ISSN (ONLINE):2395-695X
ISSN (PRINT): 2395-695X

International Journal of Advanced Research in Basic Engineering Sciences and Technology (IJARBEST)
Vol.3, Special Issue.25, February 2017

# Electronic Voting Using Android Mobile System

Sajith Kumar.S[1], Dinesh.M[2], Mohan.J[3], Dr.Veeramalai.S[4]
[1, 2, 3] UG Scholar, Department of Computer Science and Engineering
Vel Tech High Tech Dr. Rangarajan Dr. Sakunthala Engineering College Avadi, Chennai, Tamil Nadu
[4]Professor, Department of Computer Science and Engineering
Vel Tech High Tech Dr. Rangarajan Dr. Sakunthala Engineering College Avadi, Chennai, Tamil Nadu
sajithkmr1898@gmail.com[1],dineshmohan0001@gmail.com[2],
0213mohanraina@gmail.com[3], drveeramalai@velhightech.com[4]

***ABSTRACT***

*As we know in urban areas voting is the major issue as the identification of the person is the most important issue as they do not have mostly the identity proof rather than the voting card and fake voting is done on a large scale. To avoid this we are developing this project which will store the identity of the voters and at the time of voting this identity will be matched using the photo of the voters to avoid the fake voting. This system will upload the photo of the user to the database and match with the existing photo in the stored database. For a first time voter then the information about the voter will be upload to the database through scanning QR code in aadhaar card. After the confirmation of the valid voter, an OTP will be generated and send to the voters registered mobile. The OTP is provided. Then validation is verified and allowed to vote. This is fast and also helpful for the authorities to quickly do the verification and run the voting fast. So people should not waste their time in waiting in a queue for long time for doing vote. The main purpose of implementing this concept is to increase the voting percentage. So that the voter is not required to visit the voting centre to cast their vote and also to avoid fake voting.*

***INDEX TERMS** – Quick Response Code, OTP.*

## 1. INTRODUCTION

As the modern communications and Internet, now a day all people are almost accessible electronically, the computer technology users, brings the increasing need for electronic services and their security. Usages of new technology in the voting process improve the elections in natural. This new technology refers to electronic voting systems where all election data is recorded, stored and processed primarily as digital information. Now a day security is very important. In the past, usually, mostly in military and government institutions need too much security. But, now need for this type of security is growing in everyday usage. In computing, e-services and information security it is necessary to ensure that data, communications or documents are enough secure and privacy enabled.

Security is a heart of e-voting process. Therefore the necessity of designing a secure e-voting system is very important. Usually, mechanisms that ensure the security and privacy of an election can be time-consuming, expensive for election administrators, and inconvenient for voters. There are various different levels of e-voting with different security. Therefore serious measures must be taken to keep it out of public domain. Also, security must be applied to hide votes from publicity. There is no measurement for acceptable security level, because the level depends on type of the information. An acceptable security level is always a compromise between usability and strength of security method.

## 2. LITERATURE SURVEY

The use of computers or computerized voting equipment to cast ballots in an election is nothing but Electronic voting. Sometimes, this term is used more specifically to refer to voting that takes place over the Internet. Registration of voters, tally ballots, and record votes all operations performed by Electronic systems.

Voting technology in order to prevent a recurrence of the problems that threatened the 2000 U. S. Presidential Elections. The report assesses the magnitude of the problems, their root causes and how technology can reduce them. Here, the vote generation machine can be proprietary whereas the vote casting machine must be open-source and thoroughly verified and certified for correctness and security. Finally, the report provides a set of short-term and long-term recommendations on the various issues related to voting. They address a wide range of “What is” issues including voting procedures, voting equipment, voter registration, polling places, absentee and early voting, ballot security, cost and public finance of elections, etc. They then propose a novel “What could be” framework for voting technology and propose that a process for innovation be setup. The framework is “A Modular Voting Architecture [1] in which vote generation is performed separately from vote casting.

