iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** I **Month of publication:** January 2025

DOI: https://doi.org/10.22214/ijraset.2025.66716

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue I Jan 2025- Available at www.ijraset.com

A Real-Time Implementation of Smart Voting System Using Face Recognition and Fingerprint Module

Thejeshri Rajesh[1], Haripriya K[2], Dr. S. Nivetha[3]
[1, 2]*Bachelor of Engineering in Computer Science with Specialization in Artificial Intelligence and Robotics, Sathyabama Institute of Science and Technology, Chennai, India*
[3]*M.E., Ph.D, Assistant Professor, Department of computer Science and Engineering, Sathyabama Institute of Science and Technology, Chennai, India*

Abstract*: Elections are an influential part of any democratic system, and it is indispensable to ensure that the voting process is conducted in fair means. Conventional paper-based elections are labor-intensive, resource-intensive, and error-prone. In this case, technology may greatly increase the voting process's accuracy, security, and efficiency. In this, it ist an online voting system that identifies and authenticates voters using biometric and facial recognition technologies. By removing the need for physical ballot boxes and enabling voters to cast their ballots remotely, the proposed technology lowers the expense and duration of the voting process. The method operates by collecting the voter's facial picture and fingerprints and sending them to the server unit for verification. The server matches the face picture to the information in the database to verify the voter's identification. Voters are permitted to cast their ballots if their identities are confirmed; if not, they are prohibited from doing so and an error notice appears on the screen. The system is intended to be safe and impenetrable. With the use of fingerprint and facial recognition technologies, it is more difficult for someone to vote fraudulently by impersonating someone else. Additionally, the approach guarantees that each voter may only cast one vote and that the voting procedure is carried out in an open and equitable way. All things considered, the suggested online voting method has several benefits over conventional paper-based voting systems, such as more effectiveness, lower costs, better security, and greater transparency.

Keywords: Online Voting System, Face Recognition, Fingerprint Technology, Voter Authentication, Remote Voting, Secure Voting, Fraud Prevention, Transparent Voting Process.

I. INTRODUCTION

Democracy is critical in many developing countries because it allows the people to choose the government via the election process. Polling conducted by election authorities is very important. Election processes have changed significantly since achieving independence. In the beginning, voting was done using ballot sheets. Nevertheless, computerized voting machines, which allow voters to choose their favorite candidate by pressing keys that correspond to symbols, gradually supplanted the suggested technique [1]. Elections include both public and private voting, which is determined by the individual job being sought. The federal, state, and local governments all play important roles in society. Electronic voting systems provide a reliable and efficient way for members of an association or the people of a country to select the candidate of their choice. These systems fall into three categories: hybrid, supervised, and remote voting. Electoral organizations frequently undertake supervised voting, also known as offline voting. Hybrid voting systems are overseen by election officials, and voting equipment are accessible online.

Conversely, programs that employ internet-connected devices and are managed without the assistance of supervisory staff are referred to as remote voting. Results are disseminated quickly and accurately thanks to the digital voting process [2]. Electronic voting is the process of recording, storing, and processing election data primarily in digital format using electronic apparatus or devices, frequently computer-assisted. Electronic voting ensures increased transparency, reliability, and security.

It ensures increased efficiency, greater scalability, faster speeds, and lower costs. Voters cast their ballots in tightly sealed boxes that are then re-distributed around the nation's electoral circuits in a paper-based election. After the election time ends, the ballot control unit boxes are opened, and the ballots are counted by hand in front of certified voters who have been given permission by the electoral board.

