored by Jun Huang, Debiao He, Yitao Chen, Muhammad Khurram Khan, and Min Luo, presents a comprehensive exploration into leveraging blockchain technology to enhance the integrity and privacy of voting systems. Through meticulous analysis and innovative design, the authors propose a novel self-tallying protocol that ensures maximum voter privacy while maintaining transparency and trustworthiness in the voting process. By integrating blockchain's immutable ledger and cryptographic techniques, the protocol addresses critical concerns such as tamper resistance and anonymity, thereby offering a robust solution to modernize electoral systems. This literature survey delves into the intricacies of the proposed protocol, highlighting its key features and contributions to advancing the field of secure electronic voting. In [4] The paper titled "Transparent Voting System Using Blockchain" authored by V. Anitha, Orlando Juan Marquez Caro, R. Sudharsan, S. Yoganandan, and M. Vimal presents a comprehensive exploration of leveraging blockchain technology for transparent voting systems. Through a meticulous literature survey, the authors delve into existing research on blockchain's applicability in ensuring the integrity and security of voting processes. They highlight the advantages of blockchain, such as immutability and decentralization, in mitigating common issues like fraud and manipulation in traditional voting systems. In [5] "An Efficient E2E Crowd Verifiable E-Voting System" by Xinyu Zhang et al. presents a comprehensive exploration into the development of an End-to-End (E2E) crowd-verifiable electronic voting system. The paper introduces innovative strategies to enhance the efficiency and reliability of electronic voting mechanisms, addressing concerns such as security, verifiability, and scalability. Through a meticulous literature survey, the authors analyze existing approaches and identify gaps in current e-voting systems. By integrating crowd verification mechanisms, the proposed system aims to ensure the integrity and transparency of the voting process, ultimately bolstering trust in electronic voting systems. This research contributes significantly to the advancement of secure and reliable e-voting systems, offering insights into the design and implementation of future voting technologies. function will not use that node.

## III.PROPOSED ALGORITHM

### A. HAAR ALGORITHM

**DESCRIPTION**

A Haar Cascaded Classifier is a machine learning object detection technique used in computer vision. It's designed to efficiently and accurately identify specific objects or patterns within images or video streams. It works by breaking down the detection process into stages, with each stage consisting of a "cascade" of simple classifiers. These classifiers use Haar-like features to distinguish between object and non-object regions, allowing for fast rejection of non-object regions, reducing computational load.

**WORK FLOW**

**1. Integral Image Calculation:** Create an integral image to efficiently compute sum of pixel intensities within rectangular regions.
**2. Haar-like Features**: Define simple rectangular features that capture local intensity variations in different regions of the image.
**3. Feature Selection:** Select a subset of Haar-like features that are most informative for distinguishing between faces and non-faces.
**4. Adaboost Training:** Train a series of weak classifiers using the selected Haar-like features, where each weak classifier focuses on a different region of the image.
**5. Classifier Combination:** Combine the weak classifiers into a strong classifier using the Adaboost algorithm, assigning higher weights to more accurate classifiers.
**6. Cascade Classifier:** Organize the strong classifiers into a cascade structure, where each stage progressively filters out non-face regions to reduce computation.
**7. Integral Image Application:** Utilize the integral image to efficiently evaluate the Haar-like features at different scales and positions in the image.
**8. Feature Evaluation:** Compute the responses of the Haar-like features using the integral image to determine whether each region resembles a face or not.
**9. Cascade Evaluation:** Apply the cascade classifier to rapidly reject non-face regions, focusing computation on promising regions with higher likelihood of containing faces.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2024 ||

| DOI: 10.15680/IJIRCCE.2023.1205083 |

**10. Post-processing:** Refine the detected face regions using techniques such as non-maximum suppression to eliminate duplicate detections and improve localization accuracy.

**ADVANTAGES**

**1. Simplicity:** Haar features are straightforward and computationally efficient, making them easy to implement and process, even on resource-constrained devices.
**2. Robustness to Noise:** Haar features are relatively robust to noise and variations in lighting conditions, allowing for reliable face detection in real-world scenarios.
**3. Fast Processing:** The integral image technique accelerates feature computation, enabling rapid detection of faces in images or video streams.
**4. Adaptability:** Haar-based detectors can be trained to detect various object classes beyond faces, offering versatility in applications such as object detection or gesture recognition.