In “Electronic Voting” [2], Rivets addresses some issues like the “secure platform problem” and the (am) possibility of giving a receipt to the voter. Wide-scale attacks while voting from home, the need for extreme simplicity of voting equipment, the importance of audit-trails, support for disabled voters, security problems of absentee ballots, etc.

The NSF Internet Voting Report addresses the feasibility of different forms of Internet voting from both the technical and social science perspectives, and defines a research agenda to pursue if Internet voting is to be viable in the future. Internet voting is differentiating in three categories as follows:

### 2.1. Poll-site Internet voting

It provides greater convenience and efficiency in that voters could cast their ballots from any poll site, and the tallying process would be both fast and certain. More importantly, since election officials would control both the voting platform and the physical environment. Managing the security risks of such systems is feasible.

### 2.2. Kiosk voting

The voting platforms would still be under the control of election officials, and the physical environment could be modified as needed and monitored (e.g., by election officials, volunteers, or even cameras) to address security and privacy concerns, and prevent coercion or other forms of intervention. Voting machines would be located away from traditional polling places, in such convenient locations as malls, libraries, or schools.

### 2.3. Remote Internet voting

It seeks to maximize the convenience and access of the voters by enabling them to cast ballots from virtually any location that is Internet accessible. While this concept is attractive and offers significant benefits, it also poses substantial security risks and other concerns relative to civic culture.

## 3. EXISTING VOTING SYSTEM

In the existing voting system, the complete election process is divided constituency wise to facilitate the security forces and to make the election system fair. To maintain discipline and security requires a huge amount of man power so, it is bit difficult to accomplish election in a single day. Allocation of polls is done by election commission in advance. Generally polling booth is setup in school and community halls. The people can come to know about the location of voting. Time and place for voting is predefined. Each polling station is opened for at least 8 hours on the Election Day [4].

Shows first of all the voter need to reach at polling booth. The first step is the identity verification, carried out by an associated person on the duty. Then officer makes mark of inedible ink on the voter’s left forefinger thereafter voter has to sign in register followed by reaching inside the voting compartment. To mark a vote, a voter has to press blue candidate button on EVM machine against the name and symbol of his/her choice. When the button is pressed, the red lamp will glow against the symbol with beep sound which indicates that vote is successfully recorded [4]. Every time this process needs to be repeated as well as arrangement of building and manpower on the location of voting is required.

## 4. PROPOSED VOTING SYSTEM THROUGH SMART DEVICE

As the discussion begins with voting through mobile device, first an application is required through which voters can communicate. We need to use existing database in which voters information exist. Voters/citizens information is available in register database. Secure data centre is required to store and fetch the data as per requirement. Still there is a question of gathering voter's information. Assume that almost every next person is having mobile phone on which our application program will execute. [5].

After connection is established voters need to download application from a specific source. After downloading and installing, start the application. Once the application gets open it displays two options whether to create a new voter id or to vote with existing voter id.

### 4.1. Voting Through Existing Voter Id

To vote with existing voter id then we need to upload the photo which we had given while applying for voter id. The database contain the photo which we gave while applying the voter id. The uploaded photo will be send to the database to find and match the photo that is stored in the database. The database consists of voter photo and details. Once the database finds the exact match of the photo then the user is a valid voter. Then the details of the voter will be send from database to voter. Then the application displays list of candidates appear as per location which is fetched from register. From the list, voters can select any one candidate as per his/her choice then we need to give the email id or registered phone number for generating OTP. The OTP is send to the voter. After entering the OTP select the candidate and vote is accomplished. So, after selecting particular candidate counting is incremented by one centrally and another separate database is used to store count of votes. So, on this location only few persons (humans) are involved to carry out this process. So, as per Indian constitution it preserves secure ballot. If Voters do not have any smart device in such situation one common location is assigned for voting through mobile phones. After voting once we can't vote again since OTP will not be generated. The flowchart is given below in fig 4.1