The voting process requires a lot of time and resources [3]. Because the whole voting process is done online, people may cast their ballots remotely from any location while maintaining a high level of security. Since voters will be able to cast their ballots via electronic devices like laptops and PCs, the new method's implementation will ensure user privacy. Due to the system being transparent, it fosters a higher level of trust. The number of people using the voting system will rise significantly as a result [4]. This study focuses on the use of deep learning and machine learning techniques for face identification in order to enable login to a voting system. It also presents an online voting system that uses fingerprint authentication and face recognition for voting. The study provides an online voting mechanism based on facial recognition. The information about the face is sent to the server unit for further verification. The server then retrieves the data from the database and compares it with the existing data. If the information matches what is presently in the database, the person is eligible to vote. In this scenario, a notification appears on the screen and the person is subsequently blocked from voting. People are chosen by the electorate to act as voting representatives. Voters must now provide their voter ID card at the polling station in order to cast their ballot. This process is time-consuming since the voter ID card must be formally verified [5]. In addition to accelerating the voting process, our new system proposal aims to resolve these problems. The three security levels of an ATMEGA 32-based voting system are designed and constructed using the enhanced smart voting system security described in this work. Using a smart voting system to cast a paper ballot is time-consuming. Consequently, it saves time and effort, making it dependable and quick. Even in the absence of paper ballots, the technique maintains vote secrecy. Smart voting system voting devices are less expensive than other voting equipment. With a single click, a smart voting system provides results that are hundred percent impenetrable. By altering the hardware connections, the smart voting system can be compromised [6]. Three safeguards are suggested by the study. The Arduino-fingerprint reader system utilizes the Biometrics counts votes, authenticates voters, and prevents fraud. By using fingerprint scanning, it verifies voter registration and forbids the use of duplicate ballots. To use a multiple-use decentralized internet voting system, a voter needs a smartphone with a barcode scanner and their Aadhar card number. Because the program is web-based, users can cast their votes from any location [7]. The system generates voting ballots automatically. The local administrator decrypts vote data encrypted by the user, making voting safer and more reliable.

II. LITERATURE REVIEW

Rashidov [8] presents an electronic voting system designed for a higher education institution, focusing on its development and result processing. The paper outlines the main stages in the system’s design, including the base model, information flows, database schema, and functional block diagram. The system automates ballot creation and processing for various election types within the institution, such as elections for governing bodies and student representatives. Key functionalities include accountability in voting, anonymity, protection from hacker attacks, and reliability. The system facilitates voter identity verification and simplifies the voting procedure and result processing, boasting an intuitive user interface.

Raghuram, and Jayaraman (2022) [9] This paper explores the integration of online and offline voting systems with an E-Voting website, addressing challenges in the Indian electoral process. Despite the Election Commission of India's efforts to implement technologies like Voter-Verified Paper Audit Trail (VVPAT) with Electronic Voting Machines (EVM), issues like voter verification and malpractices persist. To address these, the authors propose embedding a face recognition device with the EVM and integrating an online voting platform to accommodate voters who have migrated. The system aims to increase polling rates by allowing remote voting and provides real-time updates on voter status through the online platform. Test results indicate satisfactory performance of the integrated system.

Ganesh Prabhu et al. [10] Ganesh Prabhu and colleagues highlight the inefficiencies of the traditional offline voting system in India and propose a smart online voting system as a solution. The new system enables remote voting via computers or mobile phones, utilizing face recognition and OTP for authentication, thus eliminating the need for physical presence at polling stations. The system also includes an offline voting option using RFID tags instead of traditional voter IDs. This dual approach not only simplifies the voting process but also enhances transparency and reduces the potential for vote tampering by allowing citizens to view results anytime.

Usmani et al.[11] (2017) This paper discusses various voting systems and aims to develop a multipurpose, platform-independent online voting system that operates across different operating systems. It evaluates the advantages and disadvantages of Paper Ballot, E-Voting, Internet Voting, SMS, and Miss Call Voting Systems.

Lakshmi et al. (2023)[12] This study enhances e-voting security through a two-step verification process using machine learning. It focuses on improving the security and integrity of the voting system by incorporating additional verification steps to prevent fraud and ensure accurate voter authentication. Kandan et al. (2021) [13]

This paper presents a smart voting system that integrates face detection and recognition algorithms to enhance voting security and efficiency. The system aims to reduce fraudulent voting by verifying voter identities using facial recognition, allowing remote voting.

