ISSN:0975-9646

# Paradigm Shift in Voting - Secure Mobile Voting

Neha Kapoor[1], Rampur Srinath[2], Lokesh S[3], Rajesh N[4]

*[1]PG Student, Dept of PGSCEA, The National Institute of Engineering, Mysore, India. aroraneha_25@yahoo.com*

*[2]Associate Prof & Head, Dept of PGSCEA, The National Institute of Engineering, Mysore, India. rampursrinath@nie.ac.in*

*[3]Associate Prof & Head, Dept of CSE, The National Institute of Engineering, Mysore, India. lokesh.sl29@gmail.com*

*4Assistant Prof & Head, Dept of ISE, The National Institute of Engineering, Mysore, India. nrajeshin@gmail.com*

***Abstract*— In democratic society, voting is used to collect and reflect people's opinion and making a trusted and accepted committee of representatives for successfully running the country. Currently, voting is being conducted in centralized or distributed voting booths. Voters have to present personally at the voting booth to cast their votes under the supervision of authorized election commission members. For a variety of reasons, voters may not be able to attend voting booths physically but want to cast vote remotely. In this paper, we propose an solution through mobile voting. The proposed scheme is efficient and secure.**

***Keywords*— Mobile app, Voting, Security, Android App.**

## I. INTRODUCTION

As democracies across the globe are fighting challenges related to paper voting systems related to accessibility, scalability and cost associated with the polling process. In India, the world biggest democracy, the issues are more compounded given the terrain and hostile environment in some places. Devising a cost effective alternative which can be easily rolled out for masses has always been a point of interest for various researchers.

With the spread of telecom coverage in the country, Smartphone provide one of the viable alternatives to this problem. The paper focuses on an alternate secure voting systems using Smartphone that can well be incorporated into the current large-scale election process.

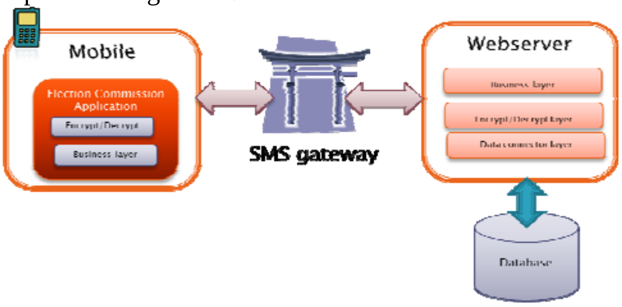
As the core element of representative democracy is the election, it is logical to say that mobile voting, which can be defined as voting via mobile devices, should be considered one of the most important drivers of mobile democracy. Although an exciting idea, various countries' experiences have proven that mobile voting has many issues that need to be solved before it can be utilized for large-scale elections. It is evident that social, legal, technical, and political problems may pose serious challenges against mobile voting.

Voting machines are the total combination of mechanical, electromechanical, or electronic equipment (including software, firmware, and documentation required to program control, and support equipment), that is used to define ballots; to cast and count votes; to report or display election results; and to maintain and produce any audit trail information.

## II. ARCHITECTURE

In cryptography, encryption is the process of encoding messages (or information) in such a way that eavesdroppers or hackers cannot read it, but that authorized parties can. In an encryption scheme, the message or information (referred to as plaintext) is encrypted using an encryption algorithm, turning it into an unreadable cipher text. This is usually done with the use of an encryption key, which specifies how the message is to be encoded. Any adversary that can see the cipher text should not be able to determine anything about the original message. An authorized party, however, is able to decode the cipher text using a decryption algorithm that usually requires a secret decryption key that adversaries do not have access to. For technical reasons, an encryption scheme usually needs a key-generation algorithm to randomly produce keys.

In the figure below the communication between mobile and election commission web application is through SMS, where encryption/decryption of message is done using Triple DES Algorithm.

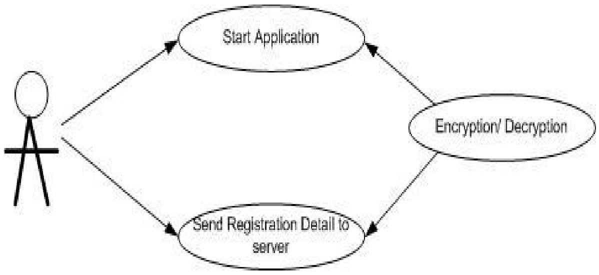


Triple DES Algorithm comes under the category of Symmetric Algorithm. When using symmetric algorithms, both parties share the same key for encryption and decryption. To provide privacy, this key needs to be kept secret. Once somebody else gets to know the key, it is not safe anymore. A few well-known examples are: DES, Triple-DES (3DES), IDEA, CAST5, BLOWFISH and TWOFISH.

