INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

IMPLEMENTATION OF SECURE E-VOTING USING ONE TIME PASSWORD ACCESS

MADHURI VISHNU BHARAD, ANKIT MUNE

1. Student of Master of Engineering in (CSE), IBSS college of Engineering and Technology, Amravati, India.
2. Head of the Department of (CSE), IBSS College of Engineering and Technology, Amravati, India

Accepted Date: 05/03/2015; Published Date: 01/05/2015

Abstract: This paper deals with design, build and test a online voting system that facilitates user (the person who is eligible for voting), candidate (Candidate are the users who are going to stand in elections for their respective party), Election Commission Officer or election administrator (Election Commission Officer who will verify whether registered user and candidates are authentic or not) to participate in online voting. This online voting system is highly secured, and its design is very simple, ease of use and also reliable. The proposed software is developed and tested to work and allows online voting. It also creates and manages voting and an election detail as all the users must login by user name and password and click on his favorable candidates to register vote. This will increase the voting percentage in India. By applying high security it will reduce false votes.

Keywords: Internet voting, e-voting, Secured Network, One time password access

Corresponding Author: MISS. MADHURI VISHNU BHARAD

Access Online On:

www.ijpret.com

How to Cite This Article:

Madhuri Vishnu Bharad, IJPRET, 2015; Volume 3 (9): 502-510

PAPER-QR CODE

INTRODUCTION

The present form of voting in general elections in India is founded entirely on paper based and largely manual voting procedures. Voting schemes have evolved from counting hands in early days to systems that include paper, punch card, mechanical lever and optical-scan machines. Electronic voting systems provide some characteristic different from the traditional voting technique, and also it provides improved features of voting system over traditional voting system such as accuracy, convenience, flexibility, privacy, verifiability and mobility. But it suffers from various drawbacks such as Time consuming, Consumes large volume of pare work.

No direct role for the higher officials, Damage of machines due to lack of attention, Mass update doesn't allows users to update and edit many item simultaneously. These drawbacks are overcome by Online Voting System. Online Voting System is a voting system by which any Voter can use his/her voting rights from anywhere in the country. We provide a detailed description of the functional and performance characteristics of online voting system. Voter can cast their votes from anywhere in the country without visiting to voting booths, in highly secured way. That makes voting a fearless of violence and that increases the percentage of voting[1] The challenge of building secure Internet voting systems has attracted a great deal of attention among researchers in applied cryptography. Over the years, numerous voting protocols have been proposed in the literature. While the number of security properties of these protocols has increased steadily over the years, new requirements have been added to the list of desirable security features. Although an impressive security level has been reached today by increasingly complex voting protocols, the all-embracing "perfect" voting system is still missing. Some of the most important open problems are long-term security. E Voting is getting to be seen a next generation approach of election in almost all countries. The ultimate aim of e-Voting is to provide voters a good environment so that voters can cast their votes with minimum cost and efforts on the internet. Up to now there are so many properties have been proposed to make the e-Voting secure process, among them some are the below given must be satisfied.

(1) Eligibility: Only eligible voters are permitted to cast their ballots.

(2) Privacy: There is no association between voter's identification and a marked ballot.

(3) Uniqueness: No voter can cast his ballot more than once.

(4) Completeness: No one can forge a valid ballot and a voter's ballot cannot be altered, the valid ballots are counted correctly.

(5) Fairness: No one can falsity the result of voting.

(6) Verifiability: Voters can verify that their ballots are counted correctly.

(7) Uncoercibility: No voter can prove what he voted to others to prevent bribery.

(8)Efficiency: The computations can be performed within a reasonable amount of time.

(9) Mobility: The voter can vote anytime and anywhere through internet.

Instead of these features, a good e-Voting system must berobust, fast and convenient.