Arputhamoni and Saravanan (2021) [14] This research focuses on an online smart voting system using biometric authentication, including facial and fingerprint detection. The system aims to improve security and reduce fake voting by comparing biometric data collected on the voting day with stored data in the database.

Mondal and Chatterjee (2019) [15] This paper introduces an Electronic Voting Machine (EVM) that leverages deep convolutional neural networks (CNN) for face recognition to ensure voter authentication. The proposed system captures and verifies the voter's facial image against pre-captured database images. Post-voting, the voter's facial data is deleted to prevent multiple voting attempts. The system demonstrates high accuracy with a recognition rate of 99.1% and addresses issues such as booth-capturing and ballot-stuffing, aiming to enhance the efficiency and security of the voting process.

Vashisht, Mohan, and Prakash (2022)[16] This paper presents a facial identification-based voting system that allows voters to cast their votes from any location within India. The system integrates high-level biometric security, requiring voters to position themselves in front of a camera for facial recognition. The voter's information is processed and verified through a web application, which maintains individual records and handles age-related eligibility checks. The system facilitates real-time monitoring and results updates by the election commission, aiming to modernize and streamline the voting process.

Gupta, Jain, and Themalil (2021) [17] This paper details an electronic voting system combining face recognition technology with the ATmega328P microcontroller. The system incorporates multiple verification layers to ensure process reliability. Voters are first authenticated using government-issued IDs, followed by facial recognition. After successful verification, voters can cast their votes electronically. The voting data is uploaded to a ThingSpeak server for real-time monitoring by the central election office, enhancing the reliability and security of the voting process while reducing manual paperwork and labor.

III. PROPOSED SYSTEM

Leveraging the features of Python, the proposed system was developed. As input, the system takes a collection of voter photos and trains the model with the help of OpenCV and CNN to aggregate results. By feeding the facial recognition model datasets, including images of voters, this system is able to accomplish its primary goal of ensuring an ethical election process. Then, to make sure that each voter only casts a ballot, the proposed work uses the trained model to identify their faces. The execution process consists of careful planning, a detailed analysis of the existing system and its implementation constraints, the creation of transition achievement methods, and an evaluation of the transition method. Fig. 2 depicts the proposed model's process flow.

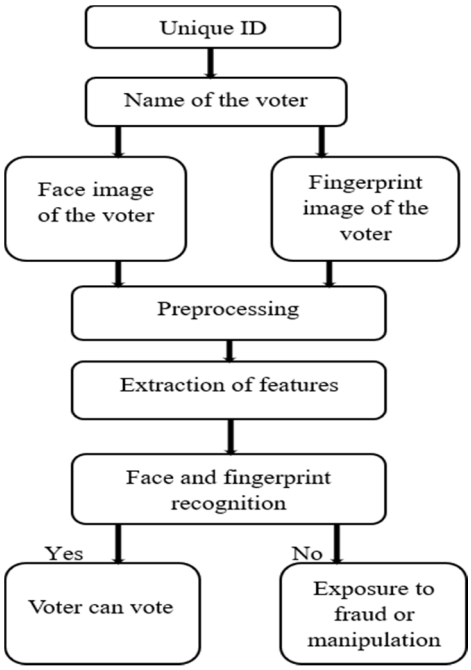


Fig. 2 Process flow of the proposed method.

To begin, the user is required to complete the registration procedure by entering necessary details such as their Aadhaar number, cell phone number, city, age, password, and any other required information. The information discussed earlier is included in the dataset collected from voters. For the registration process, individuals are provided with a username and password linked to their Aadhaar identification number. Citizens will be given a new user identification and password, to submit their ballots as part of the election process. Individuals eligible to vote have the option of using either fingerprint identification, iris recognition, or a one-time password (OTP). The information related to the individual's face and fingerprints is transmitted to the server unit for additional authentication. After this, the server will determine whether the data already exists in the database and then compares the newly added data to the existing data. Permission to cast a vote is granted only if the data matches the information already available. If this is not the case, an error message stating that the user is not allowed to cast their vote will show on the screen.

