World Academy of Science, Engineering and Technology
International Journal of Humanities and Social Sciences
Vol:6, No:8, 2012

E-Voting: A Trustworthiness In Democratic; A View from Technology, Political and Social Issue

Sera Syarmila Sameon and Rohaini Ramli

Abstract**—**A trustworthy voting process in democratic is important that each vote is recorded with accuracy and impartiality. The accuracy and impartiality are tallied in high rate with biometric system. One of the sign is a fingerprint. Fingerprint recognition is still a challenging problem, because of the distortions among the different impression of the same finger. Because of the trustworthy of biometric voting technologies, it may give a great effect on numbers of voter's participation and outcomes of the democratic process. Hence in this study, the authors are interested in designing and analyzing the Electronic Voting System and the participation of the users. The system is based on the fingerprint minutiae with the addition of person ID number. This is in order to enhance the accuracy and speed of the voting process. The new design is analyzed by conducting pilot election among a class of students for selecting their representative.

Keywords**—**Biometric, FAR and FRR, democratic, voting

I. Introduction

THE biometric voting can be considered as a convenience and secure method to avoid fraud occurring during election period. Besides that it creates a more systematic and organized election system. Therefore it can be said saving cost, time and energy. Biometric is the science that captures and analyzes human biological features with a particular device either to authentication or identification. The most commonly use biometric features is the finger print [4]. In contrast to pin codes, biometric features change over time. This is probably the most challenging property of the biometric system. One has to find a balance between a check which is too strict and generates too many rejections, and a check which is too loose and generates too many false accepts. There are two main motivations to introduce e-Voting: cost savings and increased voter participation and interest. Providing information and increasing the convenience for the citizens goes hand in hand, and it also offers disabled people the possibility to use e-Voting systems [5].

II. Impact of E-Voting To Society

Technological determinism is the theory that a developing technology will have social consequences either good or bad impacts [3].

Technology developed by the experts is according to their functional properties. In this point of view, the users of these new systems feature mainly as passive victims and society is shaped by technology.

The ways in which the boundary between 'social' and 'technical' processes or artifacts is negotiated should be examined, rather than accepting it as 'given' or taken for granted [6]. The design of the technology should be a democratic process. Hence, the technology is socially shaped or constructed by its users, not the other way around. The new voting technologies, beside the reflection of the technical aspect, it also has to consider the political, social, and organizational modalities of the systems introduced. In traditional voting procedures people are used to those media, and have to trust the procedures. With the introduction of new media in voting, this changes. With electronic voting systems, public confidence in the election relies on trust in technical experts instead of a transparent process [8].

III. Issues with Biometric System

There are two basic types of recognition errors; the False Accept Rate (FAR) and the False Reject Rate (FRR) [9]. A False Accept is when a no matching pair of biometric data is wrongly accepted as a match by the system. A False Reject is when a matching pair of biometric data is wrongly rejected by the system. The two errors are complementary: If one of the errors tried to be lower by varying the threshold, the other error rate automatically increases. There is therefore a balance to be found, with a decision threshold that can be specified to either reduce the risk of FAR, or to reduce the risk of FRR [2]. In a biometric authentication system, the relative false accept and false reject rates can be set by choosing a particular operating point (threshold). Very low (close to zero) error rates for both errors (FAR and FRR) at the same time are not possible [1]. By setting a high threshold, the FAR error can be close to zero, and similarly by setting a significantly low threshold, the FRR rate can be close to zero. A meaningful operating point for the threshold is decided based on the application requirements, and the FAR versus FRR error rates at that operating point may be quite different. To provide high security, biometric systems operate at a low FAR instead of the commonly recommended equal error rate (EER) operating point where FAR = FRR.

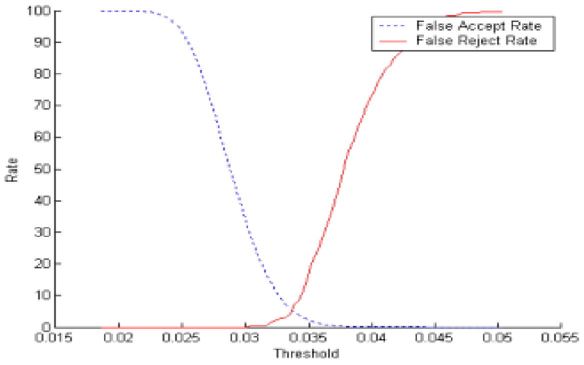

Fig. 1 FAR and FRR Graph (Extract from www.bioperf.googlecode.com/files/BioPerf%20Manual.pdf)

Sera Syarmila Sameon is with College of Information Technology, Universiti Tenaga Nasional, 43009 Kajang, Selangor, Malaysia (phone: 603-8921 2344; fax: 603-8928 7166; e-mail: sera@uniten.edu.my).

