International Journal of Scientific Research and Engineering Development-– Volume 7 Issue 5, Sep-Oct 2024

Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

Biometric-Based Voting System Leveraging Aadhaar for Voter Authentication

Narmatha B[1], Thulasimani K[2]

[1]P. G. Student, Department of Computer Science and Engineering, Government College of Engineering, Tirunelveli
[2]Professor, Department of Computer Science and Engineering, Government College of Engineering, Tirunelveli

----------**********----------

Abstract:

As everyone is aware, elections are an essential part of democracy, allowing people to voice their opinions through the selection of a candidate. "Vote" means to choose from a list. Citizens choose a leader in all candidates from a list by casting their votes, this process is voting. Voting is a crucial means by which citizens in democracies like India can express their opinions. Voters usually cast their ballots at polling locations. As the technology increases, nowadays electronic voting machine is used for casting vote. This paper is about electronic voting system using biometrics based on Aadhaar represents a significant advancement in ensuring the security, accuracy, and efficiency of the electoral process in India. The objective of this work is to improve the existing voting system that will utilize SHA (Secure Hash Algorithm) for secure biometric data processing and pattern matching algorithms for fingerprint analysis, the system aims to enhance voter authentication and ensure a secure voting process. Aadhaar is used to achieve the objective. Aadhaar, a unique identification system issued by the Indian government, incorporates biometric data such as fingerprints and iris scans, making it a robust tool for voter authentication.

Keywords **— Aadhaar, Biometrics, Finger print Authentication, Secure Hash Algorithm, Unique Identification Authority of India (UIDAI).**

----------**********----------

I. INTRODUCTION

The electronic voting system in India, utilizing Electronic Voting Machines (EVMs), revolutionized the electoral process by replacing traditional paper ballots. First introduced experimentally in 1982 and adopted nationwide after successful trials, EVMs streamline voting and counting, minimize human errors, and reduce electoral fraud risks. The addition of Voter Verifiable Paper Audit Trails (VVPAT) further boosts transparency and voter confidence. Despite challenges like technical issues and security concerns, the system has become integral to Indian elections, ensuring free, fair, and efficient democratic processes.

Due to the possibility of voting fraud, the existing system is known for its lack of openness. The primary difficulties with the existing election voting procedure are voter authentication, voting process security, and vote data protection. Consequently, the development of a secure electoral voting system is required.

The traditional voting systems, whether paper-based or electronic, have faced numerous challenges, including voter fraud, duplicate voting, and inefficiencies in the verification process. A fingerprint-based voting system offers a reliable and efficient solution by leveraging biometric technology to authenticate voters, ensuring that each individual can only vote once. Integrating this

system with Aadhaar, India's unique identification number system, enhances its reliability and security.

II. LITERATURE REVIEW

2.1. Biometric features

The measurement and statistical analysis of an individual's distinct physical and behavioral traits is known as biometrics. The primary uses of the technology are in identification and access control, as well as in identifying people or confirming their claimed identities. Biometrics include fingerprints, iris scan samples, and facial images. The fundamental idea behind biometric authentication is that each individual can be uniquely identified by their inherent behavioral or physical characteristics. The Greek words bio, which means life, and metric, which means to measure, are the origin of the word biometrics.

2.1.1. Fingerprint Recognition

Fingerprint biometrics uses the minute details contained in each individual's fingerprint for identification and authentication. A fingerprint is distinguished by these features, which include ridge patterns like loops, whorls, and arches. Ridge count, ridge shape variations, ridge path irregularities, and ridge crossovers all affect fingerprint complexity and uniqueness. Each finger print is unique due in part to the presence of sweat pores and specific ridge characteristics like thickness, width, and shape [5]. A fingerprint pattern's core and delta, which are located in its center and inside its triangle, respectively, aid in classification and analysis. When matching fingerprints, minutiae points like islands, bifurcations, and ridge ends serve as precise markers. These biometric features of fingerprints come together to create fingerprint recognition systems dependable and extensively utilized for identification and security purposes; applications range from secure access control on smartphones and other devices to criminal investigations. Ridge ending, bifurcation, dot, bridge, and crossover are the different types of fingerprint minutia.