A. Data Collection

The citizens' images are acquired by capturing 40 snaps of each individual, which serve as the input dataset. This dataset is precisely used to train the model. The dataset is created by linking individual names with their related photos, utilizing the OpenCV module in Python programming.

B. Data Preprocessing

Object detection in images is crucial. This method uses picture processing techniques such as noise reduction and filtering to find lines, areas, and textures. An AI system must handle variations in lighting or viewpoint, a task that is effortless for the human visual system but requires advanced processing power for a computer. The process involves visual transformation of data. Most visual print viewers see a picture as a two-dimensional collection of pixel intensities. A computer may decipher an image either visually or digitally.

C. Detection of features using Haar Cascade

The Haar Cascade classifiers are used in the proposed system for face detection. The Haar Cascade method uses a variety of characteristics to identify people in photos. For object recognition, it is trained using a sizable dataset of both positive and negative pictures. Applying positive labels to windows that contain the item and negative labels to those that do not contain the item, is how Haar Cascade works. This is how the Haar-like feature is calculated:

A sizable picture collection is used to train the Haar Cascade algorithm in order to identify the facial characteristics. Haar features, which are square-shaped functions used to differentiate between faces (1) and non-faces (0), are detected after the picture has been converted to grayscale. Figure 3 illustrates the four primary steps of the process: identifying Haar features, using a cascade of classifiers, using integral pictures, and implementing the AdaBoost method.

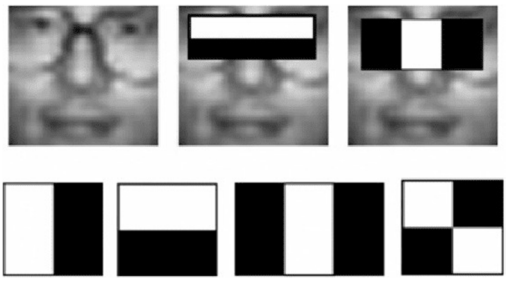


Fig. 3 OpenCV Haar Cascade image.

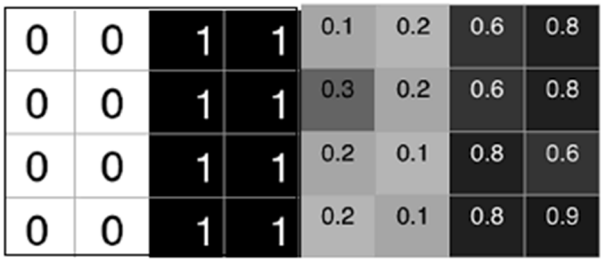


Fig.4: Pixel intensities of the Haar-features (a) ideal case (b) real case.

$$\Delta = \frac{1}{n}\sum_{dark}^{n} I(x) \frac{1}{n}\sum_{white}^{n} I(x)$$

Eq. (1) Ideal case: Δ = (1/8)*(8) — (1/8)*0 = 1
Real case: Δ = (1/8)*(5.9) — (1/8)*(1.3)=0.575
Haar features are a very useful face identification technique since they are very good at identifying rectangular characteristics. Despite having numerous features, some may also be irrelevant. Feature that is part of the face. Adaboost selects both the best features and the weak ones and trains the classifiers that use them. It creates "strong" classifiers and "weak" classifiers within the algorithm. Here a strong classifier means one which has less error rate, one which will definitely be a part of the face and a 'weak' classifier has less than 50% error rate so we know that it mostly will be a feature that belongs in the face region. Therefore, we use Adaboost to combine these weak classifiers into one strong classifier that will lead to the detection of a face.