Here during registration process the encryption and decryption of message is done using General Key. Once registration process is completed successfully the Election commission web application sends authenticated key to the mobile which is used further for encryption and decryption during voting process. The Web application maintains a database which maintains the details of contenders list, Authenticated secret key table, voter information and OTP (one time password table).

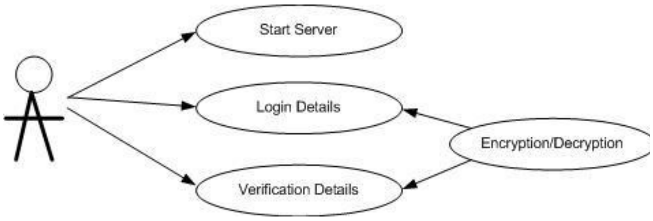
The use case of the system is shown below

*A. Registration Process*



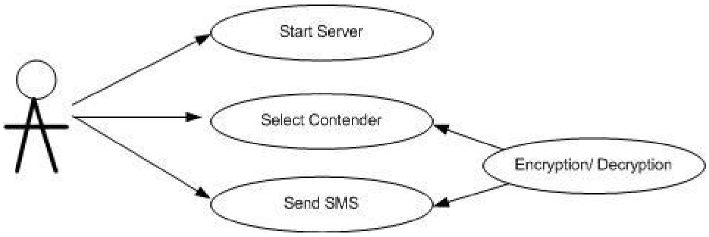
In registration process the user has to start the application and send registration details to the election commission. The user is presented with the Registration screen on launching the application. As a part of registration, the user is registered in the election commission database against the mobile number. On successful registration a mobile specific secret key is generated by the election commission and send back in encrypted format to the user. This key is updated in the mobile device of the user automatically.

B. Verification Process

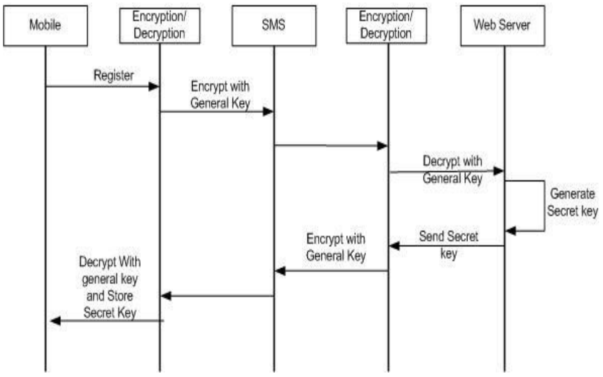


In verification process the user has to provide login details before casting vote. Once voting is initiated from the election commission office, user will be prompted to verify the correct the credentials first. The verification is based on User Mobile Number, DOB, OTP (only send to the user via registered letter) and unique Id (Aadhar Id). Once verified the next flow is triggered.

