# Secure E-Voting System For Election Using Biometric

Jitendra R. Khairnar
CTIS, *CSE*
*Sandip University*
Nashik, India
jitendrakhairnar@gmail.com

Nitin B. chavan
CTIS, *CSE*
*Sandip University*
Nashik, India
Nitin.chavan@sandipuniversity.edu.in

***Abstract*—** Elections in the country are most important events. Documentation and processes done at very large amount. Complex and big data need to handle. Manually working on this large data may reduce accuracy of operations. So computational methods can be helpful for better and fast results. In this paper we propose a online e-voting system. Basic idea of e- voting is to analyses, store and operate voting related data in the form of digital information. E-voting is available in two types : one is online voting and second is offline voting. Security of data, security of voting process, authentication and authorization are main challenges in E- voting. Because of all that reasons e-voting is very much important. The proposed system is designed such a that it can be able to handle electronic ballots with multiple scopes at the same time, e.g. parliamentary, amongst others, presidential, municipal. The system caters for integrity of an election method in terms of the practical and non-functional needs. Transparency of voting follows through altogether phases of an election method to assure the elector that his/her vote went in favor of his/her candidate of selection. Besides its main practical properties, the proposed system is designed to cater for several essential nonfunctional requirements. These results offer the right grounds that will guide the choice maker in customizing the projected system to suit his specific voting desires.

***Keywords*— *Biometric, Fingerprint, evoting, election, authorization, Privacy, security, Data Mining, Udai Data, Data integration.***

## I. Introduction

Here we are simulating the worldwide voting system from anyplace. That means that the user will access cast they vote from them home laptop, web restaurant , office PC. For this we tend to are connecting the user laptop with the voting server via local area Network (LAN). The user needs to go online to the voting server via own laptop. They will be asked for the authentication of identity. The user can then authenticate them ID using Fingerprint recognition.

The main idea of the project is to enable the citizen to vote from any wherever. Moreover to {prevent} fraud voting we also are giving a voter identification hardware which can prevent any hacker from giving false votes. One of the basic mechanisms for democracy is election. It is the way to collect the general public opinions to create a democratic government. The traditional method of election is fairly uneven full, time consuming and has a cumbersome procedure in preparation and tallying phases. To overcome these difficulties electronic voting system is introduced. EVS continues to grow as long because the world becomes a lot of dependable on the new technologies. EVS provides a great deal of advantages than ancient voting systems. It endeavours to enable capable and reliable elections.

EVS is cheap as a result of it's capitals are utile. Also it doesn't would like any geographical vicinity of voters, and it provides higher measurability for big elections meanwhile exploitation EVS should satisfy some security necessities like authentication, voter privacy, confidentiality, integrity, etc.

**1. Ethernet based LAN**: PC is interfaced with an Ethernet module. Using VB language and socket programming we are communication with PC. Here we have the IP address and port number. Once the user authenticated using fingerprint then login procedure is executed.

**2. Fingerprint Recognition:** Here we are using Fingerprint module to recognize the voter using biometric recognition.

## II. Authenticity of the Voting Process and Privacy of the Voter Rights:

Certain factors play out massive in a given voting method in any particular country. Culture itself and therefore the underpinning social factors/values mostly verify the rules and regulations that govern any voting method. In countries, where election results are determined through the voter counts that are tallied by directly depositing specially designed voting cards into the voting boxes, there are tendencies that electoral votes can get misappropriated in many ways; some voters would tend to attempt to vote more than the number of times permissible by law for a given candidate; other voters may try to vote in lieu of other illegible voters so that the voter count would weigh favorably towards one candidate or another, to mention just a few. Counterfeit/Malice is yet issue which will jeopardize the integrity of an election method. Automating an election process, while relying on state-of-the-art in computer and ICT technologies, can significantly mitigate many of the factors that would hamper a healthy progress of an election process. Nonetheless, relying totally on available information technologies can only warrant the authentication/validation of the identity of a given voter, but, still, would not have the capacity to block any attempted abuse of the voting system, viz., those voters who simply try to vote on behalf of others (fraud). Without extra measures, the integrity of a voting process, within the proper context, is far from any acceptable standard/s; the incorporation of biometry would undoubtedly have an extra worth towards achieving the specified levels of election integrity.

