# A BIOMETRIC WITH CRYPTOGRAPHY FOR REMOTE VOTING SYSTEM

**Shameem Sulthana E.S.[1], Kanmani S.[2]**

[1]Assistant Professor, AASC, Pondicherry, India. shammumunch@yahoo.com
[2]Professor & Head, PEC, Pondicherry, India. kanmani@pec.edu

## Abstract

Abstract – In this modern world everything is possible and fast. In this paper we propose a multifaceted online e-voting system. The proposed system is capable to manage through internet with multiple scopes and focus on using evidence for making access control decisions in present computing environments. To protect the election accuracy, it is necessary to have an accurate electoral roll of eligible voters. The main goal of this work is it supports a remote voter registration scheme that increases the accuracy of the current systems. In this scheme the voter identification is carried out by means of combining cryptographic and biometrics techniques. This work implements the evidence-based approach on web service and it creates an ecosystem in which evidence providers can flourish.

***Keywords:*** E-voting, Biometric System, Cryptography, Evidence, Security.

## I. INTRODUCTION

Voter registration is the process of collecting the voters' data in order to constitute an electoral roll. Most of the proposals have been focused in voting and tallying stages, giving least interest to voter registration stage. Voter registration is conventionally carried out face to face with the registration authority. Many voters are residing abroad during an election process, it has been necessary to have new methods to collect, remotely and in a secure manner, the information of such voters. As in most of the remote transactions, current remote voter registration systems face some security problems. These problems are mainly related to the inability to accurately verify the identity of the voter, which can facilitate impersonation or multiple registrations by the same voter with different data [1].

In this paper we propose a remote voter registration scheme, in which some biometric systems play an important role to protect the accuracy of the electoral roll. Biometric systems have already considered in electronic voting in the voting phase, e.g. [2, 3]. It is important to note that sometimes voter registration is related to the voter credential generation process. Some authors have made proposals about this subject [4, 5].

### *A Study on Current Remote Voter Registration Process*

In many countries like The United Kingdom [6] or United States [7] it is common to carry out remote voter registration. These methods allow the voter to fill out his or her own paper registration form remotely (e.g., at home) and return this form to the registration officers by using a delivery channel or optionally attending in person to a registration site. Any other alternative channels such as fax or e-mail (attaching a scanned copy of the filled form) [7]. Furthermore, there are countries [8] introducing the use of web interfaces to allow voters to fill out the registration form online, speeding up the remote acquisition of voter registration information. After sending the registration form, the identification of the voter is done by one or the combination of the following techniques: the verification of personal information of the voter and the verification of some physical characteristics of the voter.

### *Analyzing the problems in current Remote Voting System:*

To analyze the problem the first step consists of registration officers checking to see if the voter included in the form some personal information that it is also stored in the voter register. Some examples could be the date of 1 birth, the social security number or any other familiar information (e.g., mothers'mothers' maiden name, etc.). The problem with ith using such information for identifying the voter is that this information could be available in other databases (e.g., the member database of a socialsocial club) or could be known by people close to the voter.to the voter.

The second step consists of requiring verifying the identity of the based on checking some voter personal characterists, such as a handwriting signature stamped on the form or the face or fingerprint of the voter against an image or template contained contained

in some identity card or database. In anyany case, the accuracy of this second techniquetechnique of voter identification is based on the abilityability of the registration officers to validatevalidate the voter authentication data. The current remote voter registration methods do not check check if the same person has filled out more than a registration form by using the names of differendifferent valid voters.

*Problems Identified in Currenturrent Remote Voting Systems*

The contents of the registratio registration form can be altered after the voter has sent this form. The handwriting signature on the the form can be reused by an attacker to fill outout a different registration form. The problem identified inhandwriting signature, in fact, that it that it is not bound to the contents of the register. ThereTherefore, any change in the contents of the registratio registration form or the re-use of a valid handwriting signature in a different form cannot be detected tected by simply verifying the signature. So, therefore,therefore, the following problems may occur inin the current remote voting system.

- ❖ Accuracy to validate the voter identity;
- ❖ Prevention of multiple registers bregisters by voters;
- ❖ Integrity of voter registration infor on information.

To increase the accuracy of remote registration process, we propose the the combination of biometric systems and cryptographic functions. Below we analyze whichwhich are the improvements of adding both techniques in remote registration process.

