Global Journal of Computer Science and Technology
Volume 12 Issue 5 Version 1.0 March 2012
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Security Enhancement of E-Voting System

By Sanjay Kumar & Manpreet Singh
M. M. University, Ambala

Abstract - The term E-Voting is used in variety of different ways and it encompasses all voting techniques involving electronic voting equipments, voting over the internet, using electronic booths in polling stations and sometimes even counting of paper ballots. A voting system that can be proven correct has many concerns. The basic reasons for a government to use electronic systems are to increase election activities and to reduce the election expenses. Still there is some scope of work in electronic voting system in terms of checking the authenticity of voters and securing electronic voting machine from miscreants. Biometrics is automated tool for verifying the identity of a person based on a physiological or behavioral characteristic. It has the capability to reliably distinguish between an authorized person and an imposter. Since biometric characteristics are distinctive, can not be forgotten or lost and the person to be authenticated needs to be physically present at the point of identification, biometrics is inherently more reliable and more capable than traditional knowledge-based and token-based techniques. In this paper, we have proposed a model to enhance the security of electronic voting system by incorporating fast and accurate biometric technique to prevent an unauthorized person to vote.

Keywords : *E-Voting, Biometric, Fingerprint Recognition.*

GJCST Classification: *K.4.0*

Strictly as per the compliance and regulations of:

Security Enhancement of E-Voting System

Sanjay Kumar [α] & Manpreet Singh [σ]

Abstract - The term "E-Voting" is used in variety of different ways and it encompasses all voting techniques involving electronic voting equipments, voting over the internet, using electronic booths in polling stations and sometimes even counting of paper ballots. A voting system that can be proven correct has many concerns. The basic reasons for a government to use electronic systems are to increase election activities and to reduce the election expenses. Still there is some scope of work in electronic voting system in terms of checking the authenticity of voters and securing electronic voting machine from miscreants. Biometrics is automated tool for verifying the identity of a person based on a physiological or behavioral characteristic. It has the capability to reliably distinguish between an authorized person and an imposter. Since biometric characteristics are distinctive, can not be forgotten or lost and the person to be authenticated needs to be physically present at the point of identification, biometrics is inherently more reliable and more capable than traditional knowledge-based and token-based techniques. In this paper, we have proposed a model to enhance the security of electronic voting system by incorporating fast and accurate biometric technique to prevent an unauthorized person to vote.

Keywords : *E-Voting, Biometric, Fingerprint Recognition.*

I. Introduction

Electronic Voting Machine (EVM) is a simple electronic device used to record votes in place of ballot papers and boxes which were used earlier in conventional voting system. It is a simple machine that can be operated easily by both the polling personnel and the voters. Being a standalone machine without any network connectivity, nobody can interfere with its programming and manipulate the results. Advantages of EVM [1] over the traditional ballot paper/ box system are:

- It eliminates the possibility of invalid and doubtful votes which, in many cases, are the root causes of controversies and election petitions.
- It makes the process of counting of votes much faster than the conventional system.
- It reduces to a great extent the quantity of paper used thus saving a large number of trees making the process eco-friendly.
- It reduces cost of printing almost nil as only one sheet of ballot paper is required for each polling.

II. Present Voting System

Voting is the bridge between the governed and government. The last few years have brought a renewed focus onto the technology used in the voting process and a hunt for voting machines. Computerized voting systems bring improved usability and cost benefits but suffer from weak software which has lot of bugs. When scrutinized, current voting systems have security holes and it becomes difficult to prove even simple security properties about them. A voting system that can be proven correct would solve many problems.