Present day applications, including banking applications, guarding of high-security establishments, monitoring of passengers across border posts, amongst many others are witnessing increasing levels in the use of biometric technologies and devices. Biometrics is best outlined as measurable physiological and / or biological characteristics that may be used to verify the identity of a personal. They embrace fingerprints, retinal and iris scanning, hand geometry, voice patterns, facial recognition, Gait recognition, DNA and other techniques. They are of interest in any area wherever it's necessary to verify truth identity of a personal. Initially, these techniques were employed primarily in specialist high security applications; however, we are now seeing their uses and proposed uses in a much broader range of public facing situations.

Essentially, a biometric system follows 2 characteristic traits: identification and verification. The former involves characteristic an individual from all biometric measurements collected during a information. The question that this method seeks to answer is: “who is this?” It, therefore, involves a one-compared-to-many match. Verification involves authenticating a person’s claimed identity from his/her antecedently listed pattern. “Is this who he claims to be?” is the question that this process seeks to answer. This involves a one-to-one match [6, 7]. Verifying the identity of an individual against a given biometric measure involves 5 phases that the system must undergo. At the start, input data is read from the person through the reading sensors. Collected information is, then, sent across a network to some central database hosting a biometric system. The system can, then, perform identity matching using standardized and/or custom matching techniques. Figure 1 illustrates information flow during a typical biometric authentication method.

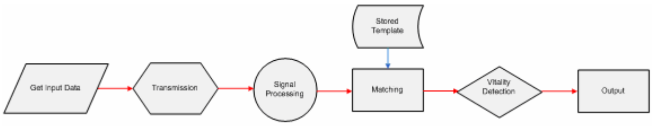

Figure 1 - Biometric System data flow

The incorporation of biometric technologies are often as straightforward as employing a single biometric. However, one biometric measure is often subject to security breaches, if not properly attended and administered. This naturally includes security passwords, fingerprints, and signatures, all of which can be spoofed when applied in a non-properly attended environment. This is considerably mitigated and system security increased with the right application of combined straightforward biometric measures. The application of combined weak biometrics results in systems that are less advanced and additional strong in terms of the protection levels earned. There are robust single biometric measures that involve retinal and iris scans that are rather onerous, if not not possible, to breach, but usually lead to more complex systems which, in turn, slow down the underlying biometric matching method due to the quantity of information process concerned. For these reasons, amongst others, the type of biometrics addressed in this work is of the former type that involves combined biometrics of the weak types. This will be elaborated upon in the succeeding sections.

Section III of this paper provides an outline of the planned e-Voting system.

## III. THE PROPOSED E-VOTING SYSTEM:

In this paper, we have a tendency to propose client/server web-enabled e-Voting software design. The architecture is illustrated in Figures 2a and 2b shown right across. Besides the most practical properties of a voting system, as described in the previous section, the eVoting system must cater for several essential non-functional requirements. Of utmost importance are the necessities for correctness, robustness, coherence, consistency, and security.

On the server aspect, a world information is maintained for all registered voters and candidates. Also, the server runs in real-time and provides backend statistics for the complete election method. On the consumer aspect, two more requirements are necessary.

In order to scale back the traffic rate on the network links, a local database at the client side is required to host the data which pertains to the local voting center. This db may be a rather dynamic one, within the sense that the information stored in its tables could vary over the election period of time. The size of the native db at any voting center is just alittle fraction of the worldwide db at the server aspect. The use of a local db enhances the performance of the voting method. However, this approach creates a synchronization downside, which will be addressed later in this section.

The second demand is that the transparency of the voting method. In essence, a voter at an electronic voting station casts his/her vote to a pc. The voter doesn't have AN insight on however his/her vote is translated and/or counted. In a paper-based election, the ballot is stuffed out by the voter and born into a sealed box by the voter himself/herself. Votes are counted in the presence of candidates or their representatives. The voter is for certain that his/her cast ballot with his/her vote choice is within the right box. Of course, ambiguity within the ballot formats (as was the case within the USA presidential election in 2000) could render the transparency a rather deceiving one. In AN electronic version, the voter puts his trust into computer hardware, software and network infrastructure that processes his/her vote. Hence, the e-Voting system in its broadest kind could render the method a non-transparent one.

