

Biometrically Secured Fingerprint Voting

Khadija Hasta¹, Aditya Date², Aparna Shrivastava³, Prajakta Jhade⁴

^{1,2,3,4} UG Student, Computer Engineering, Sinhgad Academy of Engineering, Kondhwa, Pune [India]

Abstract - In the present day, elections in most countries of the world are usually held using Electronic Voting Machines, Efforts should be made to provide Security, ensuring that no person exercises the right to vote, twice. A solution to the issue could be the introduction of Fingerprint Based Voting, where a person can be authorized to vote based on his fingerprint. The domain of the proposed paper is Internet of Things where a Fingerprint Based Biometric Voting Machine is developed using Arduino. The paper proposes an online voting system through an application where the user is recognized by his fingerprint pattern. The minutiae features of the fingers of each human being are different, thus the voter can be easily authenticated and can then cast his vote. A fingerprint module is used to uniquely store and identify the fingerprints. A key feature of the system is the ability to let a voter cast his vote only once hence maintaining the credibility of a democracy.

KeyWords: Fingerprint, Minutiae, Electronic Voting, Authentication, E-Voting, Paper Ballot System, Arduino

1. INTRODUCTION

One of the most critical ways that people can influence governmental decision-making is through voting. So, it's designed with great care to offer high security. Regarding the current voting system in India, it requires a lot of manual operations, entertain rigging to some extent, prone to security threats, are slow and are not so user-friendly according to this new age of information and technology. That is the main reason why online voting system is introduced. Therefore, to keep in mind the limitations, this voting system is brought into picture which uses voter's fingerprint as a biometric to avoid security and privacy threats.

So basically our voting system requires a voter's finger impression for identification or authentication as it is unique for each voter. Therefore, at the time of voting, when the voter places his/her finger on the fingerprint module, it scans the finger impression of the voter and the system compares that particular impression with earlier existing impressions that the database stores to get the correct identity. The comparison is based on the minutiae features of the fingerprint. If in comparison, the impression matches the

existing one stored in the database, then the system will allow the voter to go ahead for voting or else won't allow the voter for further voting procedures.

For a voting system to be faultless, some main characteristics must be prioritized first: safety, reliability, obscurity, adaptability, speed, precision, and user friendly. Online voting systems are software platforms used to securely conduct votes and elections. As a digital platform, they eliminate the need to cast your votes using paper or having to gather in person. These services help organizations save time, stick to best practices, and meet internal requirements and/or external regulations.

The primary focus of our online voting system is to develop an application that will facilitate free and fair elections as the real-time tallying of votes cannot be tempered which will lead to the faster election process and quick results. A database is kept centralized where the citizen's (consisting of voters and candidates) information is validated and clustered. The repetition of votes is checked for in this system with accurate coding. Hence with the application of this fingerprint-based EVM system, elections could be made fair and free from rigging and would be no longer a tedious and expensive job. [10].

1.1 Problem Background

In a democratic system of governance, election plays a very crucial role and the integrity of the electoral process comes out to be sacrosanct. Online voting system has been labelled as an optimum solution but is considered as a menace in some cases. Cases of non-confidential, faulty, inappropriate execution of the application that has led to security and privacy negligence have been identified in the current reports. Therefore, in order to gain the citizen's trust, these limitations and difficulties must be eliminated.

1.2 Problem Statement

Keeping in mind the security threats, reliability, user accessibility and adaptability an Online Voting System should be designed where it opens a registration form for voters to vote using their fingerprints as a biometric

2. RELATED WORK

2.1 Paper Ballot System

Before the concept of electronic voting was brought into consideration, India used paper ballots and manual counting. Due to forged voting and booth capturing, the paper ballot system was widely criticized. The printed paper ballots were also more expensive, as it needed significant post-voting resources to count hundreds of millions of paper ballots. [4].

The ballot paper has an advantage of its own that it cannot be hacked easily. Even after voting, the ballot papers are watched by the observers of the main parties. The ballot paper is still used in some countries worldwide.

The disadvantages include high cost of paper handling equipment and transport, ballot counting discrepancies, voter coercion, ballot box stuffing during and after elections, breaching due to multiple avenues that exist for the voters. [4].

2.2 Electronic Voting System (EVM)

The EVMs were first conceived by the state-owned Electronics Corporation of India and Bharat Electronics in the 1990s.

Control unit and balloting unit, are the 2 main components of the EVM and are connected by a five-meter cable. Balloting unit allows voting to a voter through labeled buttons while the control unit takes control over ballot units, stores the voting counts and provides the result through a 7 segment display. The polling booth officers take control over the control unit of the EVM while a voter operates a balloting unit in private. Once the voter enters the vote, the vote is displayed to the voter through the balloting unit. A "close" command is issued after which the vote is registered. The unit gets relocked to prevent multiple votes by the same voter [1], [3].

