ISSN 2229-5518

E-VOTING

Pratik Shete, Vaishnavi Kedari, Aishwary Porwal

Abstract— E-Voting is an Application which provides facility to caste vote for critical and corporate decisions. It helps to caste vote from remote place. In this system election is held in confidentiality by applying appropriate security measures. It allows voter to vote for any participating candidate only if he logs into the system by entering correct password which is generated by merging two shares using Visual Cryptography scheme. In this Application One time password (OTP) is used for authentication purpose. Phishing is an attempt by an individual or a group to get personal confidential information from unsuspecting victims. E-Voting focuses on security, secrecy and privacy.

Index Terms— ***Visual Cryptography; One time password; Phishing; authentication***

1 INTRODUCTION

1.1 Traditional Voting Process

Traditional Voting process is divided into different phases:

1. Authentication: In this phase voter authenticates himself or herself by showing voter id card which is done by officer. Once the authentication is done ballot paper is provided to caste the vote.
2. Vote: Vote takes place in the booth where voter can caste the vote by writing with pen on ballot paper and put it into ballot box where all the votes are mixed.
3. Vote counting: After casting vote the officer collects the ballot box and election committee is assigned to count the votes and result is announced.
4. Verification: Various verification procedures are used most procedures are public and verified by representative of candidates of competing parties. Recount is also possible if there is any fraud or error.

Traditional voting systems are not efficient due to long period of preparation, bogus voting, include papers, punch cards, mechanical levers, optical-scan machines . These systems are not efficient as they are conducted manually and therefore very often are not accurate. As a consequence, it is obligatory to carry the available voting through an electronic system

1.2 Requirements of E-Voting

The requirements in traditional voting system are also included in E-Voting and some of them are mentioned below:

1. Eligibility: Only eligible voters are allowed to caste the vote.
2. Fairness: Voting outcomes cannot be known before tally.
3. Uniqueness: No voter is allowed to caste the vote more than once.
4. Efficiency: Counting of the votes is done in minimum amount of time.
5. Privacy: No one can access the information about voters vote.
6. Accuracy: All valid votes should be counted correctly.

2 PROBLEM STATEMENT

E-Voting Application will help the voters to vote for the elections from remote places. This application is proposed to reduce the manual effort of the people as they need to go to the booths for casting their vote.

Whenever schedule date notification is get on user android device, user can cast their vote from anywhere and anytime. For casting the vote particular user should be authorized so the proposed system will done authentication of voter. The proposed system consists of three phases: online registration; vote casting and vote collecting and result phase. Proposed protocol provides secure and efficient online vote casting and can also be implemented parallel with paper ballot voting system. Proposed protocol has efficiency, security and deployable in developing countries due to its reliance on SMS messaging without requiring internet connectivity. Mobile Voting system provides convenience and access to the electorate without the geographical restrictions. Mobile phone is one of the emerging technologies to perform e-voting with democratic norms and privacy concern

3 LITERATURE REVIEW

3.1 Visual Cryptography

Visual Cryptography is a special encryption technique to hide information in images in such a way that it can be decrypted by the human vision if the correct key image is used. The technique was proposed by Naor and Shamir in 1994. Visual Cryptography uses two transparent images. One image contains random pixels and the other image contains the secret information. It is impossible to retrieve the secret information from one of the images. Both transparent images and layers are required to reveal the information. The easiest way to implement Visual Cryptography is to print the two layers onto a transparent sheet.

When the random image contains truly random pixels it can be seen as a one-time pad system and will offer unbreakable encryption. In the overlay animation you can observe the two layers sliding over each other until they are correctly aligned and the

International Journal of Scientific & Engineering Research, Volume ÑÛ¤(ÚÚÜÌ¤l û¤%ÌÉÙÜÈÙà ı l Ÿ h ¤¤
ISSN 2229-5518

hidden information appears. To try this yourself, you can copy the example layers 1 and 2, and print them onto a transparent sheet or thin paper. Always use a program that displays the black and white pixels correctly and set the printer so that all pixels are printed accurate (no diffusion or photo enhancing etc.). You can also copy and past them on each other in a drawing program like paint and see the result immediately, but make sure to select transparent drawing and align both layers exactly over each other.