D. Fingerprint Identification

Fingerprint identification is a distinct form of biometric verification because the ridge pattern found on each finger is unique and does not change over time. The proposed system uses UART (Universal Asynchronous Receiver/Transmitter) fingerprint sensor. The hardware setup of the UART fingerprint sensor is shown in Fig. 4.

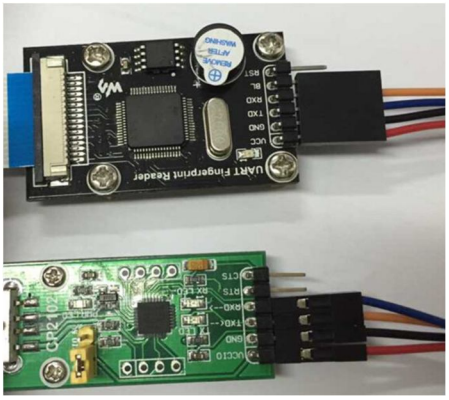


Fig. 5 Hardware setup of UART Fingerprint sensor

The operation of a UART fingerprint sensor involves capturing a fingerprint image, analyzing it to extract distinctive characteristics, and storing these characteristics as a template. During authentication, pattern matching techniques are used to compare a fresh fingerprint picture to templates that have been saved. The similarity score determines whether the fingerprint matches any stored templates, and the result is conveyed to the host system through the UART device.

E. Security

To prevent unauthorized access and misuse of data, ballots recorded by the software are securely stored. The Advanced Encryption Standard (AES) encryption technique is employed for this purpose. AES is a secure symmetric encryption algorithm based on a "substitution-permutation" network. The decryption process mirrors the encryption procedure, but in reverse. AES offers a significant speed advantage over the older Data Encryption Standard (DES) due to its larger key size. AES supports encryption and decryption with 128, 192, or 256-bit keys. The encryption process involves multiple rounds depending on the key length: 10 rounds for 128-bit, 12 rounds for 192-bit, and 14 rounds for 256-bit keys. Votes cast through the system are encrypted client-side using AES with a designated 'secret key' and securely recorded in the Google Firebase real-time database as a JSON node. The same 'secret key' is used to decrypt and unlock the votes during the counting process.

IV. RESULTS

Smart voting system employs HTML and CSS to create the front end of an online voting platform, which is then implemented in Visual Studio for smooth integration. The technology beats existing approaches by providing more security and efficiency. The system dramatically decreases the potential of fraudulent votes and streamlines the voting and counting operations. A secure network decreases the number of illegitimate votes, and the switch to online voting significantly reduces the demand for labor, making it a viable alternative.

Fig 6. homepage

The "Administrator" button is linked to the admin section of the website, where authorized personnel can manage the voting system, including adding or removing candidates, setting up voting parameters, and viewing the voting results. The "User Registration" button is linked to the registration section of the website, where eligible voters can create an account and register to vote. The "Update Details" button is linked to a section of the website where registered voters can update their personal information or change their voting preferences.

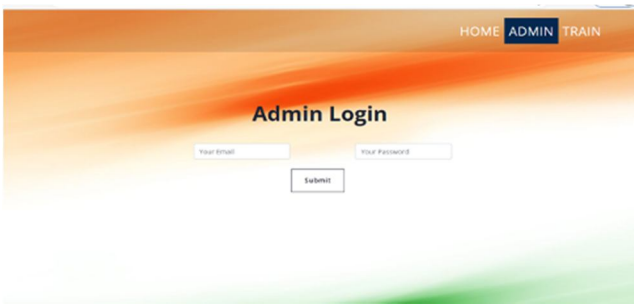


Fig 7. Admin page

This is an input form that is designed to allow administrators to log in to a website or application. Typically, this would require the user to provide a username and password to gain access to the administrator dashboard or other secure areas of the website.

Fig 8. Voting page

The form includes several fields, including one for the "member name" and another for the "party name". These fields likely allow the user to input the name of the person they wish to nominate, as well as the political party that person belongs to. In addition, the form also includes "radio buttons" which allow the user to select a "party symbol" from a set of images. These symbols could be used to visually represent the political party of the nominee.