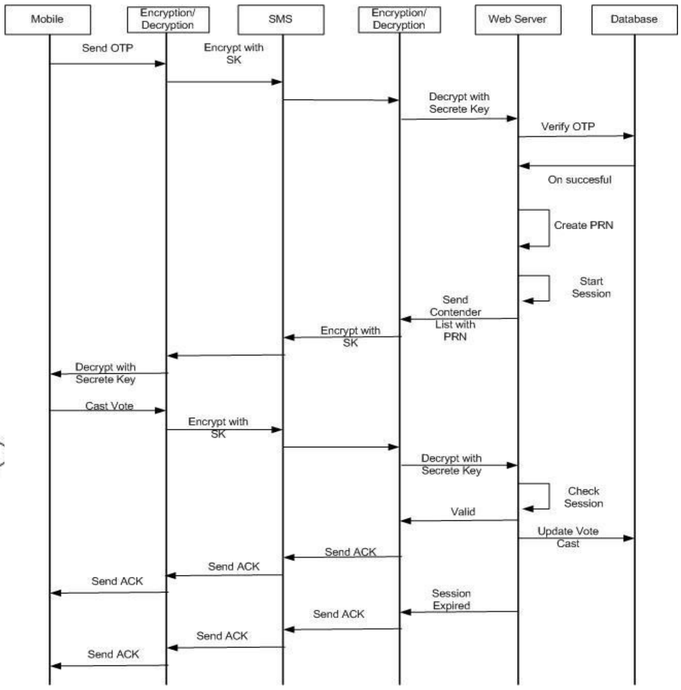
*C. Voting Process*



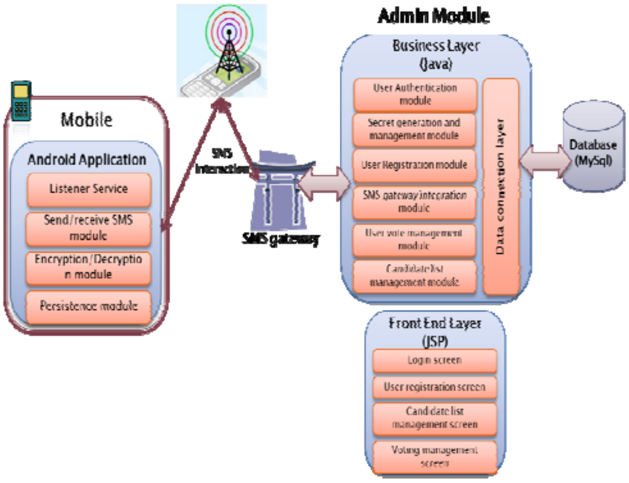
In voting process the user selects the contender and cast his vote. The screen is presented post the successful authentication/verification of user. The user can cast the vote which will be registered with the election commission.



**Registration process sequence**



Voting process sequence



Detail solution design

## III. Technology Stack Summary

*A. Programming language – Java*

*B. Mobile application development platform – Android*

*C. Web-application development – Java/JSP*

*D. Database – MySql*

## IV. Conclusion

Managing general elections and making sure to provide equal right to vote for all strata of society has inherently been an arduous tasks for the government. Governments traditionally utilized an open-source network (like postal ballot or mail in ballot) to supplement in-person voting. However, with the growth of telecom, Mobile Voting solution provides a strong alternative to traditional paper based balloting.

As a burgeoning technology, mobile voting is like any youngster, full of potential rather than accomplishments. The foremost consideration about mobile voting seems to be trust issues, not about the technology itself but rather the democratic culture of the country. This is where it is an absolute must to have a "secure and trustworthy" mobile voting and polling platform.

Mobile voting addresses issues confronting governmental elections at all levels of organizational voting as a new mobile option delivering significant benefits to current processes, including –

- Increasing voter participation in any election by offering the convenience of a secure and "virtual polling location"
- Enhancing accessibility for disabled, handicapped and elderly voters
- Reducing costs of printing, distributing and handling paper or absentee ballots
- Eliminating the fraud associated with absentee ballots
- Increasing transparency in the voting process
- Transitioning the investment in traditional voting machines to technology-based solutions employing readily available mobile smartphones and tablet devices.

## V. Enhancements

The following additional enhancement have been added during the course of design and implementation of the project

- Support for multiple people to use the same mobile for voting
- Implementation of additional One time password and delivery mechanism (postal delivery of security key) to ensure individual data integrity and privacy of the vote
- Encryption of SMS interaction (starting from the first SMS sent) to ensure secrecy of the data transmitted (complex encryption key combinations used to prevent hacking)

## VI. Limitations

- Android Service is used to asynchronously invoke the application on the Voting day. There is a risk if the user has re-started the phone post registration, this service may not be running
- The solution relies on the delivery of OTP to the enrolled people via post
- The solution relies on the availability of Android phones with OS version

## References

[1] Tandayoshi Kohno, Adam Stubblefield, Aviel D.Rubin, Dan S. Wallach (February 27,2004), "Analysis of an Electronic Voting System", pp 12-14

[2] Yang Feng, Siaw-Lynn Ng, Scarlet Schwiderski-Grosche ( June 26, 2006), "An Electronic Voting System Using GSM Mobile Technology", pp 2-3

[3] Hari K. Prasad, J.Alex Halderman, Rop Gongriijp, Scott Wolchok, Eric Wustrow, Arun Kankipati, Sai Krishnan Sakhamuri, Vasavya Yagati (April 29,2010) , "Security Analysis of India's Electronic Voting Machines"

[4] Manish Kumar, T.V. Suresh Kumar , M. Hanumanthappa, D Evangelin Geetha, "Secure Mobile Based Voting System", pp 324-326