2.1.2. Iris Recognition

Iris recognition is a biometric technology that uses an individual's iris, or the coloured portion of their eye, characteristics to accurately and consistently verify their identity. The iris process entails using specialized cameras with infrared or near-infrared light to take a detailed picture of the iris. The intricate patterns found in the iris are taken out and transformed into a digital model, including radial lines, crypts, and freckle-like spots. This model is kept in a secure location and acts as a trustworthy authentication reference point. When authentication is necessary, identity is confirmed by comparing a live iris scan to the stored model and confirming that they match. When it comes to applications requiring strict security, like border control, financial transactions, and secure facility access, iris recognition is a preferred option because of its exceptional accuracy, stability over time, and resistance to fraud. Identity is verified. Iris recognition has the benefit of being easy to use and non-intrusive. It's an easy and comfortable biometric method where people just need to glance into a camera for a short while. Its high accuracy also guarantees low rates of false acceptance and rejection, improving security and user convenience. Because of this, iris recognition has found uses in everyday situations such as unlocking smartphones in addition to high-security settings, proving its adaptability and dependability as a biometric technology.

2.1.3. Facial Recognition

A facial recognition system is a type of biometric technology that uses an individual's distinctive facial features to identify and authenticate them. It works by taking a picture of a person's face using cameras or other sensors, identifying features such as the position of the mouth, nose, eyes, and facial contours, and then transferring this data into a digital template or mathematical representation. This template can be used for further comparisons during authentication and is safely stored. Upon receiving an authentication request, the system verifies the user's identity or grants access based on whether the stored template and the live facial image match sufficiently. Facial recognition systems have found widespread application in diverse fields, including security, law enforcement, access control, and

consumer electronics, due to their non-invasive and user-friendly nature.

2.2. Traditional Voting System

Traditional voting systems, including paper ballots and electronic voting machines (EVMs), have long been the standard for conducting elections.

2.2.1. Paper Ballots

Paper-based voting is straightforward and provides a tangible record of votes. Paper ballots can be easily tampered with or lost, leading to concerns about the integrity of the election results. The manual counting of votes is subject to human error, which can lead to inaccuracies in the final tally. Transporting and securely storing large volumes of paper ballots requires significant resources and coordination.

2.2.2. Electronic Voting Machine (EVM)

EVMs were introduced to overcome some of the challenges of paper ballots. They offer faster vote counting and reduce the chances of human error. EVMs can be susceptible to hacking and other forms of cyber-attacks, which can compromise the integrity of the election. The lack of a paper trail in many EVMs makes it difficult to verify results independently, leading to mistrust among voters. Malfunctions and technical glitches can disrupt the voting process and potentially disenfranchise voters.

2.3. Biometric Voting System

Biometric voting systems utilize physical characteristics, such as fingerprints, to uniquely identify voters. These systems have been studied and implemented in various contexts to improve the accuracy and security of voter identification. Biometric systems significantly decrease the likelihood of voter impersonation and multiple voting attempts. For instance, biometric authentication can effectively distinguish between legitimate voters and fraudsters using false identities. By using unique physical traits, biometric systems ensure a high level of accuracy in voter identification. This accuracy is crucial in maintaining the integrity of the electoral process. Despite their benefits, biometric systems face challenges such as the potential for technical failures, the need for reliable hardware, and concerns about privacy and data security.

2.3.1. Aadhaar-Based Authentication

Aadhaar is a unique identification system managed by the Unique Identification Authority of India (UIDAI), which assigns a 12-digit unique identity number to Indian residents based on their biometric and demographic data. Aadhaar provides a highly reliable platform for identity verification, utilizing both demographic and biometric data. This makes it an ideal foundation for integrating with systems that require secure identification, such as voting systems. Aadhaar has been successfully integrated with various services, including banking, public distribution systems, and direct benefit transfers. These integrations have demonstrated improved service delivery and reduced fraud. The use of Aadhaar data raises concerns about privacy and the potential for data breaches. Ensuring the security of Aadhaar data and addressing privacy issues are critical for gaining public trust.

2.3.2. Security of the Aadhaar based E-Voting

Ensuring voter and vote privacy is the primary objective of a secure electronic voting system. Only votes cast by eligible voters will be considered in a secure electronic voting system that meets all requirements. Votes on anonymity are kept private. Voter accuracy cannot be changed. As a result, after the election has closed, neither ballot additions nor deletions may occur. Partial tabulation for fairness is not feasible. Vote and move on, casting a ballot, a voter cannot do anything more until the election is over. Public verifiability should be able to easily verify that the entire voting process is legitimate.