We propose a two-sided answer to the transparency problem. On the one aspect, the system prints a hardcopy of the vote cast by the voter. The voter verifies the accuracy of his/her vote and retains the copy for his/her records. On the opposite aspect, the system generates another copy of the vote with a new unique key identifier; the name and identity of the voter is concealed. This copy is saved in a very secure box and might be used later to verify the correctness of the votes as hold on within the final db destination. This aspect of the copy are often written out as a bar code which may be simply scanned and read automatically. Only a at random selected set of those copies got to be tested. This 2 sided method guarantees transparency by providing verification of the accuracy of however the cast vote is input into the system then however it's, finally, stored in the DB tables.

One of the challenges facing an e-Voting system is to insure that no voter can impersonate another voter and no voter can vote more than one time. In the proposed system, we use an identification followed by an authentication process. The identification is done via a card reader which reads the official ID card of a voter and pulls the voter record from the local DB or loads the record from the central DB if it is not found in the local one. The voter record includes a biometric description of the voter. In this study, we use a fingerprint authentication method. The voter will be rejected if his/her fingerprints do not match the stored ones. In order to reduce false rejections, we store for each voter several copies of his/her fingerprints taken at different time intervals. Fingerprints are stored as an encoded text in order to reduce storage consumed by images. This dual process should guarantee that no one can falsely impersonate a voter. In order to prevent two or more votes per voter, we use a “voting status flag” in the voter record. This flag is initialized to FALSE. The voting status flag is set to TRUE in the central DB whenever a voter identity is verified (before authentication takes place). If the authentication fails, the flag is reset to FALSE. If the voter leaves the station without completing a vote, the flag is also reset to FALSE; thus allowing the voter another chance to again to cast his/her vote. If the voter completes the voting process, the flag remains set to TRUE.

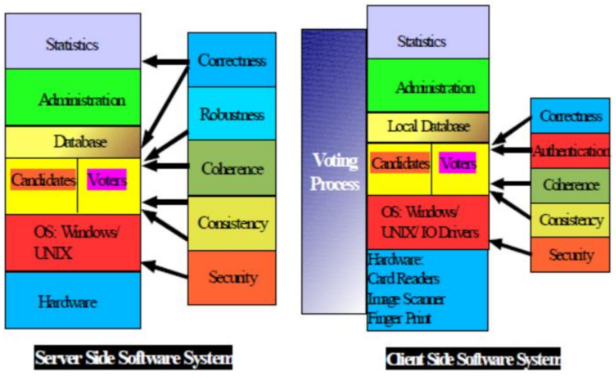

Figure 2: a) Server b) Client

Note that although the results of the vote isn't committed to the central db in due time, the flag within the voter’s central record is set to TRUE, thus eliminating the likelihood of another tried voting by the same voter, or by somebody who carries a counterfeit ID card. This requires that whenever the record of a elector is accessed for identification, even once the record is found at the native db, the flag on the central record must be checked. If it's already been set to TRUE, the voter is denied access and his/her attempt fails. If 2 individuals carrying a similar ID card (one is real whereas the opposite is counterfeit) commit to vote at a similar time, the first one to access the record will set the flag to TRUE, load the record and prevent the opposite one from accessing the record. Of course if the one with the counterfeit card obtains the record, the vote cast will fail at the next authentication step. It is attainable that a record gets loaded into 2 completely different voting centers thanks to block transfer from the central db into native DB’s. When a voter tries to access the record at any of the stations, the client will verify the central record flag. If it's been set to TRUE, access is denied; otherwise it sets the flag to TRUE and access is granted. Note that cooccurring requests to constant record are going to be synchronous by the db query serialisation method (only one query could access any table at any give time). This necessary check of the flag within the central db, however, can add additional overhead on the network. This overhead are more evaluated within the simulator, however won't be reported during this study due to time and area constraints.

