"Survey Paper on E-Smart Voting System using Cryptography"

YashSagarPachorkar[1], Damini DeepaksaPawar[2], Minesh Rajan Ahirekar[3], Sanyukta Sanjay Lakkam[4], Prof.Ajit R Patil[5]

[5]*Assistant Professor*

Department of Computer Engineering, Bharati Vidyapeeth's College of Engineering Lavale, Pune, India

Abstract- Currently voting process throughout the world is done using Electronic Voting Machines. Though this system is widely followed, there are many drawbacks of the system. People have to travel to their assigned poll booth stations, wait in long queues to cast their vote, face unnecessary problems and so on. It becomes difficult for working profession people or elderly/ sick people to cast their vote due to this system. This calls for a change in system which can be done if voting processes in conducted online. Few developed countries are trying to implement online voting system on small scale and have been successful in doing so. We propose a system which overcomes limitations of existing online system which uses bio-metric technologies and instead use One Time Password system which is more secure and accurate. As a result, the aim of this paper is twofold. Firstly, to identify the set of generic constitutional requirements, which should be met when designing an e-voting system for general elections? This set will lead to the specific (design) principles of a legally acceptable e-voting system. Second, to identify, using the Rational Unified Process, the requirements of an adequately secure e-voting system. These Requirements system from the design principles identified previously. The paper concludes that an e-voting capability should, for the time being, be considered only as a complementary means to the traditional election processes. This is mainly due to the digital divide, to the inherent distrust in the e-voting procedure, as well as to the inadequacy of the existing technological means to meet certain requirements.

Keywords- Fingerprint, Biometric, AES- DES, Encryption.

I. INTRODUCTION

The emerging Information Society has enabled people in the developed countries to perform several of their activities in a direct, electronically automated and efficient way. To keep up with the need to provide citizens with the ability to benefit from services over networks, as well as to reduce the cost and bureaucracy of public administration, governments are striving to transfer an increasing number of their activities to the new medium. E-voting can be an efficient and cost effective way for conducting a voting procedure and for attracting specific groups of people (e.g. young or disabled electors) to participate [1]. The term e-voting (electronic voting) is used hereby to denote a voting process, which enables voters to cast a secure and secret ballot over a network. In this paper, e-voting refers to general elections and/or referenda, at state and/or local level, with binding effects. Many public authorities are, in general, concerned with the compliance of electronic voting systems with the existing legal (i.e. constitutional) framework. The first aim of the paper is to discuss whether an e-voting scheme could meet the legal requirements, as these are laid down in the modern information societies.

II. OVERVIEW

Now a day in India two types of method are being used for voting. The first method is secret ballot paper, in which many papers are used and second method is EVM (electronic voting machine) which is in use since 2003. We have to propose a method for online voting that is more secure than the existing system. Here face recognition concept is used to identify the exact person whose image is stored in the database. Three levels of verification were used for the voters in our proposed system. The first one is Unique id number verification, second level of verification is election commission id or voter card number, if your election commission id number is correct then you have to go for third level of security which is the main security level where the system recognize the face and fingerprint of the real voter from the current database of face images given by the election commission. If the image taken matches with the respective image of the voter in the database, then a voter can cast their vote in the election. as you have to know that in existing system is not much more secure because in existing system security level is only voter card so any one can give vote for other person by just carrying their voter card but here we can provide a way for voting which is more secure than existing system. Online voting system is a web based application. Online voting system is an online voting technique in which people who are Indian citizens and age is above 18 years and are of any sex can cast their vote without going to any physical polling station. Online voting system is a software application through which a voter can cast votes by filling forms themselves which are distributed in their respective ward. All the information in forms which has to be entered by data entry operators is stored in database. Each voter has to enter his all basic information like name, sex, religion, nationality, criminal record etc. correctly in form taken from ward. Online voting system project is implemented in java platform using MySQL database as back end. Main aim of online voting system is to develop an online application like online reservation system, for citizens who are above 18 years of age to vote through online. Using these system citizens of India can vote through online without visiting polling booth. A centralized database is maintained by election commission of India where citizens information is maintained whenever citizen is using online voting system his/her information is authenticated with the data present in database if user is not in the list he cannot use online voting system.

Users are provided with an online registration form before voting user should fill online form and submit details these details are compared with details in database and if they match then user is provided with username and password using this information user can login and vote. If conditions are not correct entry will be canceled. Also given voter ID when registration of user is completed user gets sms with his aadhar ID and voterID.