III. METHODOLOGY

3.1. Block Diagram

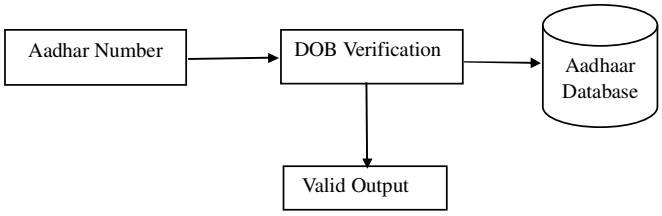

Fig 1: Eligibility Verification

The block diagram illustrates a process for verifying the eligibility of a person to vote based on their Aadhaar number and date of birth (DOB). The starting point of the process where the unique Aadhaar number of the individual is provided as input. It queries the Aadhaar database to retrieve the corresponding details, particularly the date of birth (DOB) associated with the given Aadhaar number. then calculates the age of the individual based on the current date and the retrieved DOB. It checks if the calculated age is 18 or greater. Aadhaar database represents the database that stores detailed information about individuals, including their Aadhaar numbers, dates of birth, Father's name and other details. The DOB Verification process queries this database to get the required DOB for the given Aadhaar number. Valid output represents the result of the DOB verification process. Based on the age calculation, it results whether the individual is "Eligible to vote" or "Not eligible to vote".

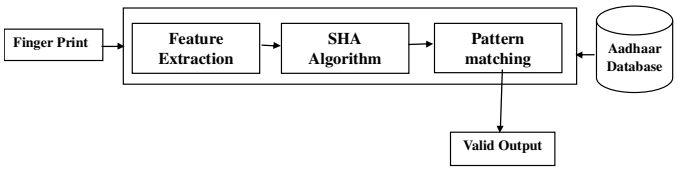

Fig 2: Biometric System

First step involves getting fingerprint from the voter. The voter must press their finger against the sensor-equipped scanner. The primary purposes of optical and solid-state sensors are to record an individual's imprint left by fingers. Visible light is used by optical fingerprint sensors to capture fingerprint images. The ridges and valleys of the fingerprint create a pattern when the user places their finger on the sensor's surface because they reflect or absorb light in different ways. Everybody's fingerprint is unique in its minute details. Solid-state fingerprint sensors do not rely on visual images; instead, they use a variety of technologies to capture fingerprint data. They are ideal for applications where security is of the utmost importance because they typically offer better resistance to spoofing and higher accuracy [9]. The feature extractor's job is to use measurements to characterize the object that needs to be found. Data integrity and security are improved by the use of the Secure Hash Algorithm (SHA). Aadhaar databases hold a wealth of data about Indian people, including photographs, fingerprint images, Iris, minutiae, and other personal information.

3.2. Feature Extraction

The fingerprint biometric system is a safe and reliable form of identification that confirms a person's identity by analyzing their fingerprint patterns and characteristics. The fingerprint features that are used to verify the person identity and proceed with authentication for further process are,

i) Ridge ending
ii) Bridge
iii) Crossover
iv) Bifurcation
v) Delta
vi) Enclosure

i) Ridge Ending

Ridge ending is critical minutiae feature where a friction ridge abruptly terminates within the fingerprint pattern. These ridge endings are vital for biometric identification as they serve as unique points that can be used to distinguish one fingerprint from another. Accurate detection of ridge endings involves analyzing the fingerprint image to locate where the ridges terminate, which is essential for creating a detailed and reliable fingerprint template. The presence, position, and orientation of these ridge endings are assessed by the system during the verification process in order to determine the validity of the fingerprint that is being presented. Any differences or irregularities in the ridge endings should be taken seriously as they may indicate that a voter has cast their ballot already or is attempting to impersonate someone.

ii) Bridge

The term "bridge" describes a particular location in a fingerprint pattern where two ridges join together or take the form of a bridge. Addition to ridge ends and bifurcations, these minute details act as distinctive traits that set one person's fingerprint apart from another. The captured fingerprint is examined for these minute details, such as bridges,

during the voter verification process [13]. The system is capable of authenticating the voter during an election by comparing the minute details it has noticed to a preregistered template. Due to the individual fingerprint's distinctiveness and minute details providing a strong and dependable means of identity verification, this biometric authentication method offers a high degree of security and works to prevent voter fraud.