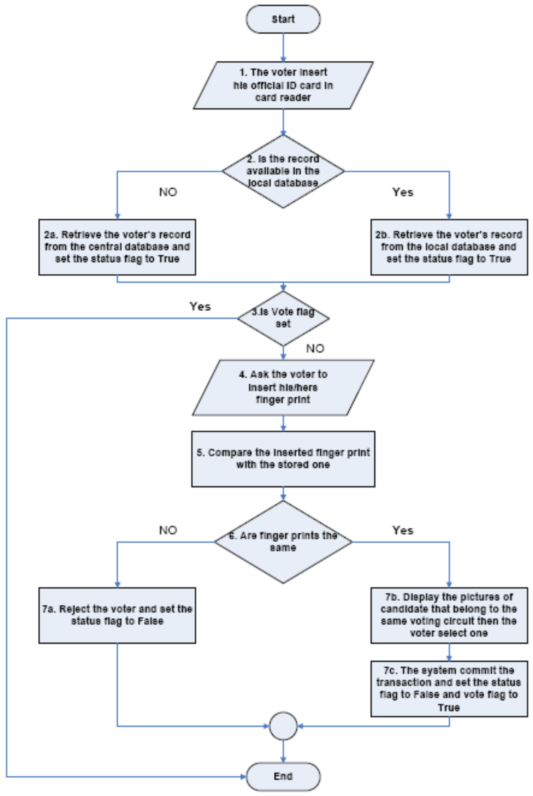
Start
1. The voter insert his official ID card in card reader
2. Is the record available in the local database
NO
Yes
2a. Retrieve the voter's record from the central database and set the status flag to True
2b. Retrieve the voter's record from the local database and set the status flag to True
Yes
3.Is Vote flag set
NO
4. Ask the voter to insert his/hers finger print
5. Compare the inserted finger print with the stored one
NO
6. Are finger prints the same
Yes
7a. Reject the voter and set the status flag to False
7b. Display the pictures of candidate that belong to the same voting circuit then the voter select one
7c. The system commit the transaction and set the status flag to False and vote flag to True
End

Figure 3- Voting Process Flow Chart

Another synchronization resolution is needed when a vote is to be registered within the record of a candidate. If a candidate is being selected by several voters at the same time, then a certain assignment plan needs to be placed in order so that all votes will be tallied (no misses) and added to the candidate’s record. Again we use a “count” flag/mutex for the candidate’s record. The COUNT flag is set initially to FALSE. When the record is selected by a voter, the flag is set to TRUE until the record count is updated, then the flag is reset to FALSE. All votes for an equivalent candidate are queued till the flag is reset to FALSE. A copy of the vote are printed only if the vote is successful and therefore the candidate’s record is updated. This requirement, initially made for transparency purposes, provides a final test for the accuracy and correctness of the process, especially in the presence of thread hang-ups. The correctness and accuracy of the system victimization the 2 flag attributes is demonstrated (physically present) within the current simulation study. When the flags were turned OFF, we noticed several violations and accuracy problems. Those were remedied when the flags' attributes were turned ON.

The voting method, as discussed above, is shown in the flow diagram of Figure 3. The overall design of the system is shown in Figure 4. The central database, Figure 4, which is mirrored out for reliability reasons, is used to store all relevant information on the candidates and voters. oting centers are distributed around the country. One or additional voting centers may share a local database. At a voting center, each voting station is equipped with a card reader, a fingerprint scanner, a touch screen, and a multimedia subsystem. The multimedia subsystem is used for people with special needs (physically challenged), such as the blind and those with difficulties in reading or comprehending images, texts, or sounds. The planned system is capable of handling electronic ballots with multiple scopes at an equivalent time, e.g. presidential, municipal, parliamentary, and others. However, the simulation environment in this study is designed only for a single voting scope.