3.2 Working of Visual Cryptography

Each pixel of the images is divided into smaller blocks. There are always the same number white (transparent) and black blocks. If a pixel is divided into two parts, there are one white and one black block. If the pixel is divided into four equal parts, there are two white and two black blocks. The example images from above uses pixels that are divided into four parts.

In the table on the right we can see that a pixel, divided into four parts, can have six different states. If a pixel on layer 1 has a given state, the pixel on layer 2 may have one of two states: identical or inverted to the pixel of layer 1. If the pixel of layer 2 is identical to layer 1, the overlaid pixel will be half black and half white. Such overlaid pixel is called grey or empty. If the pixels of layer 1 and 2 are inverted or opposite, the overlaid version will be completely black. This is an information pixel.

We can now create the two layers. One transparent image, layer 1, has pixels which all have a random state, one of the six possible states. Layer 2 is identical to layer 1, except for the pixels that should be black (contain information) when overlaid. These pixels have a state that is opposite to the same pixel in layer 1. If both images are overlaid, the areas with identical states will look grey, and the areas with opposite states will be black.

The system of pixel can be applied in different ways. In our example, each pixel is divided into four blocks. However, you can also use pixels, divided into two rectangle blocks, or even divided circles. Also, it doesn't matter if the pixel is divided horizontally or vertically. There are many different pixel systems, some with better contrast, higher resolution or even with colour pixels.

If the pixel states of layer 1 are truly (crypto secure) random, both empty and information pixels of layer 2 will also have completely random states. One cannot know if a pixel in layer 2 is used to create a grey or black pixel, since we need the state of that pixel in layer 1 (which is random) to know the overlay result. If all requirements for true randomness are fulfilled, Visual Cryptography offers absolute secrecy according to the Information Theory.

If Visual Cryptography is used for secure communications, the sender will distribute one or more random layers 1 in advance to the receiver. If the sender has a message, he creates a layer 2 for a particular distributed layer 1 and sends it to the receiver. The receiver aligns the two layers and the secret information is revealed, this without the need for an encryption device, a computer or performing calculations by hand. The system is unbreakable, as long as both layers don't fall in the wrong hands. When one of both layers is intercepted it's impossible to retrieve the encrypted information.

3.3 Visual Cryptography Algorithm

Step 1: Load Source Image

Step 2: Division of image into black and white pixel. “java.awt.image.BufferedImage” this package used for properties related to images int WHITEPIXEL = (255<<24)| (255<<16)| (255<<8) |255; int BLACKPIXEL = (255<<24); where threshold = 128;

Step 3: Pre Encryption Step: Initialize two matrix for black and white pixels. Apply Permutation Vector C0 = White matrix value; Vector C1 = Black matrix value; Typecasting of Values White [if] = (IntMatrix) C0.get (if); Black [if] = (IntMatrix) C1.get (if);

Step 4: Storing of image in the form of luminance and chrominance red = pixel >>16 green = pixel >>8 blue = pixel Factor = (red*0.299) + (green*0.587) + (blue*0.114) if (Factor > threshold) then WHITEPIXEL else BLACKPIXEL

Step 5: Encryption by Transpose Operations

Step 6: Overlay Of Shares if (Share 1 & Share 2) then Display Original Image else if (Share 1 &! Share 2) Display Share 1 else if (Share 2 &! Share 1) Display Share 2 Example: Share 1 Matrix = WWBB BBWW Share 2 Matrix = WWWW BBWB Share 1 + Share 2 = WWBBBBWB

4 PROPOSED SYSTEM

The proposed system aims at providing a facility to cast vote for critical and confidential internal corporate decisions. It has the flexibility to allow casting of vote from any remote place. The election is held in full confidentiality by applying appropriate security measures to allow the voter to vote for any participating candidate only if he logs into the system by entering the correct password which is generated by merging the two shares using VC scheme. Administrator sends share 1 to voter e-mail id before election and share 2 will be available in the voting system for his login during election. Voter will get the secret password to cast his vote by combining share 1 and share 2 using VC. Phishing is an attempt by an individual or a group to get personal confidential information from unsuspecting victims. Fake websites which appear very similar to the original ones are being hosted to achieve this. Internet voting focuses on security, privacy, and secrecy issues, as well as challenges for stakeholder involvement and observation of the process. A new approach is proposed for voting system to prevent phishing attacks.