iii) Crossovers

A crossover is a specific type of minutiae where two ridges intersect or cross each other. This pattern is less common compared to other minutiae such as ridge endings and bifurcations, but it adds to the uniqueness and complexity of a fingerprint. Crossovers contribute to the detailed fingerprint pattern used in biometric identification and verification systems. This unique pattern, alongside other minutiae like ridge endings and bifurcations, enhances the distinctiveness of a fingerprint, thereby improving the accuracy of the verification process. During voting, an individual's fingerprint is scanned, and the minutiae, including crossovers, are extracted and compared to pre-registered fingerprint templates stored in the database. The presence of crossovers helps in creating a more detailed and robust fingerprint template, which ensures a higher degree of precision in matching the voter's fingerprint with the stored data. This process is crucial in preventing fraud and ensuring the integrity of the voting system, as it verifies the voter's identity based on their unique biometric features, thereby facilitating a secure and reliable voting environment.

iv) Bifurcation

Bifurcations, a small biometric detail, are essential to confirming an individual's identity.These points show where a single ridge divides into two branches, creating a clear Y-shaped pattern. Bifurcations are extremely significant because they provide special and detailed details that add to the fingerprint's uniqueness. In order to verify the identity of the person involved in the authentication process, the existence and exact configuration of bifurcations are examined [15]. The template captured during voting process is compared to pre-registered templates that stored in the database to verify the voter's identity. The inclusion of bifurcations enhances the uniqueness of the fingerprint template, making it more robust and less susceptible to errors or fraudulent attempts. By accurately identifying and analyzing bifurcations, the fingerprint verification system ensures secure and precise voter authentication, thereby maintaining the integrity of the voting process and preventing unauthorized voting.

v) Delta

A delta is a specific reference point characterized by a triangular or Y-shaped pattern where three ridge flows meet. This formation typically occurs in fingerprints with loop and whorl patterns. The delta is crucial in classifying fingerprints and serves as a landmark for orienting and aligning fingerprint images. Its presence helps in the detailed analysis of fingerprint patterns, facilitating accurate matching and identification in biometric systems. Deltas are essential in creating a unique fingerprint template, contributing to the precision and reliability of fingerprint recognition processes. These delta points act as anchor points for additional minutiae mapping and aid in precisely orienting the fingerprint. To confirm the voter's identity, the extracted features are compared with pre-registered fingerprint templates kept in the database. The accuracy with which delta points are located and analyzed adds to the fingerprint verification process' general dependability and security, guaranteeing that only voters who are registered may cast ballots and maintaining the electoral system's integrity.

vi) Enclosure

Enclosure refers to specific features or patterns found within fingerprint ridge structures. Enclosures are small, circular or oval areas where a single ridge splits into two ridges that then converge back into a single ridge, creating a loop-like feature. These patterns are part of the minutiae points used in fingerprint analysis to identify and verify individuals. The presence, location, and type of minutiae, including enclosures, are critical for matching fingerprints in biometric systems, ensuring accurate

and reliable identification. Enclosures offer an extra degree of verification and can be utilized to boost trust in the authenticity of a fingerprint. Any disparities or irregularities in enclosure patterns have the potential to activate additional security measures, thereby augmenting the overall dependability and resilience of the fingerprint biometric voting process. Enclosures provide an additional level of scrutiny to guarantee the accuracy and integrity of the authentication in the voting process, even though they are less frequent than other minutiae types.

3.3. SHA Algorithm

In biometric systems, Secure Hash Algorithm can improve security and data integrity in a number of crucial ways. SHAs operate by generating a fixed-length output from a variable-length input known as a hash value [10]. Finding two distinct inputs that yield the same hash value is extremely difficult. The hash value serves as a unique identifier for the input data. A biometric system could make use of the SHA-256 algorithm.

➢ The eligible voter's fingerprint is already in the Aadhaar database.

➢ The fingerprint images that are present in the Aadhaar database is pre-processed to improve the quality and consistency that involves noise reduction and feature extraction.

➢ The pre-processed fingerprint images are hashed using SHA-256 algorithm. The algorithm produces 256-bit hash value as a result.

➢ The result hash values are stored in a database as pre-registered fingerprint templates.

➢ During the election process, the voter's fingerprint is capture using a fingerprint scanner.

➢ The captured fingerprint is pre-processed again.

➢ The pre-processed fingerprint image is hashed using the same SHA-256 algorithm. The result hash value is the compared with the pre-registered fingerprint templates.

➢ If two hash value is similar then the voter's identity is verified and authenticated to proceed further election process. Otherwise, the elector cannot vote.

3.4. Pattern Matching Algorithm

A fingerprint pattern matching algorithm involves multiple stages to ensure accurate identification. the algorithm aligns two fingerprint templates by translating and rotating them to find the optimal overlap. The similarity is quantified using metrics like Euclidean distance between corresponding minutiae points [14]. The matching score is calculated based on the number and quality of matching minutiae. This score is then compared to a predefined threshold to determine if the fingerprints match, achieving reliable identification crucial for biometric systems used in security and identity verification.

Step 1: Minutiae Point Representation

In fingerprint recognition, representing minutiae points is a critical step that involves identifying and encoding the distinctive features of the fingerprint's ridge patterns. Each minutia point is characterized by specific attributes: its location (x, y coordinates) within the fingerprint image, the orientation or angle of the ridge at that point, and the type of minutia (e.g., ridge ending or bifurcation). These features are extracted from the pre-processed fingerprint image, which has been enhanced to highlight ridges and valleys. The minutiae data are then stored in a structured format, such as a minutiae template, which serves as a concise and unique representation of the fingerprint. This template is used in subsequent steps for comparison and matching, ensuring accurate and efficient fingerprint recognition. Compare the exact details between the pre-processed templates and the current fingerprint. This pairing is determined by their proximity and type (ridge ending or bifurcation) [11, 12]. The closest matching minutiae point from the pre-processed fingerprint is paired with each minutiae point in the current fingerprint.

Step 2: Calculating Euclidean Distance

Calculating the Euclidean distance between two points in a fingerprint recognition system involves measuring the straight-line distance between corresponding minutiae points in the two fingerprint templates. The Euclidean distance formula in a 2-dimensional space is:

$$Euclidean\ Distance = sqrt((x1 - x2)2 + (y1 - y2)2\ )\ (1)$$

Each minutia point is represented by its coordinates (x,y) . The minutia points from the first fingerprint as $(x1,y1)$ and the corresponding minutia points from the second fingerprint as $(x2,y2)$. This distance measurement is repeated for each pair of corresponding minutiae points in the two fingerprint templates. The overall matching score can then be computed based on these individual distances, with smaller distances indicating a closer match.

Step 3: Threshold Comparison

In fingerprint recognition involves threshold comparison, where the aggregated matching score, derived from the Euclidean distances between corresponding minutiae points in two fingerprint templates, is compared to a predefined threshold value. If the matching score is less than or equal to the threshold, the fingerprints are considered a match, indicating a close similarity between the minutiae points. Conversely, if the score exceeds the threshold, the fingerprints are not considered a match, suggesting significant differences.

Step 4: Decision

If the total distance is less than the threshold, the fingerprints are deemed to match, and the voter's authentication is accepted, according to the threshold comparison. The voter's access to vote is refused if the total distance surpasses the threshold and the fingerprints are deemed to not match.

IV. PROPOSED SYSTEM

The electronic voting machine that is currently in use lacks a biometric system. Thus, voter fraud, impersonation, and administrative errors are made easy. These are the typical issues that arise during an election. The suggested system resolves these problems. An increasingly safe election process is provided by combining biometric features with Aadhaar details.

4.1. Working Principle

The voter first provides the voting system with their Aadhaar number. Following the acquisition of an Aadhar number, the voter's age is verified against the Aadhaar database. If the voter is older than 18, they are eligible to vote; if not, they are not. The eligible voter can use the fingerprint scanner to continue the authentication process by putting their finger in it. The Aadhaar database's biometric features are compared. Voting is permitted when the fingerprint pattern matches the Aadhar database; otherwise, the elector's right to vote is revoked.

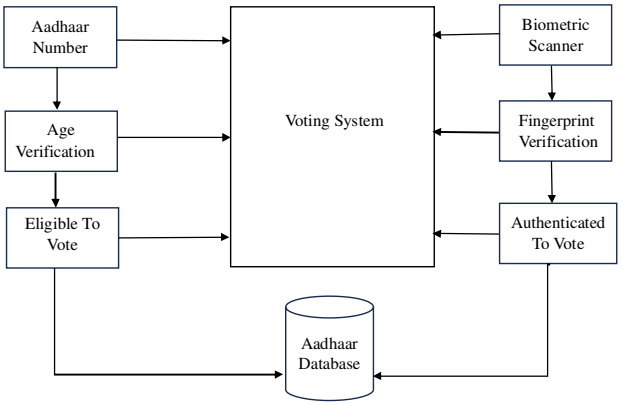

Fig 3: Architecture of Voting System

4.2. Algorithm

4.2.1 Eligibility Check

Input: Entering Aadhaar number

In order to verify their age during the election process, voters must input their Aadhar number, which starts the input phase.