## II. PROPOSED SYST

In our proposed systemsystem we have developed a web site using ASP.NE ASP.NET and in that we have given the registration option to the voter. The voter must fill up the registratioregistration form and they should upload the scanned scanned copy of the voter ID card and a photo along along with the registration form. After submittingsubmitting the registration form the voter status status will be send to the voter through e-mail. Then Then based on the given voter information the voter voter will be verified with Election Commission server. server. If it is true, then the voter will receive thethe Identity proof through e-mail which is generatedgenerated using cryptography techniques.

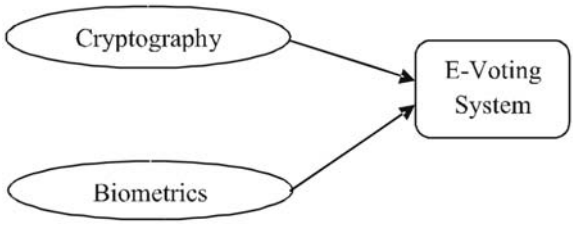


Fig. 1: E-voting System System

*Generating ID proof using Cryptographic System*

The integrity proof is repre represented in a format that can be legible by the voter, for instance, a base-32 notation [9]. Figure 1 shows the interaction between the voter and the Registration Module to carry outout the remote registration and get the integrity proof.

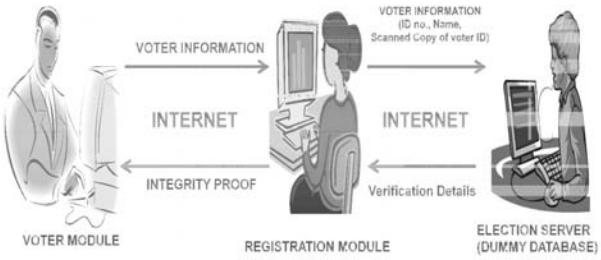


Fig. 2: Generating Identity proof

In order to get the integrity proof it is used as a combination of MD5 and SHA1 hash functions. The latest is used in its MAC implementation. This combination is conceived with the aim of preventing collisions between the digest messages, such as was found in the last years for MD5 [10,11,12,13] and for SHA1 [10,11]. The integrity proof generation is then as follows:

1. Get a digest k from thethe registration information Mi:

$$K = MD5\ [Mi]$$

2. Use k as a key to get a HMAC--SHA1 from the same registration information Mi: H = HMAC-SHA1 [Mi, KMi, K]The resultant H is the integrity pro proof. Using a combination of MD5 and HMAC-SHA1, the probability to have a collision decreases significantly. An attacker attacker needs to find a coincidence of collision for the the same text on both systems. In

addition, we are are reducing the probability of these collisions without ithout increasing the size of the digest that remains ns the same as a SHA1 (160 bits). Since *H* is based on an H sed on an HMACSHA1, it is 160 bits long, i.e. 21602160 different digests. Therefore, a base-32 notation notation (which is 25) allows a representation of SHA1 in 32 characters. These 32 characters can can be shown to the voter in six groups of five characters characters plus the two remaining ones. However, the integrity proof H can be truncated in orde order to give a higher usability. For example, taking taking only the first 20 characters, they can be shown in five groups of four characters or four groups of five characters, which is usable enough. ough.

### *2.2 Accuracy on Biometric Systeiometric System*

The voter registration system systems may use biometrics system. Registration modulemodule verifies some physical characteristics that uniquely identify the voter. In our proposeproposed system the biometric system is used to helphelp registration officers to improve the accuraaccuracy of voter identification. Biometric systems are electronic systems specialized on identifyingng a user by means of processing unique physiological physiological or behavioral characteristic of the user. user. Biometrics systems are classified based onon the unique characteristic of the user that is is used for the identification. In this proposal thethe biometrics characteristics will fulfill all the biometric requirements. In our analysis, we considered an additional requirement for remoteremote voter registration: the biometric systemsystem must be remotely available for most of the the voters. This reduces the number of potential candidates to face biometrics, since these allowallow biometric information to be acquired by means ofby means of capturing the face and compare it with the inte it with the integrity proof.

