

A Voting Method Based on QR Codes Utilizing an Android Application

Dr. Ashwani Kumar Pandey¹, Indu Bhusan Nayak²

Professor¹, Student²

Department of Computer Engineering

Laxmi Devi Institute of Engineering & Technology

Corresponding Author's Email: - *nayakindubhusan12@rediffmail.com*

Abstract

The purpose of this system is to present a real-time system that uses a rapid Response code on an Android smart phone. The notion of an e-voting application is built utilising an Android phone application, and voter information must be required to be verified by the admin side. Once the authentication is complete, the user can login, and on the day of the election, eligible voters can get the authorised quick response Code verified from the admin side. The authentication is completed by scanning the quick response code using the appliance via the mobile scanner application. Using multiplexing and DE-multiplexing, the voter information is ready to be hidden within the rapid response code. Decode and encode data from a single answer using special symbols, then split the information back into the rapid response code pattern. The notion of an e-voting application is built using Android in the proposed manner. The voter is prompted for their password after scanning the rapid response code. When the authentication is complete, the voter is allowed to proceed with the voting process. After the voting process is done, the voter receives Short Message Service confirmation, and the account is deactivated, and the user is unable to vote again. The commission is exclusively liable for reactivating the account.

Keywords: - *QR Codes Utilizing, Voting Method, Multiplexing, Authentication, Short Message Service*

INTRODUCTION

Elections are a key feature of democracy in every country, allowing people to express their views by electing their leaders. The manual approach is the traditional method. Paper-based election procedures are utilised in the manual approach. In this method, voters cast their ballots in polling booths while waiting in a lengthy line, making it difficult to cast their votes for voters, resulting in a low rate of vote casting. This conventional procedure is less transparent since there is a possibility of cheating while voting and manually counting votes. In this traditional approach, there is a high likelihood of counting mistakes, prompting some people to vote again in alternative ways. As a result, this system causes more issues and conflict among people. This, of course, necessitates a fully automated electoral procedure with online computerization.

In addition, to prevent the previously observed election trap, electoral voting counts are done in real time at the end of elections, and the results are instantly published. It is a fundamental requirement for countries to improve their electoral systems. Because of the rapid advancement of technology in computer and telecommunications, globe e-Voting method solutions are being introduced to

eliminate the challenges associated with the previous manual election methods. With the use of e-Voting technology, our elections system and public life will become simple, efficient, and low-cost. Voters may now vote in this system from anywhere in the world. Privacy, honesty, fairness, forgery attack, verifiability, and other security standards must be met by an e-voting system. This E-voting technology is more vulnerable than traditional voting. Because of the nature of the election in a digital process, data may be readily changed, which may result in a common plan and corruption.

IMPORTANCE OF SECURE VOTING SYSTEM

In most nations, selection is the next generation method to election. The key motto of E-Voting is to provide a pleasant atmosphere for voters so that they may cast ballots for voters over the internet for the least amount of money and effort. To date, several qualities have been proposed to make this scheme secure processing, and a few of the following must be satisfied.

1. Eligibility: Only eligible voters are allowed to cast their votes in the 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. Entirety: No one can copy a valid ballot and a voter's ballot cannot be changed; only the valid ballots are counted correctly.
5. Fairness: one cannot falseness the res voting result.
6. Verifiability: Voters can check their ballots that are counted correctly.
7. Uncoercibility: Voter cannot prove what that the vote to place to others to prevent bribery.
8. Efficiency: The calculation can be accessed within a practical amount of time.
9. Mobility: The voters may vote anytime and anywhere through internet.

Instead of these characteristics, an effective e-Voting system must be strong, rapid, and user-friendly. New wants and requirements are always being suggested by research as time passes. The primary goal of an E-voting scheme is to enable suitable voting on the Internet while satisfying maximum qualities and lowest restrictions at the same time.

LITERATURE SURVEY

New system of E-Voting Using Fingerprint

The numerous applications of old methods are utilized and it's booming because of its dependability and individuality.

There are two techniques namely; the particular user is identified by Automated Finger Identification.

Verifies the identified user is verified by Automated Finger Verification.

Automated fingerprint verification:

Automated fingerprint verification will be a directly connected procedure utilized in applications similar to attendance and access control systems. The scientific level, authentication systems validate a claimed characteristic whereas detection systems determine identity based exclusively on the fingerprints. An oversized number of computer algorithms are developed to automatically process digital fingerprint images. These algorithms have greatly improved the operational productivity. Minutiae filter and Gabor filter are a part of those algorithms; of those algorithms use the next steps within the figure below to undertake and do the automated fingerprint identification.