Fig 9. Updation

This section contains a form that allows voters to update their personal details, including their first name, middle name (optional), last name, Aadhar number, voter ID, email, and phone number.

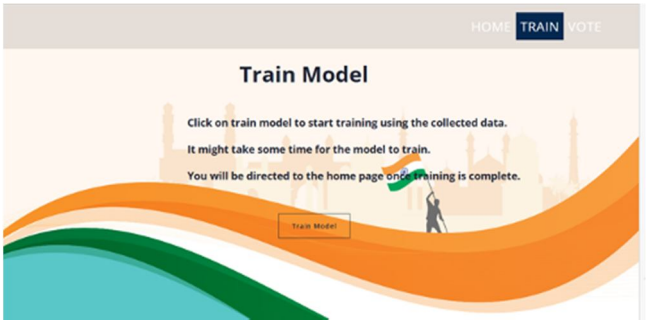


Fig 10. Training of Model

The form is submitted via a POST request to the URL defined by the train route in the backend. Once the user clicks on the "Train Model" button, the form is submitted and the model starts to train. A message is displayed to inform the user that the training process may take some time and they will be redirected to the home page once the process is complete

V. CONCLUSION

Voting can be done more effectively and securely through the help of an online voting system with facial recognition technology. Paper ballots and human counting, which may be expensive and time-consuming, are no longer necessary with this approach. Rather, the method uses fingerprints and face recognition to confirm voters' identities and stop fraud from happening. It is crucial to remember that putting such a system into place would need a large infrastructure and security expenditure. Additionally, all voters, including those with impairments, must be able to use and access the system. This simplified, online voting system can be immensely useful and can help increase the number of people that vote.

REFERENCES

[1] J. J. Arputhamoni and A. G. Saravanan, "Online Smart Voting System Using Biometrics Based Facial and Fingerprint Detection on Image Processing and CNN," 2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV), Tirunelveli, India, 2021, pp. 1-7, doi: 10.1109/ICICV50876.2021.9388405.

[2] S. Ganesh Prabhu, A. Nizarahammed, S. Prabu, S. Raghul, R. R. Thirrunavukkarasu and P. Jayarajan, "Smart Online Voting System," 2021 7th International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, India, 2021, pp. 632-634, doi: 10.1109/ICACCS51430.2021.9441818.

[3] S. Gupta, D. Jain and M. T. Themalil, "Electronic Voting Mechanism using Microcontroller ATmega328P with Face Recognition," 2021 5th International Conference on Computing Methodologies and Communication (ICCMC), Erode, India, 2021, pp. 1471-1476, doi: 10.1109/ICCMC51019.2021.9418372.

[4] N. Keerthi, A. Raghuram and R. Jayaraman, "Interfacing of Online and Offline Voting System with an E-Voting Website," 2022 6th International Conference on Devices, Circuits and Systems (ICDCS), Coimbatore, India, 2022, pp. 223-228, doi: 10.1109/ICDCS54290.2022.9780681.

[5] M. Kandan, K. D. Devi, K. D. N. Sri, N. Ramya and N. K. Vamsi, "Smart Voting System using Face Detection and Recognition Algorithms," 2021 IEEE International Conference on Intelligent Systems, Smart and Green Technologies (ICISSGT), Visakhapatnam, India, 2021, pp. 202-206, doi: 10.1109/ICISSGT52025.2021.00050.

[6] Y. V. Lakshmi, V. Amrutha, S. K. Sumaya, A. Harshitha and N. S. Keerthi, "E-Voting Through Two Step Verification using Machine Learning," 2023 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS), Erode, India, 2023, pp. 35-39, doi: 10.1109/ICSCDS56580.2023.10105007.