High security is essential to elections. There has been a lot of attention to an electronic voting by cryptographers. Many scientific researches have been done in order to achieve security, privacy and correctness in electronic voting systems by improving cryptographic protocols of e-voting systems. Currently, the practical security in e-voting systems is more important than the use of cryptographic schemes [2]. One of the main interests is seemingly contradicting security properties. On one hand, voting must be private and the votes should be anonymous. On the other hand, voters must be identified in order to guarantee that only the eligible voters are capable to vote. Hence, e-voting should be uniform, confidential, secure and verifiable. The most important requirements for e-voting can be characterized as:

- Eligible voter is authenticated by his/her unique characteristics.
- Eligible voters are not allowed to cast more than one vote.
- Votes are secret.
- Auditors can check whether all correct cast ballots participated in the computation of the final tally.
- Result of election should be secret until the end of an election.
- While voting is on, there should not be a method of knowing intermediate result that can affect the remaining voter's decisions.
- All valid votes must be counted correctly and the system outputs the final tally.
- It must be possible to repeat the computation of the final tally.

The following three dimensions are used to make a comparison of electronic voting systems for various nations [6]:

- Whether a country's system uses a paper audit trail.
- Whether the system permits an anonymous, blank or spoiled ballot.
- Whether the software is open source or proprietary.

III. Proposed E-Voting System

We have proposed a model for e-voting based on biometric technique. Biometrics has been widely used in various applications such as criminal

identification, prison security electronic banking, e-commerce [3]. Biometric authentication requires comparing a registered or enrolled biometric sample (biometric template or identifier) against a newly captured biometric sample (for example, a fingerprint captured during a login). During enrollment, a sample of the biometric trait is captured, processed by a computer and stored for later comparison. Biometric recognition can be used in identification mode, where the biometric system identifies a person from the entire enrolled population by searching a database for a match based solely on the biometric. A system can also be used in verification mode, where the biometric system authenticates a person's claimed identity from their previously enrolled pattern. This is also called "one-to-one" matching [4]. The proposed model uses biometrics in the verification mode during e-voting. Implication of error rates of different biometric techniques based on False Reject Rate (FRR) and False Acceptance Rate (FAR), we can conclude that the finger print recognition is that fast and accurate biometric technique required for making reliable and secure system [7].

The patterns of friction ridges and valleys on an individual's fingertips are unique to that individual. For decades, law enforcement has been classifying and determining identity by matching key points of ridge endings and bifurcations. Fingerprints are unique for each finger of a person including identical twins. One of the most commercially available biometric technologies, fingerprint recognition devices for desktop and laptop access are now widely available, users no longer need to type passwords – instead, only a touch provides instant access. Fingerprint systems can also be used in identification mode. Several states check fingerprints for new applicants to social services benefits in order to ensure that recipients do not fraudulently obtain benefits under fake names [5]. Fingerprints are the ridge and furrow patterns shown in Figure 1 on the tip of the finger and have been used extensively for personal identification of people. The availability of cheap and compact solid state scanners as well as robust fingerprint matchers are two important factors in the popularity of fingerprint-based identification systems

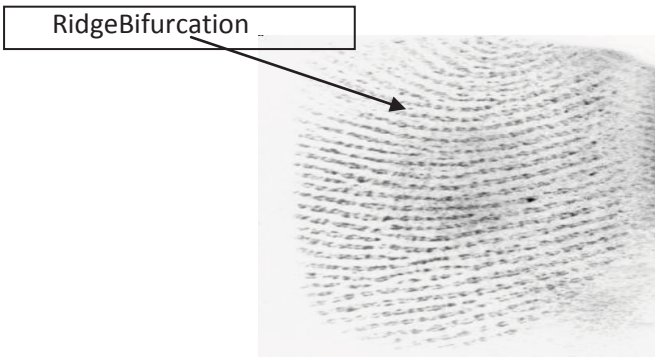

Fig.1. Ridges and Furrows

The proposed model assumes that the unique id has been assigned to each voter (Citizen of India). Each perspective voter must have a unique fingerprint registered in the database. The proposed model comprises of following steps:

Step-1: Open login window.

Step-2 : Enter P.O.id and password. /* id and password filled by Presiding Officer(P.O.) */

Step-3 : If P.O. id and password verifies

Main window /* main window will appear automatically */

Else

Print- wrong id and password

Go to step 2

Step-4: Enter user id and password. /* for voter, if the system has been successfully started by P.O. */

count=0;

Step-5 : Verify userid and password

If user id and password matches

If votedflag=false

Print- enter thumb impression

count++

If thumb impression valid

go to step 6

Else

Print-This time your thumb impression didn't match

Go to Block 1

Else

Print- you have already voted

Go to step 7

Else

Print Userid and password don't match

Go to step 7

Block 1 Print (chances left, "3-count")

If(count <=3)

Go to step 5

Print- You are not authorized

Go to step 7

Step-6 : Print- please enter your vote

Set votedflag = true

Print-thank you

Step-7 : Check current time (It should be less than closing time 05:00PM.)