III. MOTIVATION

The average election turnout over all nine phases for 2014 LokSabha election was around online is a possible idea. Indians mobile phone subscriber base crested the 1 billion users mark, as per data released recently by the country's telecom regulator. People of all age group must willingly exercise their right to vote without feeling any sort of dissatisfaction. Currently 42 percent of internet users in India have an average internet connection speed of above 4 Mbit/s, 19 percent have a speed of over 10 Mbit/s, and 10 percent enjoy speeds over 15 Mbit/s. The average internet connection speed on mobile networks in India was 4.9 Mbit/s. Online Voting overcomes various other problems faced during election process such as creating awareness among rural areas and youths, cost reduction, security, etc.

IV. OBJECTIVE

Implementation of safe and secure online system application which will make casting votes from home/office/institutes possible and thus avoiding waste of time by standing in long queues, nullifying travelling time and cost to visit given voting center, avoiding the risk of being manhandled and other related problems and in turn enable maximum voters turn out.

V. LITERATURE SURVEY

a. Advance Online Voting System -
PallaviDivya, PiyushAggarwal, Sanjay Ojha (School Of Management, Center forDevelopment of Advanced Computing (CDAC), Noida

In this paper authors propose an approach for e-actively user-friendly application for all users. This system is being developed for use by everyone with a simple and self-explanatory graphical user interface (GUI). The GUI at the server's end enables creating the polls on behalf of the client.

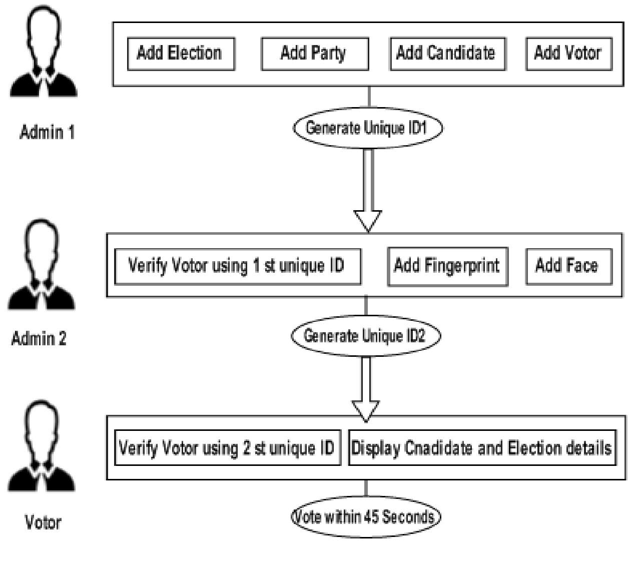
b. Online Election Voting Using One Time Password-
Prof. UttamPatil, Asst.Prof. atDr.MSSCET. Computer Science branch Vaibhav More,Mahesh Patil,8thSem at Dr.MSSCET. Computer Science branch.

Authentication technique proposed is - One Time Password (OTP). One Time Password principle produces pseudorandom password each time the user tries to log on. This OTP will be send to voters mobile phone. An OTP is a password that is only valid for single login session thus improving the security. The system takes care that no voter can determine for whom anyone else voted and no voter can duplicate anyone elsevote.This technique is imposed to ensure that only the valid person is allowed to vote in the elections.

c. Electronic Voting System Using AadharCard -
C. Tamizhvanan, S. Chandramohan, A. Mohamed Navfar, P. Pravin Kumar, R. VinothAssistant Professor, B.Tech Student Department of Electronics and CommunicationEngineering Achariya College of Engineering Technology, Puducherry, India

Electronicvoting system provides improved features of voting system over traditional voting system such as accuracy, convenience, exibility, etc. The design of the system guarantees that no votes in favour of a given candidate are lost, due to improper tallying of the voting counts.

VI. PROPOSED WORK



A. Overview

In this project we are working with three different security levels

1) Level 1: Unique id number (UID). At the time of voter registration system will request for the unique id from the voter. Uniqueid is verified from the database provide by the election commission.

2) Level 2: Election commission ID card number. In the second level of verification, the voter has to enter the electionCommission id or voter's id number. The entered id number is verified from the database provide by the election commission. Then enter the face and fingerprint details of votor.