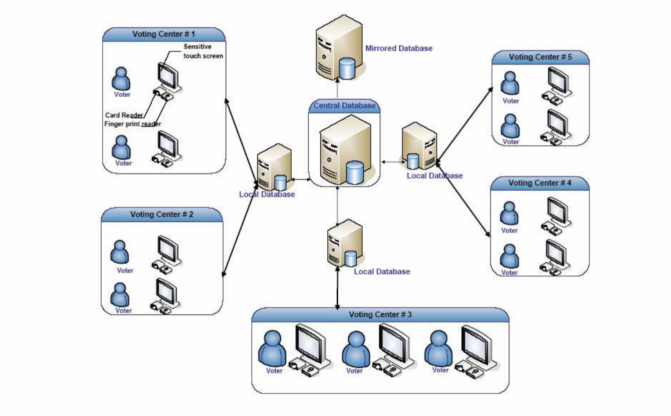

Figure 4- General schematic diagram

## III. *FINGERPRINT RECOGNITION*

Fingerprint recognition or fingerprint authentication refers to the automated method of verifying a match between two human fingerprints. Fingerprints are one of many forms of biometrics used to identify individuals and verify their identity. A fingerprint looks at the patterns found on a fingertip. There are a variety of approaches to fingerprint verification. Some emulate the traditional police method of matching pattern; others use straight minutiae matching devices and still others are a bit more unique, including things like moiré fringe patterns and ultrasonic. A greater variety of fingerprint devices are available than for any other biometric. Fingerprint verification may be a good choice for in e-voting systems, where you can give users adequate explanation and training, and where the system operates in a controlled environment. It is not surprising that the work-station access application area seems to be based almost exclusively on fingerprints, due to the relatively low cost, small size, and ease of integration of fingerprint authentication devices that will be implemented is shown in Fig 5.

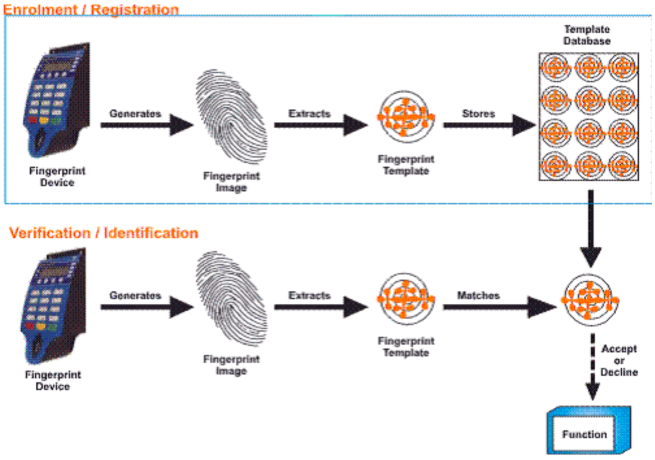

Fig. 5. Finger Print Enroiment and Verification

## IV. REFERENCES

[1] ANKIT ANAND1 , PALLAVI DIVYA2 ,AN E_CIENT ONLINE VOTING SYSTEM, VOL. 2,ISSUE.4, JULY-AUG. 2012, PP-2631-2634.

[2] ALAGUVEL.R1,GNANAVEL.G2,JAGADHAMBAL.K3, BIOMETRICS USING ELECTRONIC VOTING SYSTEM WITH EMBEDDED SECURITY, VOL. 2,ISSUE 3,MARCH 2013.

[3] FIRAS I. HAZZAA1,SEIFEDINE KADRY2,OUSSAMA KASSEM ZEIN3, WEB-BASED VOTING SYSTEM USING FINGERPRINT: DESIGN AND IMPLEMENTATION, VOL. 2, ISSUE.4,DEC 2012.

[4] MALWADE NIKITA1, PATIL CHETAN2, CHAVAN SURUCHI3, PROF. RAUT S. Y4, SECURE ONLINE VOTING SYSTEM PROPOSED BY BIOMETRICS AND STEGANOGRAPHY, VOL. 3, ISSUE 5, MAY 2013.

[5] ANKIT ANAND1 , PALLAVI DIVYA2 ,AN E_CIENT ONLINE VOTING SYSTEM, VOL. 2,ISSUE.4, JULY-AUG. 2012, PP-2631-2634.

[6] ALAGUVEL.R1,GNANAVEL.G2,JAGADHAMBAL.K3, BIOMETRICS USING ELECTRONIC VOTING SYSTEM WITH EMBEDDED SECURITY, VOL. 2,ISSUE. 3,MARCH 2013.

[7] FIRAS I. HAZZAA1,SEIFEDINE KADRY2,OUSSAMA KASSEM ZEIN3, WEB-BASED VOTING SYSTEM USING : DESIGN AND IMPLEMENTATION, VOL. 2, ISSUE.4,DEC 2012.

[8] MALWADE NIKITA1, PATIL CHETAN2, CHAVAN SURUCHI3, PROF. RAUT S. Y4, SECURE ONLINE VOTING SYSTEM PROPOSED BY BIOMETRICS AND STEGANOGRAPHY, VOL. 3, ISSUE 5, MAY 2013