If (current time < 05:00 PM)

Go to step 4 /* another user can vote*/

Else

Go to step 8

/*After 5:00 PM, no person is eligible to restart the system for voting procedure.*/

Step-8 : Exit

IV. Implementation

This proposed model has been simulated successfully on Java platform. Figure 2 to Figure 5 are

few snapshots of steps involved in the implementation of proposed model.

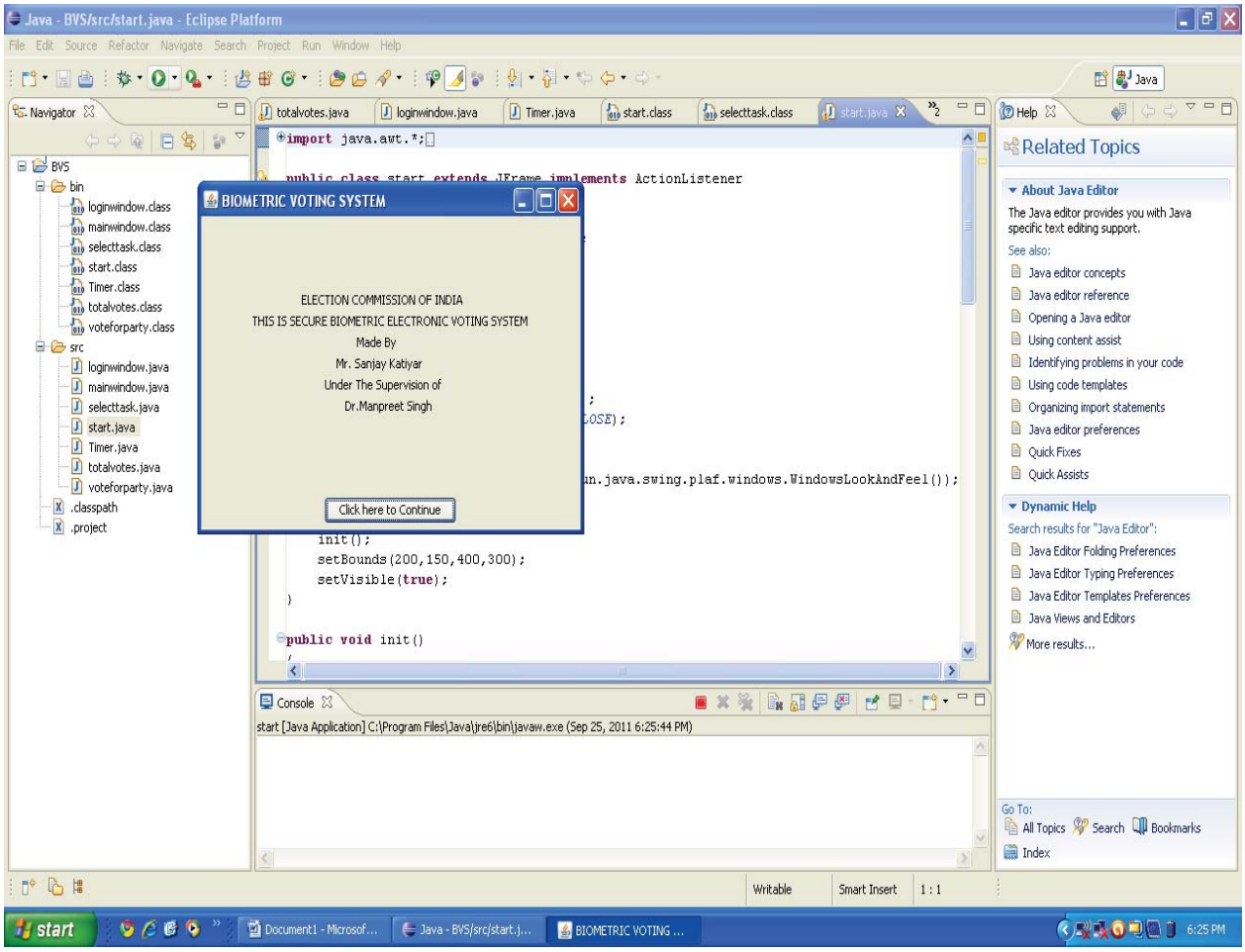

Fig.2. Home Page of Biometric Electronic Voting System

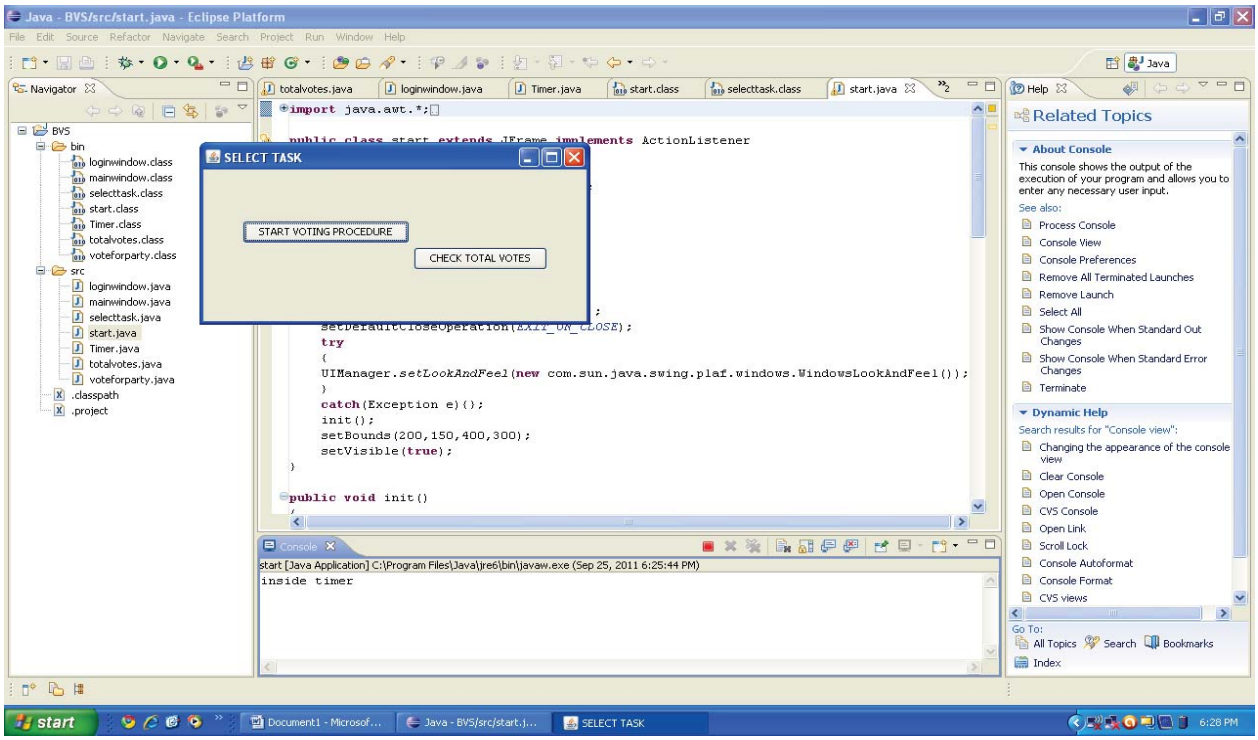

Fig.3 Login Window of Presiding Officer

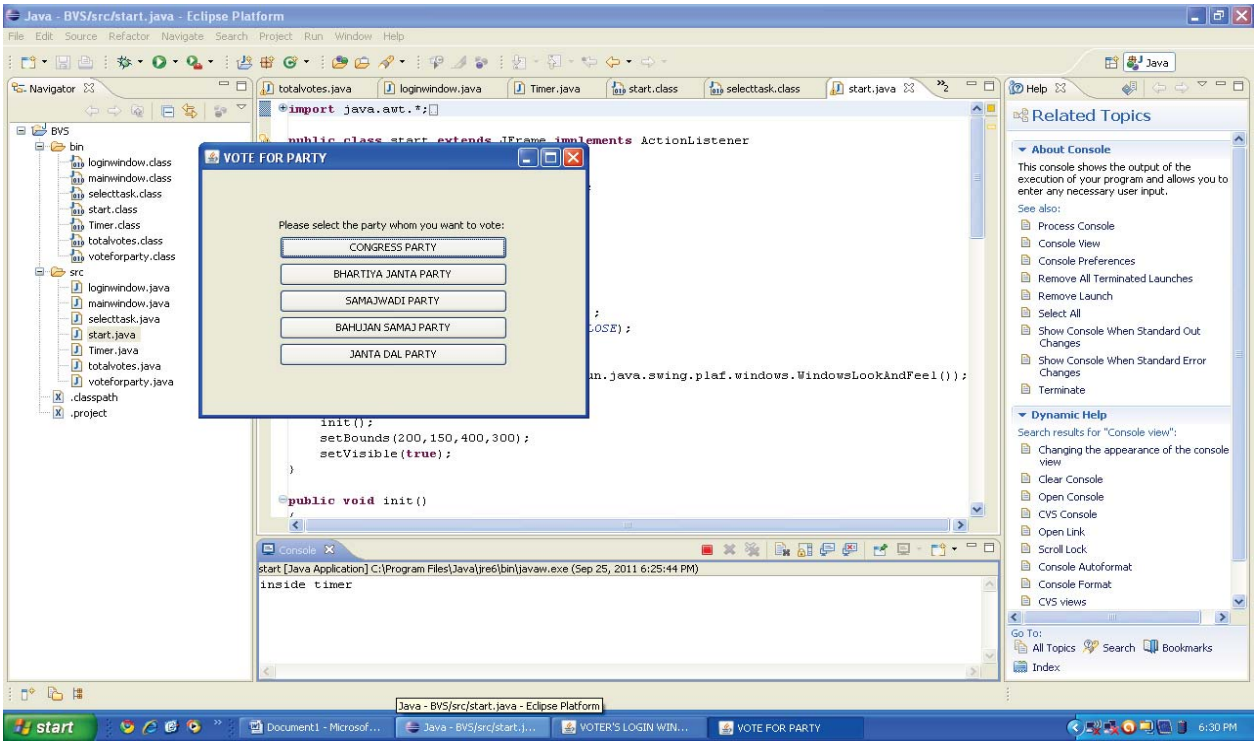

Fig.4. Voting Procedure

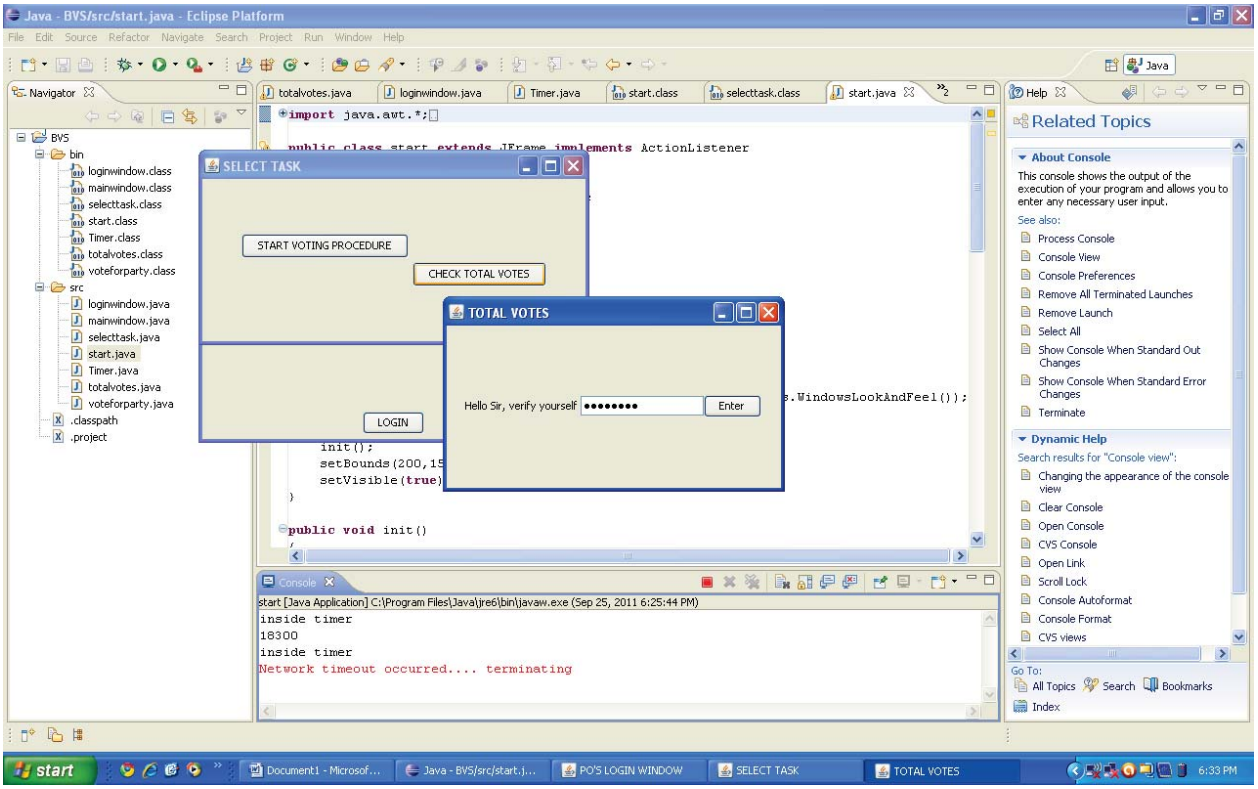