QR codes and Security Solutions

The QR Code will be visualizing in a Matrix code. This QR codes was invented in Japan in the year 1994 by Toyota subsidiary, to support the track vehicle parts all through the manufacture. Bar codes became broadly popular in reading speed, accuracy, and superior functionality. The attack method utilized within the QR code was that when a user scans the code he's directed towards a web site and then a malicious file downloads within the user's device without the knowledge of the user.

Next Generation-A Secure E-Voting system supported Biometric Fingerprint Method

Due to ascension of technology security problems have gotten increased. Fingerprint scanner and our Microsoft scanner have ability to acknowledge thumbs no matter during which angle has been pressed on scanner. All the systems that are supported biometric mechanisms are client-server architectures which pc user has privileges to manage the system. The client machine is the main application. Here a section is only if is displaying text to tell voter that you just simply must press your right thumb on Fingerprint scanner and our Microsoft scanner has ability to acknowledge thumbs no matter during

which angle has been pressed on Scanner. If fingerprints don't seem to be matching with folks that are already stored within the server database then it might prompt that you simply just are not a registered user but when voter involves scan second time then after scanning it might prompt that you simply just have already casted vote.

A Novel Data Hiding Technique Based Bio-Secure Online System

Electronic voting could even be a decent improvement over paper systems. Iris recognition cannot occur without your permission. Cover Image Creation- this is often a system generated image used for the aim of steganography which is prepared to be finally modified into stegoimage and is shipped over the ultimate public channel. Here a 160 bit secret message is obtained from a 16 bit secret key. the key secret's concatenated with the timestamp value and MD5 algorithm is applied to urge 128 bit hash code for that key.

Image Base steganography and Cryptography

Cryptography and steganography are familiar and broadly used techniques that operate on the information so on cipher or hide their content existence. The mass of

today's steganographic systems uses images, text and pictures as cover media because people frequently transmit digital pictures more email and other Internet communication. The ISC extracting process is extremely simple and consists in are markably comparison between the S nonzero AC coefficients and K nonzero AC coefficients. The ISC steganographic performances are measured by comparing it with the well-known F5 algorithm. In fact, steganography are repeated lypractical when the utilization of cryptography isforbidden: where cryptography and powerful encryption are proscribed, steganography can get out of such policies to get ahead of communication covertly. See Figure 1

RELEATED WORK MODULES

Generating QR-Code Image

This module we are creating QR Code for encoding the understanding about the voter. Voter information contains the subsequent details similar to the voter_id no, voter name, Date of Birth and Address. Every model is programmed and representative of every module in the QR Code by way of black and white with particular symbols. QR-Code can embrace in sequence over other bar codes. The format of QR Code includes unique Finder Pattern (Position Detection Patterns) located at three corners of the symbol and may be accustomed locate the positioning of the symbol, size and inclination.

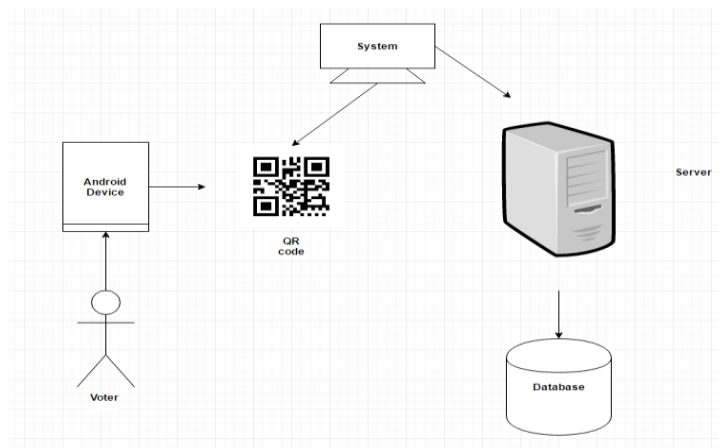


Fig.1:-Overall System Design



Fig.2:-QR Code

Mobile Authentication Module

This module is represents the authentication, which is employed for the voter to login their information for the voting processes. Logged voter is redirects to the scanner module. Authentication is employed because the basis or authorization determining whether a privilege are going to be granted to a selected user or process. The validation process are done on the net server. See Figure3

Quick Response Code Scanner Module

This module is used to check the QR-Code and examine the value of the QR-Code within the mobile. The design of QR-Code is a matrix bar code to be read by Smartphone. The codes have black modules arranged in a square pattern on a white background. In order it is encoded with the text, a Uniform Resource Locator (URL) and other data. If the voter selects the candidates, the particulars directly will be openly forwarded to the server. Fig4