Rohaini Ramli is with College of Information Technology, Universiti Tenaga Nasional, 43009 Kajang, Selangor, Malaysia (phone: 603-8921 2343; fax: 603-8928 7166; e-mail: rohaini@uniten.edu.my).

IV. Biometric Voting System

It's now appreciated that a biometric voting system has been presented that facilitates both the enumeration and voting process. Enumeration is the process of data gathering to produce a clean and reliable voter list. A potential voter is electronically identified by reading, authorizing and matching his/her fingerprint against all other fingerprint stored in database for registration purpose [7]. Additional electronic identification can be accomplished by running through name, address and picture of the voter. The fingerprint and additional data is used to identify certified voters and to identify duplicate registration in order to produce a clean database and voters list to be subsequently used for identification purposes and for voting.

V.The Architecture Of The System

Fig. 2 below shows how the main host and the database connected to phone networks via GSM modem. The function of this feature is to send notifications of updates on voting status to all registered students. To achieve this, a SMS web application that act as a server will send SMS in bulk via the SMS Gateway API from the system database to the student's mobile phone.

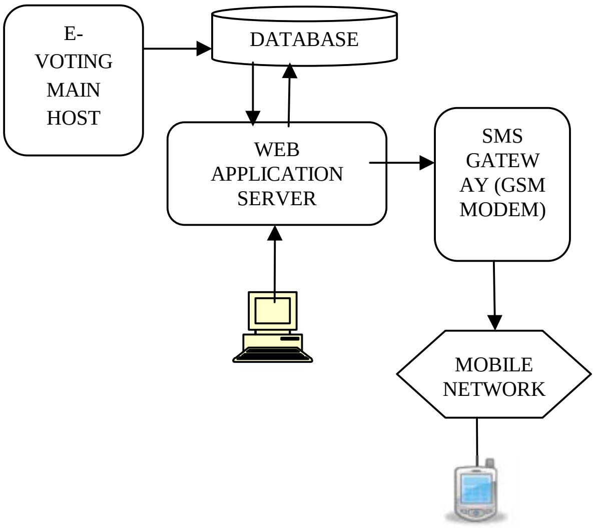

Fig. 2 The architecture of the system

VI. Design

As a pre-poll procedure, students are required to register to the voting system in order to have a certified account as a voter thru the system. A database consisting of the fingerprint impressions and their personal details (including NRIC) of all the certified voters is created. To verify the voters to allow voting during Election Day, persons listed in the database at the time of voting will touch their NRIC card to the scanner and possess their finger prints electronically (at the scanner) checked against that stored in the database.

Once a person is positively identified as being part of the database, the voting system enables that person to access the voting system using his fingerprint. This process can be shown by flowchart as in Fig. 3a. The reason why the person needs to touch the NRIC card is to control the sensitivity of the system toward the lowest FAR. With the help of NRIC number, the system will first check the match number and then their finger print that have been stored in database. Having these features it will enhance the accuracy and speed of the process. Besides that, the FRR will be maintaining at possible rate. The voter then chooses the candidate party of choice that appears in listing format on the screen. Fig. 3b show how the process flows. They now cast the votes for that choice by clicking the candidate party and once again verify the finger print. If the finger print is accessible then the data of the specified candidate is taken into account. The voter's thumb impression is verified with the previously cast votes. If there is no match then the vote is accepted and the count is increased by one. If the vote matches with any of the previous votes then the vote is rejected. The voting information is recorded at the voting station and transmitted simultaneously for storage at the main host. At this time, the voter's database becomes inaccessible throughout the voting system to prevent duplicate voting. The voter then will get a receipt acknowledging that the vote has been recorded. The voter also can select different campaign that being run on the same day.