**DISADVANTAGES**

**1. Limited Discriminative Power:** Haar-like features may struggle to capture complex facial characteristics accurately, leading to lower detection accuracy compared to more advanced algorithms.
**2. Sensitivity to Scale and Rotation:** Haar-based detectors may struggle with detecting faces at different scales or orientations, requiring additional preprocessing or post-processing steps to handle such variations.
**3. High Memory Requirements:** Storing integral images and feature templates for large datasets can consume significant memory resources, limiting the scalability of Haar-based systems.
**4. Dependency on Training Data:** Haar classifiers heavily depend on the quality and quantity of training data, requiring sufficient and diverse annotated datasets for effective training and generalization.

**B. RESNET ALGORITHM**

**DESCRIPTION**

ResNet (Residual Neural Network) is a deep learning architecture that introduced residual connections, addressing the vanishing gradient problem. It consists of several residual blocks, each containing multiple layers. These blocks enable the network to learn residual mappings, making it easier to optimize deeper networks. By skipping connections, ResNet allows gradients to flow directly through the network, facilitating the training of extremely deep networks. The skip connections add identity mappings, helping to preserve useful information throughout the network. With its skip connections, ResNet achieved state-of-the-art performance on various image recognition tasks, enabling the training of deeper networks with improved accuracy and efficiency.

**WORKFLOW**

**1.** Preprocess face images to ensure uniform size and quality.
**2.** Pass the preprocessed images through a ResNet-based encoder.
**3.** Extract high-level features from the encoded representations.
**4.** Compare feature vectors using distance metrics like cosine similarity.
**5.** Establish a threshold to determine matching criteria.
**6.** Calculate distances between feature vectors of query and reference faces.
**7.** Apply the threshold to identify potential matches.
**8.** Evaluate matches based on similarity scores.
**9.** Implement post-processing steps like non-maximum suppression.
**10.** Output final matched pairs or identities.

**ADVANTAGES**

**1.Effective Deep Learning:** ResNet enables the training of very deep neural networks, surpassing previous limitations of gradient vanishing or exploding during training.
**2.Skip Connections:** Skip connections facilitate the flow of gradients, allowing for easier optimization of deep networks and preventing the degradation problem.
**3.Improved Performance:** ResNet architectures often achieve state-of-the-art performance on various image recognition tasks, including object detection and segmentation.
**4.Efficient Training:** ResNet's skip connections reduce the training time and computational resources required to converge, making it feasible to train deeper networks efficiently.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2024 ||

| DOI: 10.15680/IJIRCCE.2023.1205083 |

**DISADVANTAGES**

**1.Increased Complexity:** Implementing and understanding ResNet architectures can be more complex compared to shallower networks due to the presence of skip connections and deeper layer structures.

**2.Overfitting Risk:** Deeper networks like ResNet are prone to overfitting, especially when trained on smaller datasets or with insufficient regularization techniques.

**3.Memory Consumption:** Deeper networks require more memory for both training and inference, which can be a limitation on resource-constrained devices or platforms.

**4.Hyperparameter Tuning:** Tuning the hyperparameters of ResNet architectures, such as the number of layers or filter sizes, can be challenging and time-consuming to achieve optimal performance.

### C. ADVANCED ENCRYPTION STANDARD

**DESCRIPTION**

The Advanced Encryption Standard (AES) is a widely used symmetric encryption algorithm. It operates on fixed-size blocks of data, typically 128 bits. AES employs a substitution-permutation network comprising several rounds, with the number of rounds dependent on the key size. During each round, a combination of substitution and permutation operations is applied to the data. The algorithm employs a key expansion process to generate round keys from the initial secret key. AES provides robust security against various cryptographic attacks, including brute-force and differential attacks. It has three key sizes: 128, 192, and 256 bits, offering different levels of security. AES encryption and decryption are efficiently implemented in hardware and software, making it suitable for a wide range of applications, including secure communication and data storage.