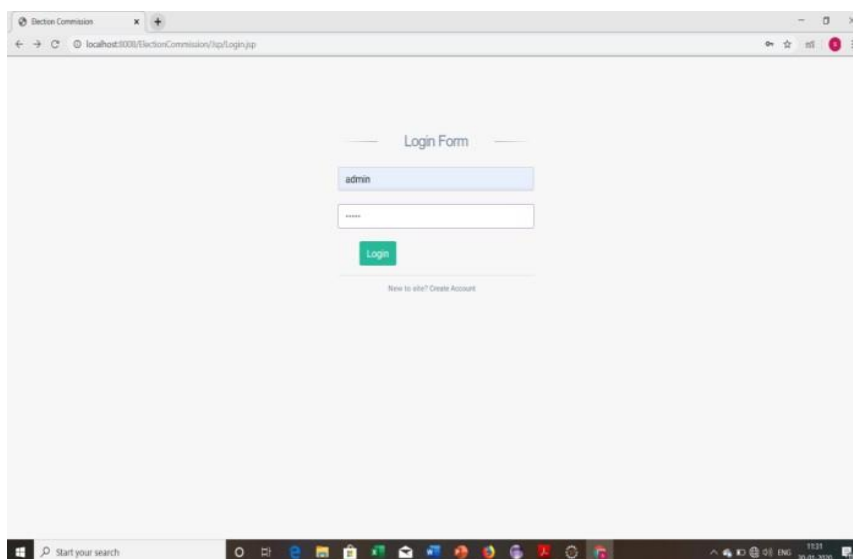


Fig.3:-Login form



Fig.4:-QR-Code Smartphone

Web Service Client Module

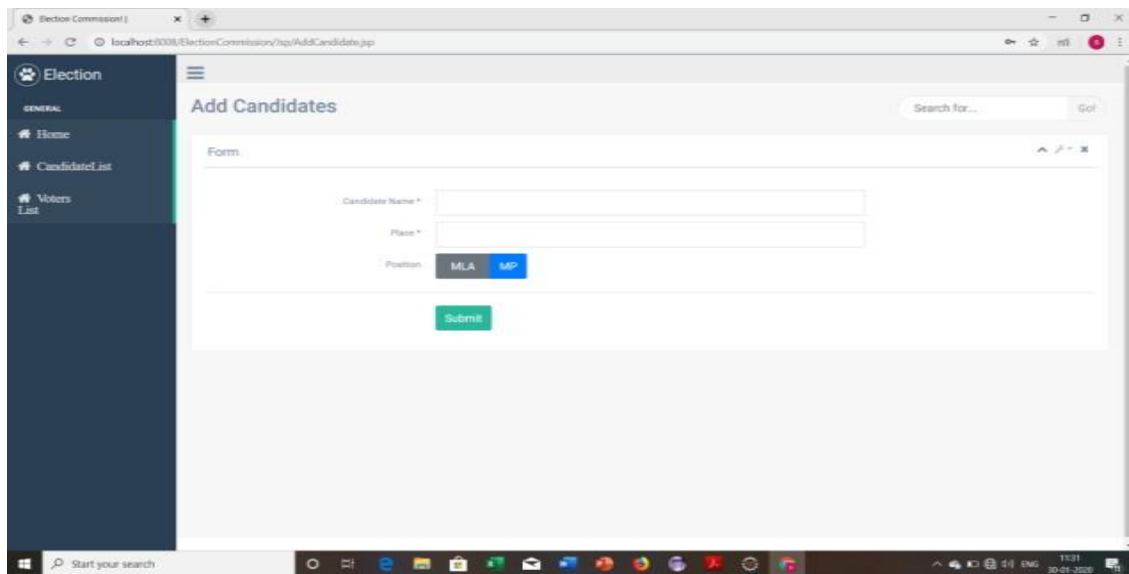


Fig.5:-Client Server

This module has the method of storing the chosen candidate information from the client, which are send through the net service. of these information's are going to be stored within the database. We are maintaining a centralized server so as to receive the chosen voter list from the database internet. during this module the candidate see they data retrieved from the database.

CONCULSION

According to this approach, we proposed using a Quick Response (QR) code on an Android smartphone to record real-time voting data. The QR- Code will validate the captured voting identification number (Id) and transfer it from beginning to finish through the smartphone, where it will be decoded as a QR code and sent to the

server for verification. The voter official sends the list of selected candidates to the server, and the server's answer assists the user in determining the validity of the voters. The specified account will be deactivated after the voting process is done.

REFERENCES

1. Bouras, C., Katris, N., & Triantafillou, V. (2001). An electronic polling service to support public awareness using web technologies.
2. Cranor, F. Electronic voting,"Encyclopedia of Computers and Computer History.
3. Autade, K., Ghadge, P., Kale, S., Kulkarni, N. J., & Mujgond, S. S. (2012). E-voting on Android

- System. International Journal of Emerging Technology and Advanced Engineering, 2(2), 242-245.
4. Belenky, A. S., & Larson, R. C. (2006). To queue or not to queue. OR/MS Today, 33, 30-34.
 5. Krimmer, R. (2006). Electronic voting 2006. GI Lecture Notes in Informatics, P-86, Bonn.