2 LITERATURE REVIEW &RELATED WORK

In the past, people go to polling place and take the blank ballots, then punch a hole or append the seal. If the seal is not clear enough, or the vote is damaged by soiling, it may bring some debate on the result. In order to resolve these situations, the technology of electronic voting (e-voting) comes into existence. By using information technology, E-voting system can cast and count votes with higher convenience and efficiency, even make the electoral procedures simple and reduce the mistake rate of ballot examination[7]

List of locations and methods used during the 2002 pilots using Internet voting systems.[8]

Date	Location	Voting Method	Technology Provider
April 26-May2, 2002	Liverpool City Council	Internet, Telephone and Text message	elections.com
April 26-May 2, 2002	Sheffield City Council	Internet, Text message and Kiosk	elections.com
April 25-27, 2002	St. Albans City & District	Internet, Telephone and Kiosk	Oracle
April 25-27, 2002	Crewe & Nantwich Borough Council	Internet and Kiosk	Oracle
April 26-30, 2002	Swindon Borough Council	Internet and Telephone	Votehere.net

Fig1Location, Method and Provider

Background

This software is being developed for use by everyone with a simple and self explanatory GUI. This is software that can be used by people to vote in an election. All the user must do is login and click on his favorable candidates to register his vote. The development and testing is done on Ethernet. While online voting system has been an active area of research in recent years, the use of insecure Internet, well documented cases of incorrect implementations reported recently. These challenges are to be resolved so that public should cast their vote in secure and convenient way. Proposed online voting system is a voting system by which any Voter can use his/her voting rights from anywhere in country. Online voting system contains

a) Voter's information in database.

b) Voter's Names with ID and password.

c) Voter's vote in a database.

d) Calculation of total number of votes.

Various operational works proposed in the system are: Recording information of the Voter in database. Checking of information filled by voter. Discard the false information. Each information is sent to election commission.

Product Perspective

The product is an election conducting tool with a simple GUI. The product is developed using): ASP.NET 4.0. Languages: C# Component Programming: C# component classes Database technologies: MS SQL Server 2012,ADO.NET Web Development: XML,HTML, DHTML, JavaScript, AJAX, JQuery Development Tool: Visual Studio 2010.

User Characteristics

Users are considered to be technically novices but expected to be able to use a computer / hand held terminal (HHT) and to click against the favorable candidate on the GUI.

Product Functions

The product has a server back-end which takes care of authenticating the users and maintaining necessary data structures. The GUI at the server's end enables creating the polls on behalf of the client. The users must connect to the server to authenticate their identification against the

password and get one time password at their email id or via sms then vote using the GUI at their end. High-level security objectives are documented in the e-Vote Security

Objectives document:

• Vote Authenticity

• Voter Anonymity

• Data Confidentiality

• Data Integrity

• System Accountability

• System Integrity

• System Disclosability/Openness

• System Availability

• System Reliability

• Personnel Integrity

• Operator Authentication and Control

3 METHODOLOGY, OBSERVATIONS:

The modules of my project are as follows.

- Election Admin
- District admin
- City admin
- Taluka admin
- Village admin
- Area admin
- Candidates

- Voters
- Encryption/Decryption module

In this voter is act as a client and the server is an election admin. Election admin first do the state wise registration. Register the different party of that state. Election admin decide the multiple admin such as district admin. District admin decide the city admin. City admin decide the Taluka admin. Taluka admin decide the area admin and area admin verify the original document of the voter. Voter first registers their name then submits their ID proof as their ADHAR CAR D. This adhar card should be verified by the area admin. If the ID proof is valid the voter should be applicable for the vote otherwise he\she not. As the voter is valid they can devote their vote on election date within the specified time.

The main aim of my project is the security of the vote that should be devoted by the voter. For the purpose of security we will use the Advance Encryption Standard Algorithm (AES). Encryption and decryption on the basis of AES algorithm.

Advance Encryption Standard (AES) Algorithm:

- AES is a block cipher with a block length of 128 bits.
- AES allows for three different key lengths: 128, 192, or 256 bits.
- Encryption consists of 10 rounds of processing for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys.

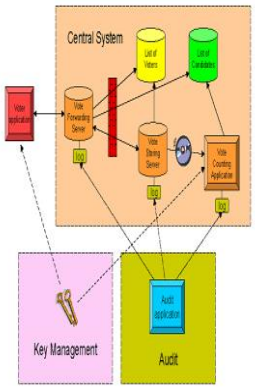

Fig 2 System design

Except for the last round in each case, all other rounds are identical.

Each round of processing includes one single-byte based substitution step, a row-wise permutation step, a column-wise mixing step, and the addition of the round key. The order in which these four steps are executed is different for encryption and decryption. Each round of processing works on the input state array and produces an output state array.