[7] V. Laxmi Vashisht, H. Mohan and S. Prakash, "Smart Voting System Through Face Recognition," 2022 4th International Conference on Advances in Computing, Communication Control and Networking (ICAC3N), Greater Noida, India, 2022, pp. 909-913, doi: 10.1109/ICAC3N56670.2022.10073982.

[8] J. Ma and L. Chen, "Initial Investigation into Using Two-Level Regional Voting Approach for Face Verification," 2012 IEEE/ACIS 11th International Conference on Computer and Information Science, Shanghai, China, 2012, pp. 23-27, doi: 10.1109/ICIS.2012.62.

[9] I. Mondal and S. Chatterjee, "Secure and Hassle-Free EVM Through Deep Learning Based Face Recognition," 2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon), Faridabad, India, 2019, pp. 109-113, doi: 10.1109/COMITCon.2019.8862263.

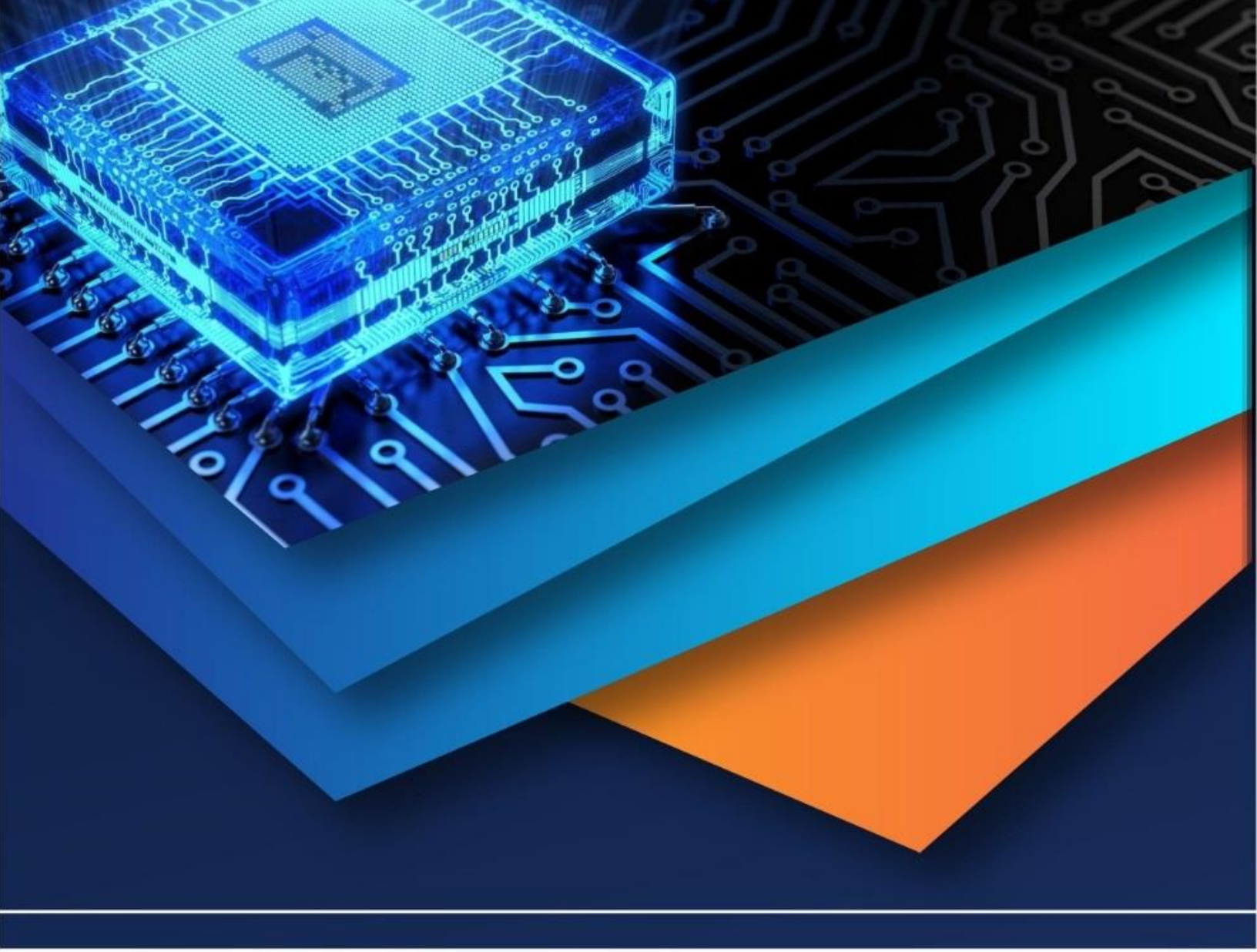
[10] A. Rashidov, "E-Voting System in a Higher Education Institution," 2023 IEEE International Conference on Computing (ICOCO), Langkawi, Malaysia, 2023, pp. 188-193, doi: 10.1109/ICOCO59262.2023.10397903.