Fig.5. Vote Counting

We have implemented the proposed model by integrating it with FTA 5454(A10) - Fingerprint Time and Attendance system as shown in Figure 6. It can store 3000 fingerprint templates and 50000 transaction records.

Fig.6. Device used for Fingerprint Recognition

V. Conclusion

We have presented a model for electronic voting wherein fingerprint is embedded as biometrics for voter identification. The future work will concentrate on implementation of fast and accurate fingerprint recognition and other related technical aspects in the system.

References Références Referencias

1. Everett, S., Greene, K., Byrne, M., Wallach, D., Derr, K., Sandler, D., Torous, T. (2008). Electronic voting machines versus traditional methods: improved preference, similar performance. Proceeding of 26th Annual SIGCHI Conference on Human Factors in Computing Systems, Florence, Italy, April 5-10, 2008, 883-892.
2. Ansper, A., Buldas, A., Oruaas, M., Piirsalu, J., Veldre, A., Willemson, J., Kivinurm, K. (2002). The Security of Conception of E-Voting: Analysis and Measures. Technical Report by National Electoral Committee.
3. Phillips, P., Martin, A., Wilson, C., Przybocki, M. (2000). An Introduction to Evaluating Biometric Systems. IEEE Computer, 33(2), 56-63.
4. Zebbiche, K., Khelifi, F., Bouridane, A. (2008). An Efficient Watermarking Technique for the Protection of Fingerprint Images. EURASIP Journal on Information Security, 2(1), 1-20.
5. Carrigan, Robert, Milton, Ron, Morrow, Dan (2005). "Automated fingerprint identification systems", Computer World Honors Case Study, 1-5.
6. Kumar, Sanjay, Walia, Ekta (2011). Analysis of Electronic Voting system in Various Countries. International Journal on Computer Science and Engineering, 3(5), 1825-1830.
7. Kumar, Sanjay, Walia, Ekta (2011). Analysis of various Biometric Techniques. International Journal of Computer Science and Information Technologies, 2(4), 1595-1597.

This page is intentionally left blank