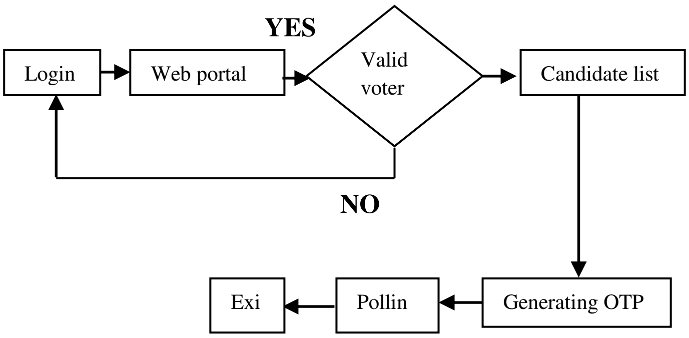

**Fig 4.1 Existing Voters System**

### 4.2. New Voter

The database does not contain the details about the person who is going to apply his/her first vote. Hence we need to enter the details of the voter into the database. The details are registered into the database by scanning QR code in the aadhaar card and also we need to upload the photo. Thus the details are registered in the database and it will send a voter id number to the voter. Then the application displays list of candidates appear as per location which is fetched from register. Then we need to give the email id or registered phone number for generating OTP .From the list, voters can select any one candidate as per his/her choice and after selecting the candidate voting is accomplished. So, after selecting particular candidate counting is incremented by one centrally and another separate database is used to store count of votes.

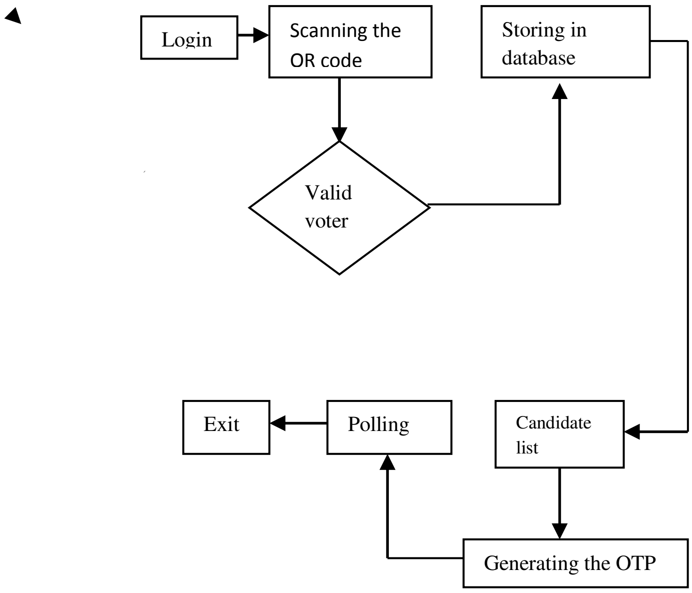

**Fig 4.2 New Voters System**

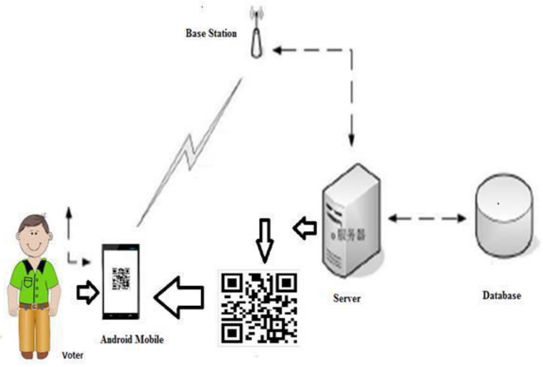

*Fig4.2.2 over View Of a system Architecture*

## 4.3 MOBILE AUTHENTICATION MODULE

This module represents the authentication, which is used for the voter to login their details for the voting processes. Logged voter is redirected to the scanner module. Authentication is used as the basis or authorization determining whether a privilege will be granted to a particular user or process. The validation process are done on the web server.

## 5. DISTRIBUTED SYSTEMS

Here the information about the voters, data of the candidate and the number of votes are stored by the means of the distributed systems. We follow the concept of distributed systems for avoiding traffic while accessing. Hence the servers will not get crashed. Hence the voters can easily access the data from the servers.