3) Level 3: Face and fingerprint recognitionwith respective election commission id number. In this level, Eigen face algorithm is used to verifythe facial image of the voters from the database provided by the election commission.

B. Mathematical Model

Simply minimizing total expected waiting time across all polling stations is insufficient as this may allow long voter waiting times in some polling stations in order to decrease voter waiting time in other polling stations. This is undesirable in an election process as we seek to provide equity to all voters so that no one particular group of voters is disadvantaged or disenfranchised. However, there is no universal way to interpret "equity." The ideal case is that the expected waiting time in queue at every polling station is the same. But it is generally not feasible to achieve this ideal situation. Therefore, the following metric (the average absolute differences of expected waiting times among polling station) can be used as a proxy for "equity:"

$Z(X) = Wi(xi)-Wj(xj)\,|\,/(N(N-1)/2);$

(where N is defined as the total number of voting polling station, X = (x1,x2, ...,xN)', xi (i = 1,...,N) is the number of voting machines allocated to polling station i, and Wi(xi) (i = 1,...,N) is the expected waiting time for voters at polling station i. Thus, the allocations that provide the best "equity" are the global optimal solutions to the following optimization problem:

$\mathrm{Min}\{Z(X)\ |\ X = \mathrm{lambda}\}$

where is the set of feasible solutions, and |lambda | is finite.

Algorithm

AES(Advanced Encryption Standard)

Pseudo code for AES

Key Expansion: The keyexpansion routine creates round keys word by word, where a word is an array of four bytes. The routine creates 4x(Nr+1) words. Where Nr is the number of rounds. The process is as follows

The first four words are made from the cipher key (initial key). The key is considered as an array of 16 bytes (k0 to k15).

The first four bytes (k0 to k3) become w0, the four bytes (k4 to k7) become w1, and so on. The rest of the words (wi for i=4 to 43) are made as follows

1. If (i mod 4) != 0, wi=wi-1 xor wi-4.

2. If (i mod 4) = 0, wi=t xor wi-4.

Here t is a temporary word result of applying SubByte transformation and rotate word on wi-1 and XORing the result with a round constant.

Modifications in AES Key Expansion

Certain changes made in the above key expansion process improves the encryption quality, and also increases the avalanche effect. The changes are

1. The Rcon value is not constant instead it is being formed from the initial key itself, this improves the avalanche effect.

2. Both the s-box and Inverse s-box are used for the Key Expansion process which improves non-linearity in the expanded key and also improves the encryption quality.

3. We do not use the S-box and Inverse S-box as such for this algorithm; instead we perform some circular shift on the boxes based on the initial key this improves the key sensitivity.

FINGERPRINT

The steps followed by the main fingerprint matching process and percentage calculation, is shown in the pseudo code procedure below.
Procedure Fingerprint Match –

Input: Input image and a set of Template images

Output: Matched Fingerprint

Step 1–Call Procedure MinutiaeExtract(I) and store the result in m1.

/*Extract minutiae set of input image I in m1*/

Step 2–Call Procedure MinutiaeExtract(T) and store the result in m2. /*Extract minutiae set of template image T in m2*/

```
Step 3–Align the minutiae according to the leftmost minutiae of each image.

Step 4–Find the amount of matching minutiae by iterating over the smaller of the two minutiae set.

Step 5–Print matching percentage

Step 6–Return template image with highest matching percentage.
```

The steps for minutiae extraction from a fingerprint image and subsequent elimination of false minutiae, as described in the previous section, are illustrated in the pseudocode procedure given below.

```
 Procedure Minutiae Extract –

Input: Fingerprint Image

Output: Extracted Minutiae Set

Step 1–If the image is color then convert it into grayscale

/*Pre-processing begins*/

Step 2–Perform histogram equalization on the image.

Step 3–Calculate a suitable threshold for binarization.

Step 4–Binarize the image using the above threshold.

Step 5–Repeatedly thin the image until the ridges are one pixel thick.

/*Minutiae Extraction begins*/

Step 6–Slide a 3X3 window across a pixel of the image.

Step 7–Calculate the summation of the 8 neighbors.

Step 8–If the center pixel of the window is 1 then go to step 9, else goto step 10.

Step 9–If the sum = 1 then it is a termination, else if the sum = 3 then it is a bifurcation.

Step 10–Repeat Steps 6 to 9 for each pixel of the image.

/*Post-processing begins*/

Step 11–Calculate the inter-ridge width D for each row.

Step 12–Find the average over all such D.

/*False Minutiae Removal*/

Step 13–If the distance of a ridge from neighboring ridges is less than D then discard the minutiae.

Step 14–Repeat the above process for bifurcation pairs and ridge-bifurcation pairs.

Step 15–Return the final minutiae set.
```

7.3 Methodologies

1) Every New User in the India is first register for Voting. So, our first step is registration

2) At that time of Registration System Capture, the Face of the user by using Web Camera and Store the Face sample in theServer Database for Security Purpose.