For encryption, each round consists of the following four steps: 1) Substitute bytes, 2) Shift rows, 3) Mix columns, and 4) Add round key. The last step consists of XOR the output of the previous three steps with four words from the key schedule.

For decryption, each round consists of the following four steps: 1) Inverse shift rows, 2) Inverse substitute bytes, 3) Add round key, and 4) Inverse mix columns. The third step consists of XOR. The output of the previous two steps with four words from the key schedule.

The last round for encryption does not involve the “Mix columns” step. The last round for decryption does not involve the “Inverse mix columns” step.

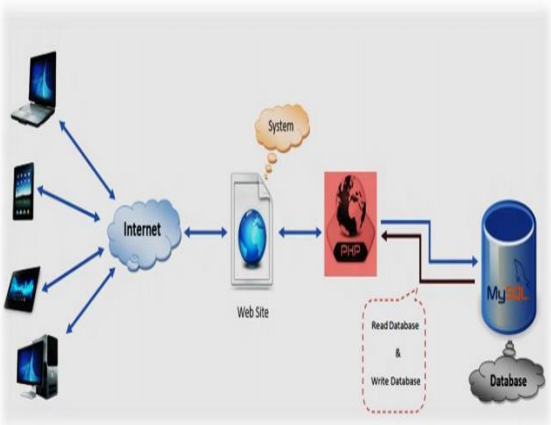

Fig 3 Block diagram of the Internet e-voting system

4 APPLICATION

Cost effectiveness – Online elections are cost effective, especially when considering production costs of printing, postage, and mailing ballots.

Security and confidentiality – A properly designed online voting system has safeguards in place to assure security of ballots and protection of voter identities.

Transparency – Online elections, particularly those run by a third-party, eliminate the chance of election mismanagement or fraud. An audible trail helps increase voter confidence.

Accuracy and expedience – Since online voting utilizes electronic ballots, there are no rejected, mismarked, or invalid votes. Results are automatically calculated, eliminating the need for manual tabulation or dreaded recounts

Empowerment – Voting is the most powerful way for members to have a voice in the leadership and direction of their organization. When allowed to vote in fair and open elections, members will feel a greater sense of value, ownership, and responsibility. This is why it is important to reach as many members as possible with different election methods including online voting.

5 CONCLUSION:

The goal of the project is to develop the secure online system so that general public will devote their vote from anywhere in the world where there an internet. The secure implementation of the system is done by using the security algorithm i.e. Advance encryption Standard algorithm. My project will produce more security for the sensitive data as compared to others.

6 REFERENCES:

1. Ankit Anand, Pallavi Divya: “An Efficient Online Voting System”(July-Aug. 2012 pp-2631-2634)

2. Ioannis Katakis, Nicolas Tsapatsoulis, Fernando Mendez, Vasiliki Triga, and Constantinos Djouvas:” Social Voting Advice Applications -Definitions, Challenges, Datasets and Evaluation”

3. Rolf Haenni, Oliver Spych er:” Secure Internet Voting on Limited Devices with Anonymized DSA Public Keys”

4. Alexander. Stakeholders: “Who is your system for? IEEE: Computing and Control Engineering, 14(1):22{26, April 2003}.”March 2004

5. Benjamin J. Alfonsi: E-Voting Advocates Hold Out Hope, IEEE DISTRIBUTED SYSTEMS ONLINE 1541-4922 © 2004 Published by the IEEE Computer Society Vol. 5, No. 3;

6. B. Swaminatha, J. Cross Datson Dinesh: “Highly Secure Online Voting System with Multi Security using Biometric and Steganography”

7. Jung-Ying Lai,Chun-Fang Lin,"Design and Implementation of an Electronic Voting System with Contactless IC Cards", Graduate Institute of Information and Computer Education, National Kaohsiung Normal University.

8. "A Survey of Internet Voting, September 14, 2011"(Voting System Testing and Certification Division 1201 New York Avenue, NW, Suite 300 Washington, DC 20005)

9. DAVIDCHAUM:" Secret-Ballot Receipts: True Voter-Verifiable Elections"(IEEE SECURITY & PRIVACY).