EVMs have a major edge over the paper ballot system. Paper ballots, which act as a major chunk of the costs incurred, have been replaced by electronic ballots which further restricted the wastage of tons of papers.

When it comes to disadvantages, cases have been reported regarding faulty EVMs, VVPAT-EVM mismatch, and EVM tampering but are not proven by any evidence so far [6], [7].

3. PROPOSED SOLUTION

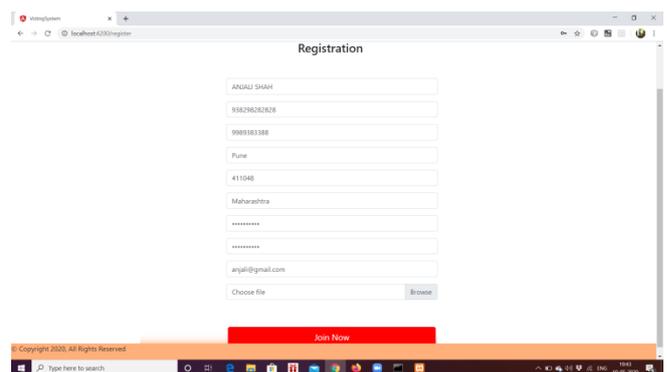
An electronic voting website will be created for registration and voting. Through the registration form, data of all the voters will be collected and database will be created.

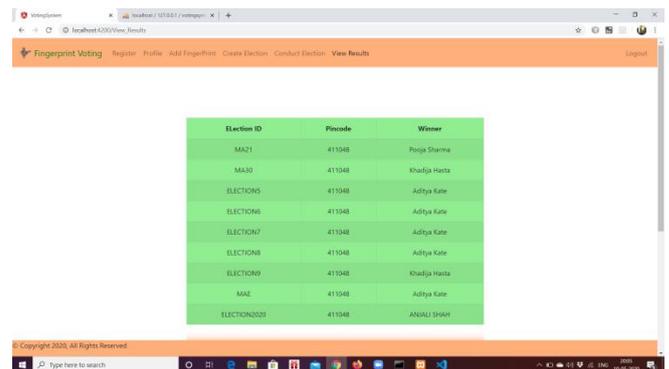
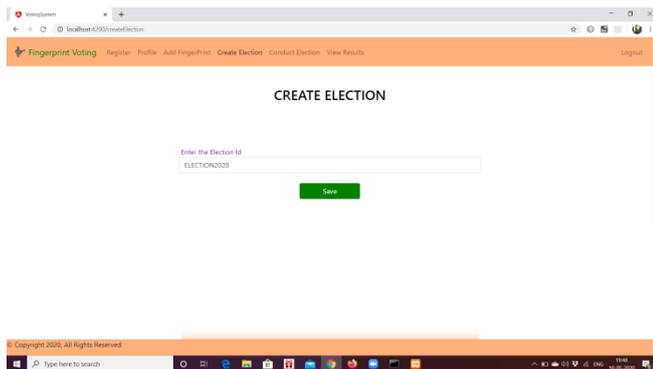
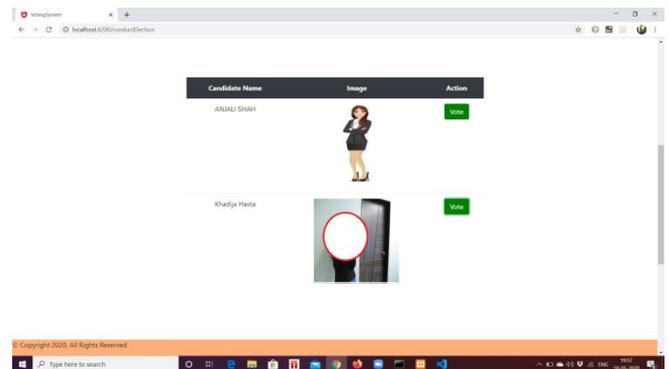
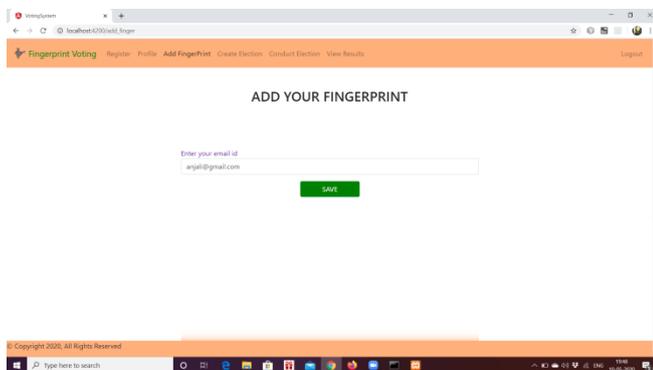
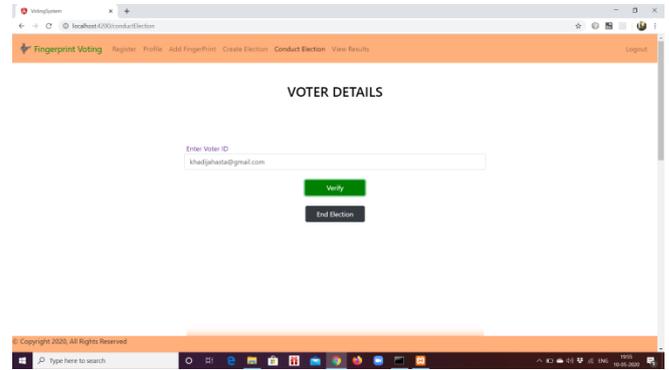
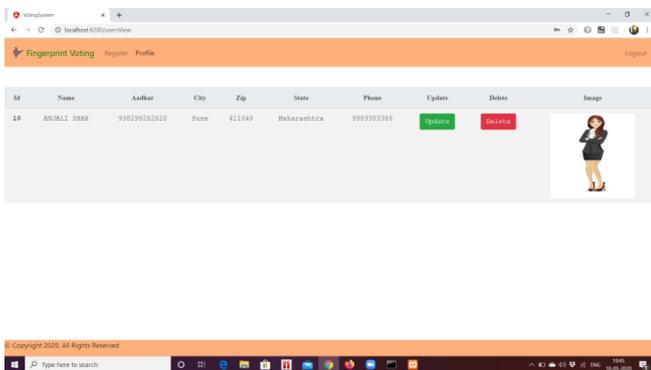
3.1 Algorithm