[11] Z. A. Usmani, K. Patanwala, M. Panigrahi and A. Nair, "Multi-purpose platform independent online voting system," 2017 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), Coimbatore, India, 2017, pp. 1-5, doi: 10.1109/ICIIECS.2017.8276077.

[12] Nwachukwu-Nwokeafor K.C, Igbajar Abraham, Design of a Secured Online Voting System for electoral Process, International Journal of Innovative Science, Engineering & Technology, Vol. 2, Issue 12, December 2015, pp. 456-471.

[13] Mr. Mayur Patil, Mr. Vijay Pimplodkar, Ms. Anuja R. Zade, Mr.Vinit Vibhute, Mr..Ratnakar Ghadge, A Survey on Voting System Techniques, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 1, January 2013, pp. 114- 117.

[14] Prof. Anisaara Nadaph, Ashmita Katiyar, Tushar Naidu, Rakhi Bondre, Durgesh Kumari Goswami, An Analysis of Secure Online Voting System, International Journal of Innovative Research in Computer Science & Technology, Volume-2, Issue-5, September-2014, pp. 48-51.
[15] Syed Afaq Ali Shah, Uzair Nadeem, Mohammed Bennamoun, Ferdous Sohel and Roberto Togneri, "Efficient image set classification using linear regression based image reconstruction", 2017.
[16] Qasim Abbas, Sarah Javaid and Tanzeel HussnainAbass, "Location-free Voting System with the help of IOT Technology", 12th International Conference on Mathematics Actuarial Science Computer Science and Statistics, pp. 14-20, 2018.
[17] Hossain Faruk, M.J., Islam, M., Alam, F., Shahriar, H., Rahman, A.: Bie vote: A biometric identification enabled blockchain-based secure and transparent voting framework. In: 2022 Fourth International Conference on Blockchain Computing and Applications (BCCA), pp. 253–258 (2022). https://doi.org/10.1109/BCCA55292.2022.9922588
[18] Lalitha, V., Samundeswari, S., Roobinee, R., Swetha, L.S.: Decentralized online voting system using blockchain. In: 2022 International Conference on Applied Artificial Intelligence and Computing (ICAAIC), pp. 1387–1391 (2022). https://doi.org/10.1109/ICAAIC53929.2022.9792791
[19] Kohno, T., Stubblefield, A., Rubin, A.D., Wallach, D.S.: Analysis of an electronic voting system. In: IEEE Symposium on Security and Privacy, 2004. Proceedings. 2004, pp. 27–40 (2004). https://doi.org/10.1109/SECPRI.2004.1301313
[20] Rezwan, R., Ahmed, H., Biplob, M.R.N., Shuvo, S.M., Rahman, M.A.: Biometrically secured electronic voting machine. In: 2017 IEEE Region 10 Humanitarian Technology Conference (R10-HTC), pp. 510–512 (2017). https://doi.org/10.1109/R10-HTC.2017.8289010



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY