International Journal of Electronics and Communication Engineering.
ISSN 0974-2166 Volume 8, Number 1 (2015), pp. 91-98

http://www.irphouse.com

# A Secure Smartphone Based Voting System with Modified EVM Using Elliptic Curve Cryptography

**Dhiraj P. Girase**

*STES' Smt. Kashibai Navale College of Engineering,*
*Savitribai Phule Pune University, Pune, India*

**Abstract**

The wide-spread use of mobile devices has made it possible to develop smartphone based voting system as a complement to the existing electronic voting system. Smartphone based voting system completely rules out the chance of invalid votes and its use results in reduction of polling time, increase in voting percentage.

In proposed voting system, both ways of voting are available i.e. Booth Voting using modified EVM (Electronic Voting Machine) and e-Voting using smartphones (Smartphone Based Voting System). In this system, booth voting can be done using modified EVMs and e-Voting through smartphones can be done using an android application. Both systems are connected to a common server, which maintains the list of voters and required database.

Both efficiency and security strength for smartphone based voting system are achieved by securing votes using the Elliptic Curve Cryptography (ECC) algorithm. ECC is chosen as it has smaller key size than other public key cryptographies and its homomorphic encryption property which is able to keep users' anonymity.

**Keywords** — android, ECC, EVM, smartphone based voting.

## I. INTRODUCTION

There are various systems available for voting such as Ballot Voting System, Electronic Voting Systems. These systems have some disadvantages such as time consumption during voting process, less percentage of voting, booth capture, inconvenience for migrated people (voter) etc. Since nobody likes to wait in line at the polling place, percentage of voting is less when using such type of voting systems. Hence there is need to develop an efficient system for voting which can provide

secure and easy way of voting complementary to existing system, so as to increase voting percentage.

For more than two decades, e-voting has been investigated. Despite its argument for and against [1], it is implemented in the real environment, either in a small or large scale, such as in Estonian public election [2].

On the other hand, smartphones have been widely used in India, whose number of subscribers has reached over 51 million in 2013 and expected to cross 104 million in 2014 [3]. Its popularity, flexibility and portability have inspired people to use it in various functions, not only as a voice exchanging tool, but also as a polling machine (e.g. vote a TV idol).

In general, e-voting systems must meet the principles and requirements for an election which include [4]:

- Confidentiality
- Anonymity
- Integrity

Due to its resource limitation, smartphone based voting system has more challenges than the common e-voting systems in terms of performance and security. In our smartphone based voting system, the data transferred from smartphone to the voting administrator is secured by elliptic curve cryptography (ECC) as it has more advantages than other public key cryptographies, in terms of key size, for instance.

Those factors are useful to meet the mobile devices' computing performance, the confidentiality, integrity and anonymity of the votes.

The rest of the paper is organized as follows. Section 2 reviews the related works and our contribution; section 3 provides the overall voting scheme and its analysis; section 4 contains the advantages of the proposed scheme and the last section 5 is the conclusion and future works.

## II. RELATED WORKS AND OUR CONTRIBUTION

Mobile voting system using elliptical curve cryptography was proposed in 2009[5]. In that system, the encryption scheme is too tedious and complex. Much more hardware is required to implement that scheme. Thus it is more complex for practical implementation. Also in that system, only mobile voting system is proposed. This would create problem if network fails. Not all the voters have smartphones. So an alternate way, such as Booth voting must be there for voting.

Thus the proposed system provides a combination of booth voting and smartphone based voting which provides a more convenient means of e-voting. In proposed smartphone based voting system, an android application is used to encrypt vote. A unique and relatively less complex algorithm is used in this scheme, such that users' identity and the vote are handled by separate machines.

The main idea behind this scheme is that, the administrator will only know about the voter's identity and not the vote casted by him/her. Similarly the counter will only know about the vote and not the voter's identity. In this way better security is achieved for smartphone based voting.

**A. System Overview**

The proposed system provides both means of voting i.e. Smartphone Based Voting and Booth Voting.

**1. Smartphone Based Voting System:**

It consists of a smartphone having android application for voting. Voters, who want to vote through smartphone, will have to download the Android application for voting from authorise website. Vote will be encrypted by the android application with certain predefined steps and sent to the mobile number provided by election authorities. On successful voting, voter will receive acknowledgement message.

**2. Booth Voting**

It can be done using modified version of Electronic Voting Machine (EVM). In this case, voter has to enter his Voter ID for casting vote. Rest of the process for Booth Voting is same as conventional system.