**WORK FLOW**

1. Generate round keys from the initial encryption key using a key schedule algorithm.
2. Add the initial round key to the plaintext.
3. Perform multiple rounds (typically 10, 12, or 14) of substitution, permutation, and mixing operations.
4. Substitute each byte of the state with a corresponding byte from the S-box.
5. Shift the rows of the state cyclically to the left by different offsets.
6. Combine and mix the columns of the state using matrix multiplication.
7. Add the round key to the state, which is derived from the round key schedule.
8. Omit the MixColumns operation in the final round.
9. Repeat the rounds for each block of plaintext data.
10. The final state represents the ciphertext, which is the encrypted form of the plaintext input.

**ADVANTAGES**

**1. Security:** AES offers a high level of security, as it is widely recognized and extensively analyzed by cryptographic experts.

**2.Efficiency:** It is computationally efficient, allowing for fast encryption and decryption, especially when implemented in hardware or optimized software.

**3.Scalability:** AES supports key lengths of 128, 192, and 256 bits, providing flexibility to meet various security requirements.

**4.Standardization:** AES is a standardized encryption algorithm adopted by governments, organizations, and industries worldwide, ensuring interoperability and compatibility.

**DISADVANTAGES**

**1. Key Management:** Proper key management is crucial for AES, as compromised keys can lead to security breaches. Secure key distribution and storage can be challenging, especially in large-scale systems.

**2. Resource Intensive:** AES encryption and decryption can be resource-intensive, particularly for devices with limited computational capabilities such as embedded systems or IoT devices.

**3. Potential Vulnerabilities:** Although AES is highly secure, there is always a risk of undiscovered vulnerabilities or attacks, necessitating continuous monitoring and updates to mitigate emerging threats.

**4. Side-channel Attacks**: AES implementations may be vulnerable to side-channel attacks, where attackers exploit unintended information leakage such as power consumption or timing variations to deduce cryptographic secrets. Mitigating such attacks requires careful design and implementation of cryptographic algorithms and protocols.