Process:

Age Verification The point at which the individual's unique Aadhaar number is entered into the process. To obtain the relevant information, especially the date of birth (DOB) connected to the provided Aadhaar number, it makes a query to the Aadhaar database. then determines the person's age using the retrieved DOB and the current date. It determines whether the computed age is eighteen or older.

Output:

Eligible or Not To obtain the necessary DOB for the specified Aadhaar number, the age verification

procedure runs a query against this database. The outcome of the DOB verification procedure is represented by valid output. Whether a person is older than eighteen and therefore "Eligible to vote" or "Not eligible to vote" is determined by calculating their age.

4.2.1 Fingerprint Authentication

Input: Fingerprint Scan

When the elector inserts their finger into the scanner, the input phase starts. For the purpose of authentication, the voter's fingerprint is scanned by the voting system.

Process: Fingerprint Verification

The system captures the fingerprint of the elector and compared it, against the stored templates in the database. Both the fingerprint must match for verification.

Output: Approve to vote or denied

The elector's stored fingerprint and current fingerprint must match in order for voting to be authorized. The voter's right to vote will be denied, otherwise.

V. IMPLEMENTATION

5.1 VOTER

Implementation process begins when the voter enters their Aadhar number as input the moment when each person's distinct Aadhaar number is input into the system. It queries the Aadhaar database to retrieve the data, particularly the date of birth (DOB) associated with the supplied Aadhaar number. then uses the current date and the retrieved DOB to determine the person's age. It establishes if the calculated age exceeds eighteen years of age. The age verification process queries this database to retrieve the required DOB for the given Aadhaar number. Valid output is a representation of the DOB verification procedure's result. A person's age determines whether they are "Eligible to vote" or "Not eligible to vote" based on whether they are older than eighteen.

5.2 VOTING SYSTEM

The elector puts their finger inside the scanner. The voting system scans the voter's fingerprint for the purpose of authentication. The fingerprint of the elector is taken by the system and compared to templates that are stored in the database. To ensure authenticity, both fingerprints must match. Voting authorization requires a match between the voter's stored fingerprint and current fingerprint. If not, the voter will not be allowed to cast a vote.

VI. CONCLUSION

The best answers to issues pertaining to the Indian voting system can be found in this system. The voting percentage is raised in part by this system. Voters can cast their ballots through fingerprint recognition authentication in our voting process, which makes sure that no unauthorized person can manipulate the voting process.

After studying fingerprint based secure voting system, it is reasonable to conclude that the majority of the issues encountered by the EVM system during the voting period have been resolved. This document guarantees a safer voting process, which is essential for a developing country to grow healthily. This paper proposes a biometric online voting system that uses a fingerprint scanner. It is faster and more accurate than the previous system. There will be an opportunity to prevent invalid votes through the online voting system that uses a fingerprint scanner. Voting under this system will only be available to those who have been verified and registered.

One of the cutting-edge methods for confirming and identifying a person is fingerprint analysis, a difficult field in the biometrics industry. By comparing two fingerprints, the fingerprint verification stage determines whether they belong to the same individual. Even though a number of strategies have been put forth in the literature thus far, each has advantages and disadvantages of its own. The majority of them are the subject of this paper, which also offers an improved solution.

Future developments and improvements are made possible by the fingerprint-based voting system. Potential areas of future research include: Expanding accessibility by enabling remote voting within electoral boundaries. Strengthening security protocols to safeguard voter information and system integrity. Investigating the use of cutting-edge

biometric authentication techniques to achieve even higher accuracy. We can help advance safe and effective democratic processes by expanding and continuously improving the Fingerprint-based voting system.

REFERENCES

[1] Khasawneh, M., Malkawi, M., & Al-Jarrah, O. (2008). A Biometric-Secure e-Voting System for Election Process. Proceeding of the 5th International Symposium on Mechatronics and its Applications (ISMA08). Amman, Jordan.