## 6. SERVER GENERATED OTP

Server-generated one-time passwords (OTPs) commonly are implemented as randomized password strings that are generated in real time after verifying simple-password credentials. Some more advanced implementations combine KBA elements to facilitate derived OTPs (such as server-generated grid cards for shared pattern recognition, digitally signed OTPs that are based on server-generated data, and so on). channel (out-of-band) from the session in the browser The generated OTPs then are delivered to users via a different, such as e-mail, SMS (Short Message Service) text messaging to mobile devices, direct phone calls that use computer-generated speech, and so on. Users then can use the OTP to sign-in to the application, by entering it into a designated field on the page. Christo Ananth et al. [3] discussed about a project, in this project an automatic meter reading system is designed using GSM Technology. The embedded micro controller is interfaced with the GSM Module. This setup is fitted in home. The energy meter is attached to the micro controller. This controller reads the data from the meter output and transfers that data to GSM Module through the serial port. The embedded micro controller has the knowledge of sending message to the system through the GSM module. Another system is placed in EB office, which is the authority office. When they send “unit request” to the microcontroller which is placed in home. Then the unit value is sent to the EB office PC through GSM module. According to the readings, the authority officer will send the information about the bill to the customer. If the customer doesn’t pay bill on-time, the power supply to the corresponding home power unit is cut, by sending the command through to the microcontroller. Once the payment of bill is done the power supply is given to the customer. Power management concept is introduced, in which during the restriction mode only limited amount of power supply can be used by the customer.

Many organizations in the public sector have started to deploy this type of solution to implement strong user authentication. This approach significantly improves authentication strength as it employs two-factor authentication and out-of-band delivery of OTPs.

## 7. QR – CODE SCANNER MODULE

This module is used to scan the QR-Code and read the value of the QR-Code inside the mobile. QR-Code is a matrix bar code designed to be read by Smartphone. The code contains of black modules arranged in a square pattern on a white background. The information encoded may be text, a URL, or other data. In this application we scan the QR code by a QR scanner so that the information about the candidate are perfectly stored in database without any errors.

## 8. CONCLUSION

Some of these advantages are lesser cost, faster Electronic voting systems have many advantages over the traditional way of voting. Tabulation of results, improved accessibility, greater accuracy, and lower risk of human and mechanical errors. Context QR codes can provide great value when used in situations that dynamically change depending on the context. Augmented reality is an interesting field for the application of this concept, as it enables user interaction with different technologies**.** It is very difficult to design ideal e-voting system which can allow security and privacy on the high level with no compromise. Future enhancements focused to design a system which can be easy to use and will provide security and privacy of votes on acceptable level by concentrating the authentication and processing section. The main purpose of implementing this concept is to increase the voting percentage. So that the voter is not required to visit the voting centre to cast their vote and also to avoid fake voting.

## REFERENCES

[1] Caine, D. Brunel, and L. Benin, "Distributed compressive sampling for lifetime optimization in dense wireless sensor networks," IEEE Trans. Ind. Inf., vol. 8, no. 1, pp. 30–40, 2012.

[2] J. M. Shapiro, "Embedded image coding using zero trees of wavelet coefficients," IEEE Trans. Signal Process., vol. 41, no. 12, pp. 3445–3462, Dec. 1993.

[3] Christo Ananth, Kanthimathi, Krishnammal, Jeyabala, Jothi Monika, Muthu Veni, "GSM Based Automatic Electricity Billing System", International Journal Of Advanced Research Trends In Engineering And Technology (IJARTET), Volume 2, Issue 7, July 2015, pp:16-21

[4] D.Wu, Y.T.Hou, Andy. Q. Zhang, "Transporting real-time video over the internet: Challenges and approaches," Proc. IEEE, vol. 88, no. 12, pp. 1855–1877, Dec. 2000.

[5] S. Jim, D. Kim, T. T.Nguyen,D. Kim, M. Kim, and J.W. Jeon, "Design and implementation of a pipelined data path for high-speed face detection using FPGA," IEEE Trans. Ind. Inf., vol. 8, no. 1, pp. 158–167, 2012.