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2024 ||

| DOI: 10.15680/IJIRCCE.2023.1205083 |

## IV.RESULTS


Fig 1: Home page


Fig 2: Admin Login

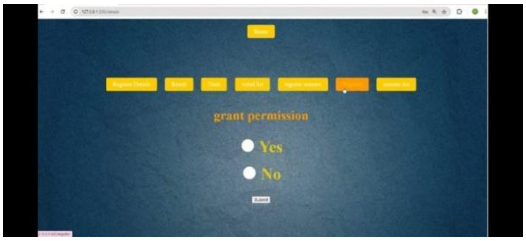


Fig 3: Admin Page

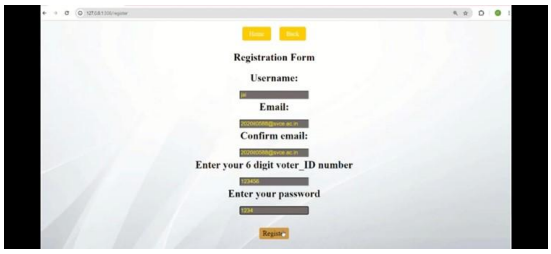


Fig 4: Registration Form Page

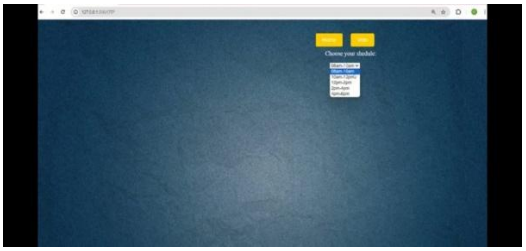

Fig 5: Slot Selection Page

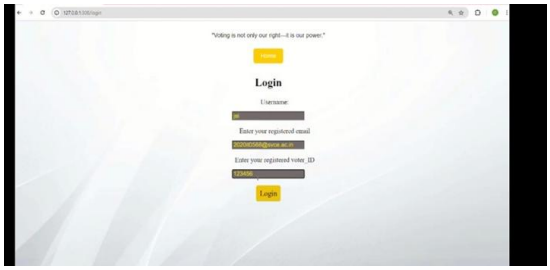


Fig 6: User Login Page


Fig 7: Voting Page

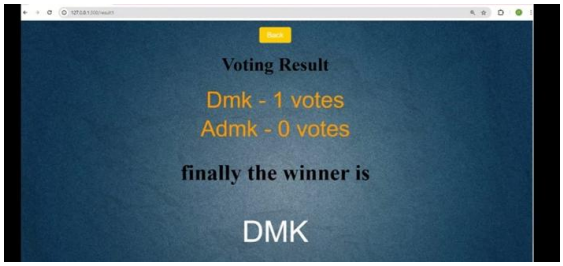


Fig 8: Result Page

The **Figure 1** represents the home page of the system where administrators and users can access the login functionality. The **Figure 2** represents the admin login page of the voting system. This allows admins to log in to the system and manage voter databases, oversee the election process, and ensure the security of the voting system.The **Figure 3** represents admin page of the voting system. This allows the adminto register voter details and nominee details, and to oversee the lists of both votersand nominees, as well as the election results. The admin also has the option to train the model. Additionally, the admin has access to grant permission for the functioning of the page on election day, allowing users to log in and cast their votes on that particular day. The **Figure 4** represents Registration form page. It collects

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2024 ||

| DOI: 10.15680/IJIRCCE.2023.1205083 |

essential details such as voter's name, voter id, email id and password. It serves to verify the eligibility of voters and ensures accurate participation in the electoral process. The **Figure 5** represents the slot selection page. Users need to select the scheduled slots according to their availability to cast their vote on election day. The **Figure 6** represents the user login page. The user needs to enter their name,email address, and voter ID to log in and cast their vote. The **Figure 7** represents the voting page. The user can select the candidatethey wish to vote for. Additionally, the user must enter their password to casttheir vote. The **Figure 8** represents the result page of the e-voting system. It displays theoutcome of the election, listing details such as nominee names, votes received, and final standings. It offers transparency to voters, ensuring the integrity of the electoral process and enabling stakeholders to verify the results. Additionally, it serves as an official record of the election outcome, facilitating post-election analysis and audits by relevant authorities.

## V.CONCLUSION AND FUTURE WORK

The integration of facial recognition technology, particularly using HAAR Cascade Classifiers, in e-voting systems offers a transformative opportunity to enhance electoral processes. By leveraging facial features for robust voter authentication, it minimizes fraud risks and streamlines the voting experience. Deep learning models combined with facial recognition improve accuracy, bolstering system security. However, successful implementation requires privacy safeguards, bias mitigation, and transparency for public trust. Incorporating OTP verification enhances security and accessibility. This approach sets a new standard for efficient and secure e-voting, paving the way for a more inclusive democratic electoral landscape. Stakeholders must prioritize these technologies while upholding privacy, fairness, and accountability principles for widespread acceptance in modern democracies. In the future, incorporation of blockchain technology is anticipated to significantly bolster security and transparency, creating an immutable ledger for vote tracking and reducing the potential for tampering. To increase voter participation and convenience, the development of mobile voting applications is planned, which will allow secure voting from anywhere, leveraging the ubiquity of smartphones. Further advancements in identity verification will be explored through the integration of additional biometric authentication methods, such iris scanning, complementing facial recognition to ensure that voter identity is confirmed with even greater accuracy. Additionally, plans involve creating a user-friendly interface for real-time election result tracking, establishing a robust auditing system for post-election analysis, and ensuring the integrity of the voting process. These advancements aim to elevate the e-voting system's security, transparency, and accessibility, aligning with modern democratic standards.

## REFERENCES

1. Haibo Yi, “Securing e-voting based on blockchain in P2P network”, Yi EURASIP Journal on Wireless Communications and Networking (2019) 2019:137, https://doi.org/10.1186/s13638-019-1473-6.
2. J. Ben-Nun, N. Fahri, M. Llewellyn, B. Riva, A. Rosen, A. Ta-Shma, and D. Wikström, ‘‘A new implementation of a dual (paper and cryptographic) voting system,’’ in Proc. 5th Int. Conf. Electron. Voting (EVOTE),2012, pp. 315–329.
3. Jun Huang, Debiao He, Member, IEEE, Yitao Chen, Muhammad Khurram Khan, Senior Member, IEEE, and Min Luo, “A Blockchain-Based Self-Tallying Voting Protocol with Maximum Voter Privacy “, Ieee Transactions on Network Science and Engineering, Vol. 9, No. 5, September-October 2022.
4. K. T. Sri, K. R. Sri, and N. Pedamallu, ‘‘E-voting system using blockchain,’’ J. Xi’an Univ. Archit. Technol., vol. 13, no. 5, pp. 527–533, 2021.
5. S. Al-Maaitah, M. Qatawneh, and A. Quzmar, ‘‘E-voting system based on blockchain technology: A survey,’’ in Proc. Int. Conf. Inf. Technol. (ICIT),Jul. 2021, pp. 200–205.
6. S. Heiberg, K. Krips, J. Willemson, and P. Vinkel, ‘‘Facial recognition for remote electronic voting–missing piece of the puzzle or yet another liability?’’ in Proc. Int. Workshop Emerg. Technol. Authorization Authentication. Switzerland: Springer, 2021, pp. 77–93.
7. S. K. Vivek, R. S. Yashank, Y. Prashanth, N. Yashas, and M. Namratha,‘‘E-voting systems using blockchain: An exploratory literature survey,’’ in Proc. 2nd Int. Conf. Inventive Res. Comput. Appl. (ICIRCA), Jul. 2020,pp. 890–895 Taş and Ö. Ö. Tanriöver, ‘‘A systematic review of challenges and opportunities of blockchain for E-voting,’’ Symmetry, vol. 12, no. 8,p. 1328, Aug. 2020.
8. Syada Tasmia Alvi a,⇑ , Mohammed Nasir Uddin b , Linta Islam b , Sajib Ahamed b, “DVTChain: A blockchain-based decentralized mechanism to ensure the security of digital voting system voting system”, Journal of King Saud University – Computer and Information Sciences 34 (2022) 6855–6871.
9. T. Moura and A. Gomes, ‘‘Blockchain voting and its effects on election transparency and voter confidence,’’ in Proc. 18th Annu. Int. Conf. Digit.Government Res., Jun. 2017, pp. 574–575.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2024 ||

| DOI: 10.15680/IJIRCCE.2023.1205083 |

10. U. Can Cabuk, E. Adiguzel, and E. Karaarslan, ‘‘A survey on feasibility and suitability of blockchain techniques for the E-voting systems,’’ 2020, arXiv:2002.07175.
11. U. Jafar, M. J. A. Aziz, and Z. Shukur, ‘‘Blockchain for electronic voting system-Review and open research challenges,’’ Sensors, vol. 21, no. 17, p. 5874, 2021.
12. V. Anilkumar, J. A. Joji, A. Afzal, and R. Sheik, ‘‘Blockchain simulation and development platforms: Survey, issues and challenges,’’in Proc. Int. Conf. Intell. Comput. Control Syst. (ICCS), May 2019,pp. 935–939.
13. V. Anitha a,* , Orlando Juan Marquez Caro b , R. Sudharsan a , S. Yoganandan a , M. Vimal a, “Transparent voting system using blockchain”, Elsevier.
14. Xinyu Zhang , Student Member, IEEE, Bingsheng Zhang , Member, IEEE, Aggelos Kiayias , Thomas Zacharias , and Kui Ren , Fellow, IEEE, “An Efficient E2E Crowd Verifiable E-Voting System”, Ieee Transactions On Dependable And Secure Computing, Vol. 19, No. 6, November/December 2022.
15. Y. Abuidris, R. Kumar, and W. Wenyong, ‘‘A survey of blockchain based on E-voting systems,’’ in Proc. 2nd Int. Conf. Blockchain Technol. Appl., Dec. 2019, pp. 99–104

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

## IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details