An application form will be created for registration purpose of the voter. Through this registration form, the data of all the voters is collected and a database is created. This database will be available on server. An admin will be available to administer the whole voting process i.e. from the login of the candidates and the voters to the results of the election process. Admin will authenticate the user by verifying the user's identity proofs and fingerprint. The voter is then allowed to enter the election by entering his/her voter id and fingerprint.

At the time of voting the voter would scan his finger on fingerprint scanner which will match the template generated by the current fingerprint of the voter and the previously stored template on the database.

If the voter's fingerprint matches the fingerprint previously stored and if he has not yet casted his vote, then he would be further sent for casting his vote, else he would not be allowed to vote, thus not letting a person vote twice. E-ballot using a website would appear on the screen under his name. The voter would cast his/her vote by clicking on the option available. After the voter has voted, a POP UP window will appear and notify the voters about the candidate for which he has casted his vote. As the database is available on the main server the voter can cast his vote from anywhere or any region by entering his region's ward number.





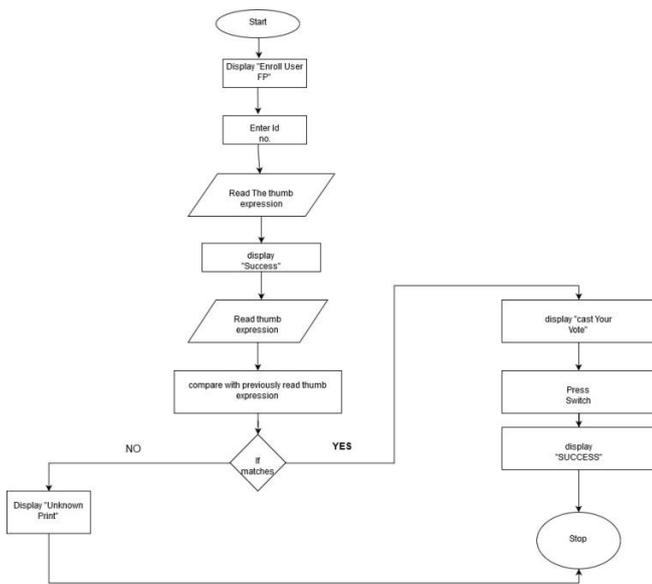


Fig. 1. Flowchart of an Online Fingerprint Voting System

3.2 Architecture

The architecture of our project contains a website, a fingerprint module and a database where the information of the different actors taking part in the process is saved. The frontend of the project is done using AngularJs, server side using Php and database used is Mysql.

The information of the actor is passed on to the database using the User Interface. Also the fingerprint is passed on to the fingerprint module where it is extracted and stored into the database.

When a voter comes to exercise his vote, his fingerprint is taken and matched with the one present in the database to authenticate the voter. If the fingerprint given matches the one in the database then he is allowed to vote, else a warning is issued.