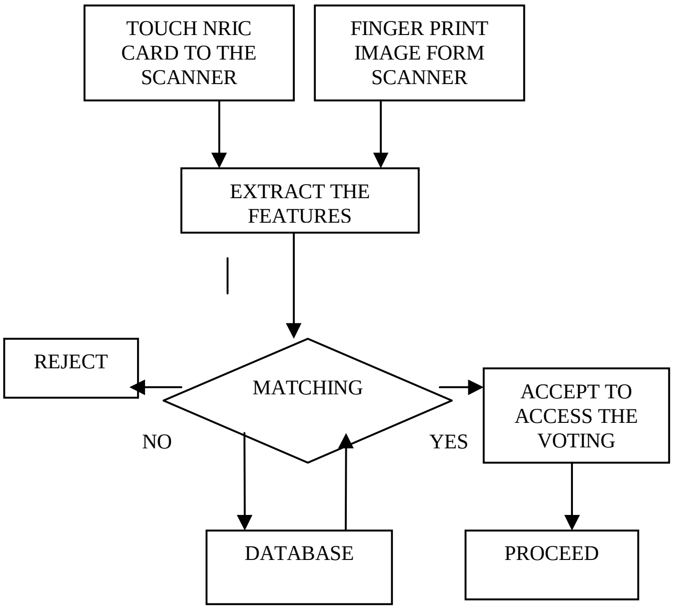

Fig. 3(a) Finger print verification process

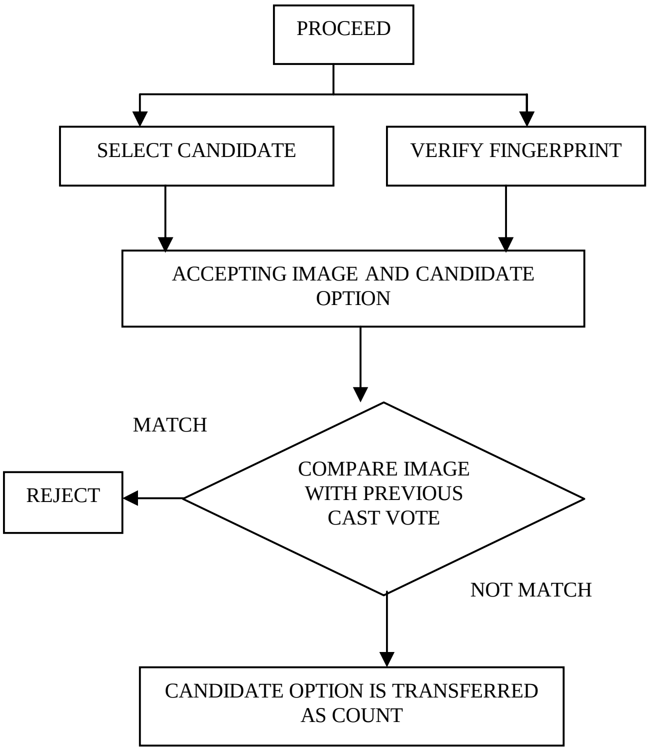
PROCEED
SELECT CANDIDATE
VERIFY FINGERPRINT
ACCEPTING IMAGE AND CANDIDATE OPTION
MATCH
REJECT
COMPARE IMAGE WITH PREVIOUS CAST VOTE
NOT MATCH
CANDIDATE OPTION IS TRANSFERRED AS COUNT

Fig. 3(b) Casts Vote Process

At the end of voting, the system can provide the count of votes for each candidate, the total votes cast, and the names of all persons who voted. All the data collected in the voting system is first stored in the voting machine itself before it is sent to the main host through local network. The voters can view the status of the candidate in the web based application. This is achieved by connecting the database of the system to the web based server. The updated data also will be announced directly to the voters via SMS. This function is applicable to the voters that registered with phone number including. It also offers a service to send a reminder to the student that yet to vote. The application is done by setting up the GSM setting; COM port, baud rate, data bit, stop bit and flow control at the main host. By clicking the connect button, it is then connected to the SMS gateway (GSM Modem).