3) At the time of election, we will use three level of security first one is unique id verification second one is voter id verification third one is face recognition.

4) System will be checking whatever unique id and voter id entered by the voter is correct or not.

5) If unique id or voter id is correct than system will take image of voter and compare with the respective image of database or server.

6) If the image in database is matching with the captured image of the voter, then he/she is allowed to cast is vote.

7) On the voting page all the party whatever party contest in the election symbols /buttons will be there. Voter can cast his /her vote in the election.

8) As soon as voter will give vote the id of voter logout automatically so we can say that a voter can give only one vote.

9) On counting form only election commission authorized user can login with the secure id and password if both id and password is correct then voting process will be continuing.

Tools and Technologies Used:

This proposed concept is a web-based system so basic features related with web-based technologies such as client-server, database,image processing properties determine the software requirement of the system. The software product is a standalone system and it is not the part of larger system. The system will be made up of two parts.Before the Election Day the application is used for general purposes such as viewing candidates' profiles and election results inpast years. On the Day of Election another independent Android application is used for voting operations. This application will beavailable online on authorized government sites and can be downloaded for free. This application will be installed on voter'stechnology used. These votes are accepted by the system on the server. The Election Commission Authority arranges the wholesystem according to its requirements on the server where the system is running.

VII. FUTURE SCOPE

This system can enhance the application by linking it to the Aadhar Card database in order to retrieve more details of the license/vehicle owner.

VIII. REFERENCE

[1]. PallaviDivya, PiyushAggarwal, Sanjay Ojha (School Of Management, Center For Development of Advanced Computing (CDAC), Noida , ADVANCED ONLINE VOTING SYSTEM, International Journal of Scientific Research Engineering Technology (IJSRET) Volume 2 Issue 10 pp 687-691 January 2014 www.ijsret.org ISSN 2278 0882.s http://www.ijsret.org/pdf/120437.pdf

[2]. C.Tamizhvanan, S.Chandramohan, A. Mohamed Navfar, P.Pravin Kumar, R.Vinoth Assistant Professor1, B.Tech Student Department of Electronics and Communication Engineering Achariya College of Engineering Technology, Puducherry, India , Electronic Voting System Using Aadhaar Card, International Journal of Engineering Science and Computing, March 2018 http://ijesc.org/upload/6bba24b1bfd8257c1d476cdbfa04dd69.Electronic%20Voting%20System%20Using%20Aadhaar%20Card.pdf

[3]. Prof. UttamPatil, Asst.Prof. atDr.MSSCET. Computer Science branch Vaibhav More, Mahesh Patil ,8thSem at Dr.MSSCET. Computer Science branch, Online Election Voting Using One Time Password , National Conference on Product Design (NCPD 2016), July 2016 http://mobilityresearchforum.com/ncpd2016/wp-content/uploads/2016/08/NCPD2016_paper_4.pdf

[4]. ChetanSontakke,SwapnilPayghan, ShivkumarRaut,ShubhamDeshmukh, MayureshChande, Prof. D. J. Manowar BE Student Assistant Professor Department of Computer Science and Engineering KGIET, Darapur, Maharashtra, India, Online Voting System via Mobile ,International Journal of Engineering Science and Computing, May 2017 http://ijesc.org/upload/6085ddf59ba19a4326520f45f6e2d504.Online%20Voting%20System%20via%20Mobile.pdf

[5]. R.Sownderya, J.Vidhya, V.Viveka, M.Yuvarani and R.Prabhakar UG Scholar, Department of ECE, Vivekanandha College of Engineering for Women, India, Asian Journal of Applied Science and Technology (AJAST) Volume 1, Issue 2, Pages 6-10, March 2017 http://ajast.net/data/uploads/2ajast-2.pdf