Both these systems are interfaced with a common server i.e. PC which will maintain all the electoral database including list of voters, voter ID, their mobile numbers, Voter ID Card (VIC) codes, passwords.

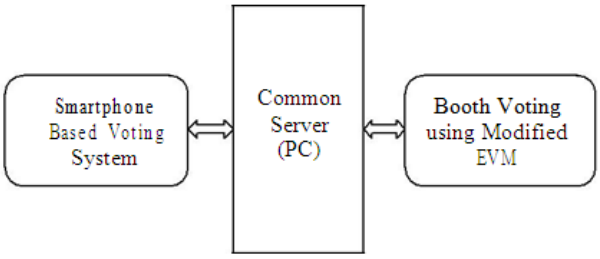


**Fig.1: Overview of Voting System**

**B. Block Diagram Description:**

As shown in figure 2, the block diagram consists of four modules:

**1. Smartphone and Android Application:**

- An android application will be developed, for encryption of voter's vote and password, with Elliptic Curve Cryptography algorithm.
- Voter has to enter his Voter ID and password in the application to cast vote.
- Application will encrypt the password and vote using encryption scheme.
- Then it will send this cipher text to the mobile number provided by Election Commission.

**2. GSM Module:**

- GSM module will be connected to the common server using RS232 serial bus.
- It will receive the cipher text sent from smartphone by the user.

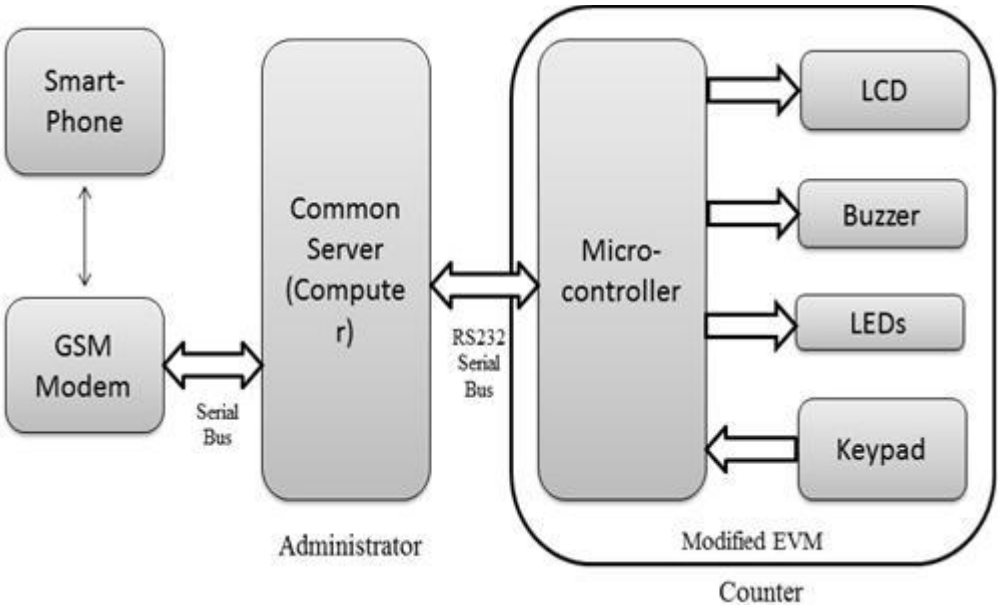


**Fig.2: Architectural Block Diagram**

**3. Administrator:**

- Administrator is nothing but a PC acting as a common server. It stores all the database of voters.
- The voter authentication will be done by administrator.

**4. Modified EVM or Counter:**

- The booth voting will be done using this module.
- Modified EVM will be consisting of...

– Microcontroller
– Keypad
– LCD, LED's
– Buzzer interfaced with microcontroller.

## III. PROPOSED SMARTPHONE BASED VOTING SCHEME AND ANALYSIS

After the text edit has been completed, the paper is ready for the template. Duplicate the template file by using the Save As command, and use the naming convention prescribed by your conference for the name of your paper. In this newly created file, highlight all of the contents and import your prepared text file. You are now ready to style your paper; use the scroll down window on the left of the MS Word Formatting toolbar. In general, a smartphone based voting system has some entities which are usually used in other electronic or mobile voting systems, like in [6, 7]. It can be described as in figure 1.