VII. Experimental Results

We have conducted the Pilot Election with three RFID and fingerprint scanners for selecting class representative. For that, we have created the database which consists of the fingerprint of 30 students (15 males and 15 females) from College of IT. It will subsequently match the scanned fingerprint against the stored template. All details including mobile number of these 30 students are stored in database. The system is programmed to recognize a fingerprint twice. Upon verification, they will have the access to vote for their desired candidates. Mismatched fingerprint certainly would indicate denial from the access. During the voting, the voter first touches their NRIC number and places his/her thumb on the scanner.

If the number and fingerprint matches with the one stored in database he/she is allowed to vote. They now cast the votes for that choice by clicking the candidate party and once again verify the finger print. In case the print is not stored before, or if the same person votes again, the system would reject the vote. There are four candidates for the representative selection. Student is asked to vote for the candidates. Table I below shows the pilot election results.

TABLE I
Pilot Election Result

Name of the Candidate	Count of the Votes Polled
Alicia Lee	5
Ghobirajah A/L Selva	9
Mohd Azni B Isa	10
Faisal Ali	6
Total Vote Cast	30

All 30 students then will receive the result of the election once the campaign is closed by admin. The result can be retrieved by web based (portal) or by SMS.

From the test, it can be observed that the time taken for the system to recognize and authenticate a person is much faster, when the NRIC number is also taken into account. This in because the system will check for both input; the NRIC number and the finger print. So then the number of FAR and FRR will be in acceptable rate. Without the number, the system will check the print alone, and a little error will either contribute to False Accept or False Reject. This mean the sensitivity of the Biometric system (in term of FAR and FRR) now is low by the help of matching case of NRIC number and finger print.

Beside of the technical aspect analysis, it also been observed that the respond from the student is overwhelming. All the 30 students and also the rest of students in the University need to fill in the survey form regarding their satisfaction and opinion of this type of election process. Most of them agreed with this technology that helps them to trust the election process compared to conventional ways. And from the feedback, the student also satisfied with the time that they need to spent during the process and received the status of the winner immediately (and directly to their phone) once the election is closed.

VIII.Conclusion and Future Direction

By the use of E-voting system, the student’s representative is elected in more systematic and organized, with better security compared to conventional way. This model uses fingerprint for the purpose of voter identification and authentication. As the fingerprint of every individual is unique, it helps in maximizing the accuracy. In this work, we focus on how to recognize the finger print twice. The second recognition during casts vote is important part.

If the finger print is accessible and no match from previously casts vote then the data of the specified candidate is taken into account. If the vote matches with any of the previous votes then the vote is rejected. At this time, the voter's database becomes inaccessible throughout the voting system to prevent duplicate voting. Another added feature is to announce the result thru SMS. Having this feature the voters will receive the result instantly. For future work, we will focus on implementation of fast and accurate fingerprint recognition. These include on how to enhance the captured image by various techniques to minimize or to remove the false minutiae. We also would focus on the behavioural of the voters toward the technology during implementing it.

REFERENCES

[1] Biometric Performance Display and Comparison Tool-Manual, Brian O' Mullane http://www.bioperf.googlecode.com/files/BioPerf%20Manual.pdf

[2] Biometric-solutions Website http://www.biometric-solutions.com/index.php?story=performance_biometrics.

[3] Dahlbom & Mathiassen, 1993: 196Dahlbom, B. and L. Mathiassen (1993), Computers in Context. The Philosophy and Practice of Systems Design. Oxford: Blackwell.

[4] Deutschland, G. Lassman, Bewertungskriterien zur Vergleichbarkeit biometrischer Verfahren, 2002, http://www.teletrust.de/down/kritkat_2-0.zip

[5] Equal access to electoral procedures, Good practice guidance, http://www.electoralcommission.gov.uk/files/dms/GoodPracticeequalaccessfinalversion_11561-9041__E__N__S__W__.pdf

[6] Green, Owen and Pain, 1993 Green, E., Owen, J. and D. Pain (1993), Gendered by design? Information Technology and Office Systems. London: Taylor and Francis.

[7] Hello-engineers Website http://hello-engineers.blogspot.com/2009/06/paper-presentation-biomtric-voting.htm

[8] IPI, 2001 Internet Policy Institute (2001) Report of the National Workshop on Internet Voting: Issues and Research Agenda. March 2001.

[9] Phodei Ibrahim Sheriff, 2011 www.thepatrioticvanguard.com/spip.php?article6212