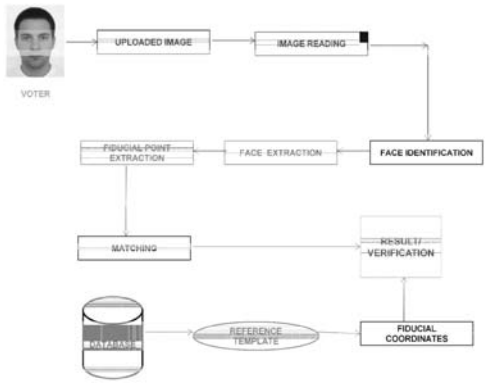


Fig. 3: Biometric System Design

Using pre-existing biometricbiometric systems comparative analysis [15, 1616] and taking fingerprint biometrics as reference, ence, the proposed biometrics systems fulfill thethe requirements. However, as we will explain in thethe definition of our proposal, fingerprints do not give any advantage over the current solution solutions on remote registration environment. The valuvalues for face have been obtained by using aa capturing and storing the images in database [17, 1817, 18].

This proposal system will will protects from alterations the contents of the voter voter registration information by binding such information to the voter identify. This is reached by means of combining biometrics and cryptographic techniques that do not require a public key infrastructure.

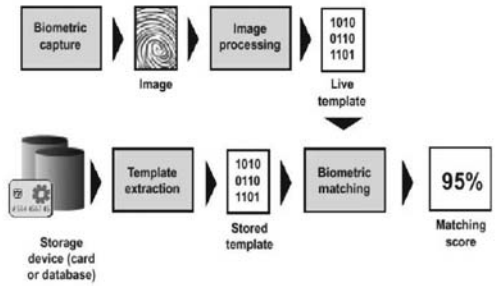


Fig 4. Accuracy on Biometrics

The proposed biometric system willwill provide the highest level of accuracy in remote voting system. That means a biometric metric characteristic that can give at the same time both authentication and integrity to the contents.

### *2.3 Generation and ValidationValidation of a Registration Proof*

Based on the previous analysis, analysis, we will use a face biometric system in this stage. The voter carries out a communicationcommunication with the Validation Module. This communication mmunication is done by means of Web cameral. Then Then the voter is asked to give the integrity proof. He or she types the proof previously shown by thethe Registration Module, i.e. the groups of characters that represent the integrity proof.

By doing this process, the the face of the voter is bound to the contents of thethe registration information. The registration prooff is then stored by the Validation Module. TheThe validation process

facilitates the detection of of people who attempt to create more than one record. Therefore, the probability of imperso impersonation is low in our proposed system. An additional validation consists on checking ecking the voter registration information against the associated registration proof. This check wwill consist of verifying if the integrity proofs fs match. That means, if the hash of the voter registration registration form has the same value as the one recor recorded as part of the registration proof.

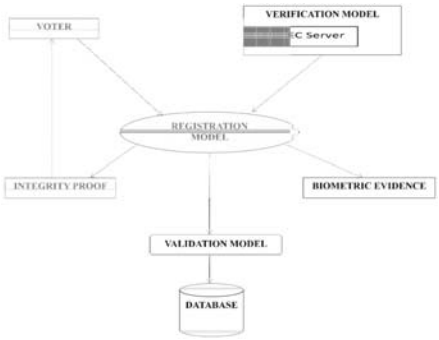


Fig 5. System Design

## III. CONCLUSIONSCONCLUSIONS

In this paper we proposed osed the use of biometrics systems to increase rease the voter identification accuracy of voters s that make a remote registration. Current remote voter registration systems have important ortant issues that can facilitate voter impersonation. nation. These issues are mainly voter identification accuracy, accuracy, multiple registrations from the same personperson and voter registration information integritintegrity. In our proposed system an identificatidentification context, biometrics systems can automate the the detection of multi registrations made by the same person. Finally, we identified and proposedproposed some biometrics methods, such as face biobiometrics that can also bind the registration infor information to the voter identity. Combining this later later feature with the use of cryptographic algorithms, such as hash functions, we also provided a way ay to protect the integrity of voter registration information that can be suitable to implement in current environment.

## REFERENCES

[1] Election Law Blog. The Extremely Extremely Weak Evidence of Voter Fraud in Crawford, the Indiana Voter ID Case. May, 2007 2007. Available at http://electionlawblog.org/archives/00 rg/archives/008378.html

[2] Victor Morales-Rocha1, Jordi Jordi Puiggalí1 and Miguel Soriano, Secure Remote Voter Registration -. Proceeding of 3rd international Conference on Electronic VotingVoting 2008, GI-Edition Lecture Notes in Informatics matics August 6th9th, 2008 in Castle Hofen, Bregenz, Bregenz, Austria. pg 95-108.