The entities include:

- User: who gives the vote
- Certificate authority: who gives the certificate to the user
- Administrator: who checks the users' eligibility
- Counter: who count the users' votes

For the election monitoring process and receiving complaints from entities involved, [6] adds an election commissioner (EC) in the scheme, in addition to the other entities. Before the election, EC will conduct process of registration or enrollment and authentication. At that time, each voter will be given a valid Voter ID, a password and a unique Voter Identification Card (VIC). Several code words will be printed on the VIC card. Each Voter ID will be linked with a mobile number provided by corresponding voter.

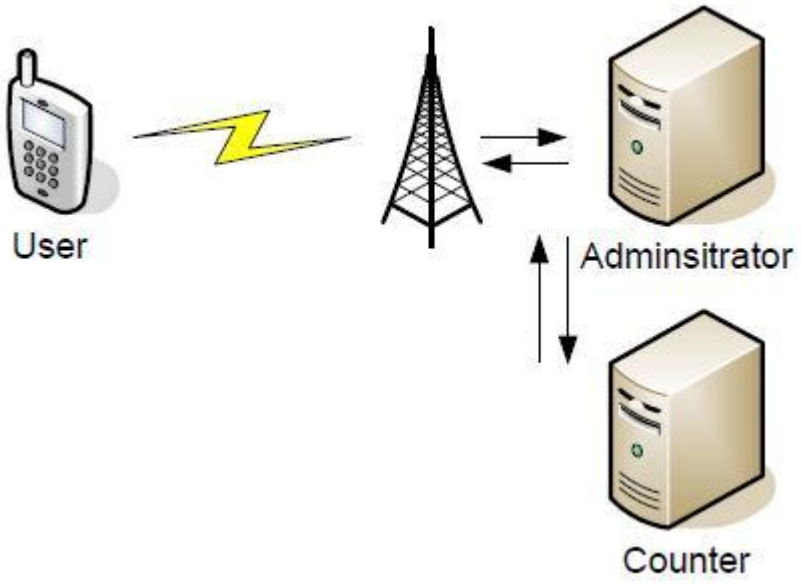


**Fig.3: Smartphone Based Voting Scheme**

Following Symbols are used:
Upri: User's Private Key (password),
Apub, Apri: Administrator's Public and Private Keys,
Cpub, Cpri: Counter's Public and Private Keys.

**Steps for Smartphone Based Voting:**

1. The voter will send his Voter ID to the Administrator.
2. Administrator will check its validity and checks whether voting has already been done from this Voter ID or not.

3. If both conditions satisfy, then it will ask the voter to send one of the combinations in the matrix on the VIC card provided to the voter.
4. The voter will send the corresponding code to the administrator.
5. Administrator will verify that code from its database and if verified, it will send the list of candidates to the user.
6. The voter then encrypts the vote using Android App. The process is as follows:

a. The vote will be first encrypted with the Counters' Public Key (Cpub)
b. This cipher text is then signed with the user's Private Key i.e. password (Upri).
c. This whole text will be encrypted again with the Administrator's Public Key (Apub). Encryption: Apub[[Cpub[Vote]] Upri]

7. This cipher text will be sent to the administrator. Once receiving the vote, the administrator checks its validity by decrypting the cipher text by using its Public Key (Apub) and Private Key (Apri). The Password part of the decrypted message is separated and it will be compared with that linked with the mobile number from which the SMS received.
8. If password is matched then list of the voters is updated to avoid votes from the same user. The remaining cipher text will be sent to the counter.
9. If password is exactly reverse of the original, then directly go to "step 12".
10. Counter will then decrypt that cypher text using its Public Key (Cpub) and Private Key (Cpri).
11. Counter will send acknowledgment to the administrator.
12. The administrator confirms the voting and forwards the acknowledgment to the user.