[2] Yinyeh, M. O., & Gbolagade, K. A. (2013). Overview of Biometric Electronic Voting System in Ghana. International Journal of Advanced Research in Computer Science and Software Engineering.

[3] Annisara Nadaph, Rakhi Bondre, Asmita Katiyar, Durgesh Goswami, "An Implementation Secure Online Voting System" International Journal of Engineering Research And General Science, Volume 3, Issue 2, [ISSN2091-2730] Page no. [1110-1118].

[4] A. K.Agarwala, D. T. Shahani, and P. V. Indiresan. Report of the expert committee for evaluation of the upgraded electronic voting machine (EVM). Sept. 2006.

[5] Abdullah Saud1 , Nazar Elfadil, "Biometric Authentication by Using Fingerprint Recognition System", International Journal of Scientific Engineering and Science, Volume 4, Issue 5.

[6] R. Murali Prasad, Polaiah Bojja and Madhu Nakirekanti, AADHAR based Electronic Voting Machine using Arduino, International Journal of Computer Applications (0975 – 8887) Volume 145 – No.12, July 2016.

[7] V Kumar Yadav, S Batham, M Jain and S Sharma (2014). An approach to electronic voting system using UIDAI. 2014 International Conference on Electronics and Communication Systems (ICECS).

[8] B. Rudrappa. Gujanatti, Shivaram N. Tolanur, Murughendra S. Nemagoud, & Shanta S. Reddy, Sangameshwar Neelagund. A Finger Print based Voting System. International Journal of Engineering Research and, V4(05), 887–892. (2015).

[9] Wencheng Yang , Song Wang , Jiankun Hu , Guanglou Zheng and Craig Valli, "Security and Accuracy of Fingerprint-Based Biometrics: A Review" , Symmetry.

[10] Iti Malviya, Prof. Tejasvini Chetty, " Performance and Limitation Review of Secure Hash Function Algorithm", International Journal on Recent and Innovation Trends in Computing and Communication , Volume: 7 Issue: 6.

[11] Roli Bansal , Priti Sehgal and Punam Bedi, "Minutiae Extraction from Fingerprint Images - a Review", IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 5, No 3, September 2011.

[12] Neeraj Bhargava, Ritu Bhargava, Manish Mathuria, Minaxi Cotia, "Fingerprint Matching using-End and Bifurcation Points", International Conference in Recent Trends in Information Technology and Computer Science.

[13] Ziad Alqadi , Mohammad Abuzalata , Yousf Eltous , Ghazi M. Qaryouti, " Analysis of Fingerprint Minutiae to Form Fingerprint Identifier", International Journal On Informatics Visualization, VOL 4 (2020) NO 1.

[14] K. Martin Sagayam, D. Narain Ponraj, Jenkin Winston, Yaspy J C, Esther Jeba D, Antony Clara, "Authentication of Biometric System using Fingerprint Recognition with Euclidean Distance and Neural Network Classifier", International Journal of Innovative Technology and Exploring Engineering (IJITEE), Volume-8 Issue-4, February 2019.

[15] U.A. Wakpanjar., Shamkule, A. A., Tiwari, R. J., Sagane, S. C., Akshay, P., & Raut, N. V. Online voting system using fingerprint scanner. 3421–3423. (2018).

[16] P., Abdallah, A., Mohammed, E., Abdallah, E., Osman, A. Ali, M. Implementation of Electronic Voting System Using Fingerprint Recognition Technique. (2016).

[17] Harminder Kaur, Poonam Dabas, "Minutiae Based Fingerprint Recognition", International Journal of Engineering Research & Technology (IJERT), Vol. 3 Issue 6, June – 2014.

[18] Anandaraj S, Anish R, Devakumar P.V, "Secured electronic voting machine using biometric". IEEE, 2015 International Conference on Innovations in Information, Embedded and Communication Systems, .19-20 March 2015.

[19] S. Chakraborty, Mukherjee, S., Sadhukhan, B., & Yasmin, K. T. Biometric voting system using aadhar card in india. International journal of Innovative research in Computer and Communication Engineering, 4(4).(2016).

[20] R.S. Raj, Raghavendra, A., Madhushree, K. R., & Bhargavi, D. An online voting system using biometric fingerprint and Aadhaar card. IJCAT International Journal of Computing and Technology, 1(4), 87-92(2014).