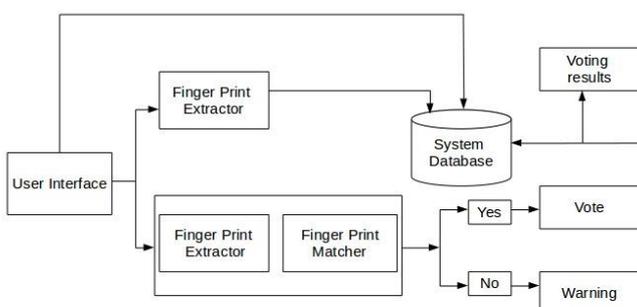


Fig. 2. System architecture of the fingerprint voting system

4. PERFORMANCE EVALUATION

The hardware setup successfully implements the EVM with the help of the Fingerprint module and Arduino. The result of the voting count gets displayed on the website, and thus the winner of a particular election is announced. Operation shows innovative and secure process of voting. We have designed Biometric voting machine for small scale purpose like institutes and organization. This concludes that fingerprint is useful for voting.

To test accuracy of the system, fingerprints of around 55 people were collected. Later on, while conducting voting process, from among 60 people (5 not registered) the fingerprints of 53 people were recognized accurately by the system. Using the confusing matrix, the value of True Positive (TP) and False Negative (FN) was calculated to be 53 and 2 respectively with a sensitivity of 97%. The system was found to be quite user friendly and easy-to-understand.

5. CONCLUSION

The paper is used to enhance security by eliminating bogus voting and vote repetition using fingerprint based authentication. Expected outcome of our proposed architecture is safe and secure voting system with accurate and fast voting results. Our proposed architecture will definitely overcome the drawbacks of the traditional methods and would ensure secure results.

6. FUTURE SCOPE

According to the presented work in this paper, there are very advanced attributes that we can put on with the system. Attribute merging in multimodal biometric can be work by various combinations of attributes. The proposed method can be extended by fusing other biometrics traits such as irises, DNA , palm print and gait [10].

We could work on conceiving an algorithm which can predict the specific minutiae plot points, gender and the accurate age of the person to whom the fingerprint belongs. When a thumbprint impression is given as input, it should show the minutiae points, the gender and the accurate age in the output graphical user interface. The proposed algorithm for the minutiae recognition, gender categorization and age categorization can be tried on the raw fingerprint images. Criminal identification can be done in a more proper and efficient manner as the proposed algorithms can be tested on the data or fingerprints identified from the crime scene. Fingerprints and gaits go hand in hand and the relationship between these two can be scrutinize in the near future Fuzzy logic and genetic are some of the eminent soft computing techniques which can be used.

Programming could be comprised with Neural Network and Support Vector Machine to acquire more exact output. To increment the achievement, the fingerprint biometrics can be fused with other biometric techniques near future [5], [7].

International Conference on Electronic Systems, Signal Processing, and Computing Technologies, 2014.

7. REFERENCES

[1] Himanshu Agarwal and G.N. Pandey "Online Voting System for India Based on AADHAAR ID" 2013 Eleventh International Conference on ICT and Knowledge Engineering.

[2] Smita B. Khaimar, P. Sanyasi Naidu, Reena Kharat "Secure Authentication for Online Voting System".

[3] Shivendra Katiyar, Kullai Reddy Meka, Ferdous A. Barbhuiya, Sukumar Nandi "Online Voting System Powered By Biometric Security" 2011 Second International Conference on Emerging Applications of Information Technology.

[4] UIDAI. (2012). Role of Biometric Technology in Aadhaar Authentication.

[5] Ashwini Walake, Prof. Ms, Pallavi Chavan, "Efficient Voting system with (2,2) Secret Sharing Based Authentiation", (IJCSIT) International Joulal of Computer Science and Infonation Technologies, Vol. 6 (1), 2015, 410-412.

[6] Adam Stubblefield, Aviel D. Rubin, Dan S. Wallach, and Tadayoshi kohno "Analysis of an Electronic Voting System", in IEEE, May 2004.

[7] Pranay R. Pashine, Dhiraj p, Ninave, Mahendra R, Kelapure, Sushil L. Raut, Rahul S, Rangari, Kamal O. Hajari, "A Remotely Secured EVoting and Social Govellance System Using Android Platform", International Journal of Engineering Trends and Technology (UETT) - Volume9 Number 13 - Mar 2014.

[8] Shivendra Katiyar, Kullai Reddy Meka, Ferdous A, Barbhuiya, Sukumar Nandi, "Online Voting System Powered By Biometrie Security Using Steganography" Second International Conference on Emerging Applieations of Infonation Technology, 2011.

[9] Rahul V. Awathankar , Monika A Wadhai , Suraj Sawant, "I- Voting: A System For Every Citizen of India" International Journal of Control Theory and Application, Volume 10, [ISSN-0974-5572] Pageno.[125-130]

[10] S.M, Jambhulkar, Prof. Jagdish B. Chakole, Prof. Praful. R. Pardhi "A Secured Approach for Web Based Internet Voting System using Multiple Encryption", 2014