[3] Mohammed Khasawneh , Mohammad Malkawi , A Biometric-Secure e e-Voting System for Election Processes, ProceedingProceeding of the 5th International Symposium on MechatronicMechatronics and its Applications (ISMA08), Amman,Amman, Jordan, May 27-29, 2008.

[4] Krivoruchko, T: Robust Coercion Coercion-Resistant Registration for Remote E-Voting, ting, Proceedings of the IAVoSS Workshop onon Trustworthy Elections (WOTE 2007), 2007.

[5] Requirements and Evaluation uation Procedures for eVoting, Melanie Volkamer, Margaret Margaret McGaley, ARES'07: Second International Conference onAvailability, Reliability and Securit Security, IEEE, 2007

[6] Electoral Commission' website website to register to vote. Available onlineonline at http://www.aboutmyvote.co.uk/ register.uk/register/CitzSelet .cfm?officeID=214 & CFID=1279901 799012&CFTOK EN=71181288

[7] FVAP Voting Assistance Guide. Guide. Available online at http://www.fvap.gov/pubs/vag.htm1#ch3

[8] Department of Defense U.S., Report on IVAS 2006, As Required by Section Section 596 of the National Defense Authorization Act for Fiscal Year 2007, December 2006.

[9] RFC 4648. October 20062006. Available at http://tools.ietf.org/html/rfc4648#sectio 8#section-6

[10] Wang, X. et. al.: Cryptanalysis Cryptanalysis of the hash functions MD4 and RIPEMD. InIn Advances in Cryptology -EUROCRYPT 2005 2005, 24th Annual International Conference on thethe Theory and Applications of Cryptographic phic Techniques, Aarhus, Denmark, May 22-26, 2005, Proceedings (2005), vol. 3494 of of Lecture Notes in Computer Science, Springer, pp r, pp. 1-18.

[11] Wang, X.; Yu, H.: How to break MD5 and other hash functions. In Advances Advances in Cryptology -EUROCRYPT 2005, 24th Annual Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus,Aarhus, Denmark, May 22-26, 2005, Proceedings (200 (2005), vol. 3494of Lecture Notes in Computer Science, Springer, pp. 19-35.

[12] Hawkes, P. et. al.: MD5 collision, October 2005. Available at http://eprint.iacr.org/2004/264.

[13] Klima, V.: Finding MD5 collisions on a notebook PC using multi-message modifications. In International Scientific Conference Security and Protection of Information, May 2005.

[14] S. Prabhakar, S. Pankanti, and A. K. Jain, "Biometric recognition: Security and privacy concerns," *IEEE Security Privacy Mag.*, vol. 1, no. 2, pp. 33–42, 2003.

[15] Jain, A.; Ross, A.; Prabhakar, S: An Introduction to Biometric Recognition. IEEE Transactions on Circuits and Systems for video Technology, Vol. 14, No.1, pp. 4-20, January 2004.

[16] Tiltont, C.: The Role of Biometrics in enterprise Security. Dell Power Solutions. 2006.Available online at http://www.dell.com/downloads/global/power/ps 1q06-20050132-Tilton-OE.pdf.

[17] Hof, S.: E-Voting and Biometric Systems? Electronic Voting in Europe. pp. 63-72. 2004.

[18] F.Song, H.Liu,David Zhang,J.Yang , A Highly scalable incremental facial feature extraction method, Neurocomputing vol:71(2008) pg:1883-1888.

[19] Schweisgut, J: Coercion-resistant electronic

**Prof.E.S.Shameem Sulthana** received her MCA from Bharathidasan University, Trichy (May'2000) and she has completed M.Phil. (Comp. Science) from Mother Teresa Women's University, Kodaikannal. (June'2005). Now, She is pursuing her Ph.D. in Bharathiar University, Coimbatore. Her research area is Web Service Security.

She worked as a LECTURER in Bharathidasan Arts & Science College. After that she served as a LECTURER in MCA department in Vivekananda Engineering College. At present she is working as a ASSISTANT PROFESSOR in Dept. of Computer Science, Achariya Arts & Science College, Pondicherry.

Her research interests are in Web Technology, Network Security, Web Security. She is a Life member of computer society of India, ISTE and institute of engineers India. She has published many papers in international conferences and journals.