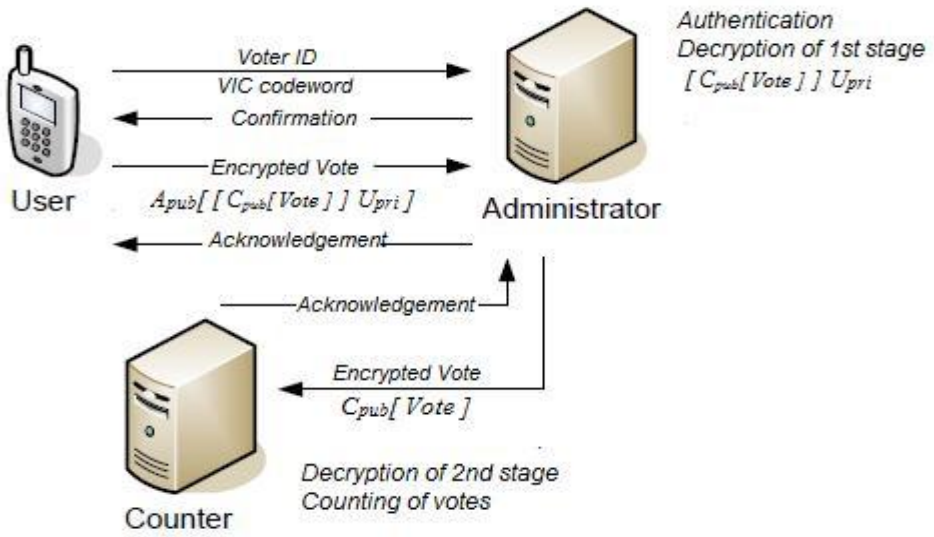


**Fig.4: Smartphone Based Voting Process**

**Steps for Booth Voting:**

1. Voter has to enter his voter ID using keypad.
2. The Modified EVM will send this voter ID to Common Server which will check its validity and checks that whether voting has already been done from this voter ID or not.
3. If not, then it will allow voter to cast his vote else not.
4. After successful voting, Administrator will confirm the voting and will update the list of voters.

The outputs of both these systems will be maintained on common server.

## IV. ADVANTAGES

By using this scheme for voting, we get various advantages as given below:

1. Increase in security of smartphone based voting. Three layer security is provided to the smartphone based voting system i.e. password protection, VIC code words and encryption with ECC.
2. Forceful voting through smartphone based system is prevented.
3. Less time consuming.
4. Android application is used, which increases feasibility, as most of the people use android OS smartphones.
5. Modified EVM has improvement in terms of security over conventional EVM.
6. It eliminates chances of dummy voting and multiple voting.

## V. CONCLUSIONS AND FUTURE SCOPE

### A. Conclusions

Following conclusions are drawn from above scheme:

After analysing conventional voting systems, an efficient and secure voting system is designed. Successful implementation of ECC algorithm for developing secure voting system is done. This system has improvements in terms of security, speed, accuracy, feasibility.

The system provides an alternate way of voting and reduces time required for voting resulting in the increase in voting percentage.

The android application is easy to operate, so that common man can easily cast his vote through it. For booth voting security is increased.

### B. Future Scope

Future improvements can be done in the work done above, which can enhance the security and voting percentage. In case of detection of forceful voting, it can inform to cops directly with a message containing location of the corresponding mobile device.

Complementary online voting system can also be introduced in this system by adding some extra features.

**REFERENCES**

[1] S. P. Everett, K. K. Greene, M. D. Byrne, D. S. Wallach, K. Derr, D. Sandler, and T. Torous, "Electronic voting machines versus traditional methods: improved preference, similar performance, " Proc. the twentysixth annual SIGCHI conference on Human factors in computing systems, ACM, April 2008.

[2] A. H. Trechsel and F. Breuer, "Voting: E-voting in the 2005 local elections in Estonia and the broader impact for future e-voting projects, " Proc. the 2006 international conference on Digital government research, ACM, 2006, pp. 40-41.

[3] BuddeComm, "Global - Mobile - Subscriber Statistics, " [on-line] accessed on April 13, 2009 from http://www.budde.com.au/.

[4] B. I. Simidchieva, M. S. Marzilli, L. A. Clarke, and L. J. Osterweil, "Specifying and verifying requirements for election processes, " Proc. the 2008 international conference on Digital government research, Digital Government Society of North America, 2008.

[5] Tohari Ahmad, Jiankun Hu, Song Han, "An Efficient Mobile Voting System Security Scheme based on Elliptic Curve Cryptography", 2009 Third International Conference on Network and System Security.

[6] NIST, "Recommended Elliptic Curves for Federal Government Use, " [on-line] accessed on April 14, 2009, from http://csrc.nist.gov/, NIST, 1999.

[7] X. Yi, P. Cerone, and Y. Zhang, "Secure Electronic Voting for Mobile Communications, " Proc. Vehicular Technology Conference, vol. 2, 2006.

[8] www.google.com

[9] www.wikipedia.com