Our system consists of 6 modules: Registration, One Time password, Send 1st share of password, Login, New candidate, Results

International Journal of Scientific & Engineering Research, Volume
ISSN 2229-5518

A. Registration

In this module admin will verify the user and register the user who will vote. Registration module will take all the personal information about the voter for the verification purpose.

B. One time password

One time password module will be used for authentication purpose where administrator will take the voters mobile number and OTP will be sent to his phone if the OTP is entered correctly voter will be authenticated.

C. Send 1st share of password

As soon as the user registers the system will break the password and the first half of password will be sent to the user's email-id and the 2nd share the user needs to enter while login

D. Login

This module enables the user and admin to login to the system by entering id and password.

E. New Candidate

Admin will add the number of candidates nominated for Election whenever new election is announced.

F. Results

Admin and user can view the election result by using the election id once the election results are out.

5 SYSTEM OVERVIEW

Our system is capable of performing remote voting using one time password as security feature into it and specially crafted for corporate uses. Confidentiality in election is provided by giving security measures to allow the voter to vote for any participating candidate only if he logs into the system by entering the correct password which is generated by merging the two shares using visual cryptography. Our system has the flexibility to allow casting of vote from any place. Attempts are made by hackers to get the private information out. Websites similar to original ones are used to achieve this. Thus our system using internet voting focuses on security, privacy, and secrecy issues, as well as challenges for stakeholders involved and observation of the process. Therefore our system is developed to remove the efforts needed in the traditional voting process.
We have implemented an android voting system application which provides security mechanism using visual cryptography
The system will send a notification or toast after successfully verifying OTP and voting for a particular candidature. It is money saving, time saving application which is easy to use and provides a good graphical user interface.

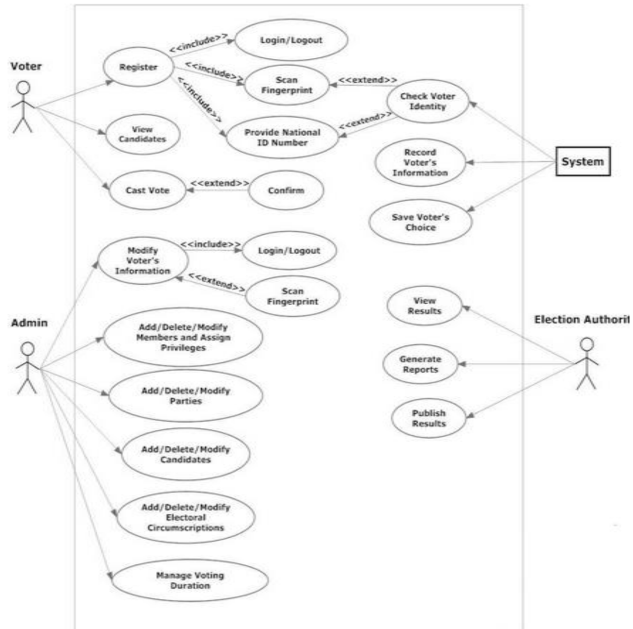

Fig: UseCase Diagram

6 CONCLUSION

In this paper we have proposed an online mobile electronic voting system which provides online voting from remote locations located geographically anywhere using OTP method and visual cryptography scheme.
The system makes note of each authenticated user in database and then makes count of votes and final phase is of generating results where privacy and secrecy is maintained while voting and phishing is prevented.
The authenticity of user is checked by validating via OTP and Aadhar card or other SSID number etc. The privacy of votes submitted are maintained by deleting database contents of voters.

ACKNOWLEDGMENT

We are thankful to all those who helped us throughout the course of writing this paper. Their valuable and insightful inputs and constructive criticisms have been of utmost importance.

REFERENCES

[1] http://scihub.cc/http://ieeexplore.ieee.org/document/743297/
[2] https://www.ijarcsse.com/docs/papers/Volume_3/11_November2013/V3I11-0160.pdf
[3] http://ccis2k.org/iajit/PDF/vol.10,no.4/4313.pdf
[4] https://www.scribd.com/document/245942120/Feasibility-Study-on-e-Voting-System

International Journal of Scientific & Engineering Research, Volume ÑÛ(ÚÚÜÌ l û%ÌÉÙÜÈÙà ı l Ÿ h ll
ISSN 2229-5518