E-Voting System on Android Platform

Prof. Rahul Patil
Department of Computer Engineering
Bharati Vidyapeeth,
College of Engineering,
Navi Mumbai.

Pritam Bhor
Department of Computer Engineering,
Bharati Vidyapeeth
College of Engineering,
Navi Mumbai.

George Ebenez
Department of Computer Engineering,
Bharati Vidyapeeth
College of Engineering,
Navi Mumbai.

Ashish Rasal
Department of Computer Engineering,
Bharati Vidyapeeth
College of Engineering,
Navi Mumbai.

Abstract: **The advancement in the mobile devices, wireless and web technologies has given rise to the new application that has made people perform most of their activities in a direct, electronically automated, and efficient way, and hence has also made the voting process very easy and efficient. The e-voting system promises the possibility of convenient, easy and safe way to cast vote and make the vote count in an election. This paper provides the specification and requirements for E-Voting using an Android platform. We propose a novel system for E-voting using android, in our project the voter will have to enter their unique Voter ID. The system makes use of OTP for validation of the user. Later on, the vote along with the Voter ID will be encrypted using Blind signature based on RSA. These details will be stored in the database in encrypted format.**

I. INTRODUCTION

Voting for any social issue is essential for modern democratic societies now a day. So it is becoming very important to make the voting process more easy and efficient. In other hand the rapid development in operating system of the mobile phones gives rise to the application development on the large scale. The main reason behind the tremendous development in android application development is that the android is an open source operating system. It means that the software developers can have customization rights. As well as the software development kit provides tools to build and run android applications.Security and accuracy are the first and foremost requirements for any voting system. Hence, EVS should satisfy at least the following security requirements which are described in[1,2,3]:

- Eligibility: only authorized voters who satisfy predetermined criterion can vote.
- Uniqueness: no one can vote more than once.
- Privacy: a vote is kept secret and no one can determine for whom anyone else voted,
- Integrity: election process is secure so no one can change anyone else's vote without being discovered. In addition no one can duplicate anyone else's vote.
- Accuracy: every voter can make sure that his vote has been taken into account in the final tabulation.

European countries already madeexperiences with e-voting. Mentionable experiments took place in Switzerland, the United Kingdom and the Netherlands, whereby the systems used by these experiments are considerably different. Common to all of them is to support voters with a new convenient way to participate in elections. [5]

Existing e-voting systems include Direct-recording electronic (DRE) voting system in which a (DRE) voting machine records votes by means of a ballot display provided with mechanical or electro-optical components that can be activated by the voter (typically buttons or a touchscreen); that processes data with computer software; and that records voting data and ballot images in memory components. After the election it produces a tabulation of the voting data stored in a removable memory component and as printed copy. The system may also provide a means for transmitting individual ballots or vote totals to a central location for consolidating and reporting results from precincts at the central location. These systems use a precinct count method that tabulates ballots at the polling place. They typically tabulate ballots as they are cast and print the results after the close of polling.

Another existing E-Voting system is based on RFID (radio frequency identification) to identify voter. If the voter is valid the candidate list will be shown to the voter.

E-Voting system based on biometrics uses special hardware which consists of either a fingerprint scanner or retina scanner. The identification of voter is done by this hardware. Then theVoter can vote for any one candidate of his choice.

Disadvantage of the existing systems:

- Old systems were rigid hence they were oflittle use.
- Hardware modules were required.
- No robust technology.
- Earlier systems were desktop based hence there was no ubiquitous solution for on the fly voting.
- Hardware failure was a real risk.

II. RELEVANT SECURITY TOOLS

For a e-voting system maintaining confidentiality of the data is very important, following cryptographic techniques will be very useful for such a system:

1. Blind Signature using RSA
2. Homomorphic encryption

Let us look into each of these tools in detail

1. Blind Signature using RSA

Blind signature schemes, first introduced by Chaum, allow a person to get a message signed by another party without revealing any information about the message to the other party. The blind signature's particular characteristic that neither the signers do not know the content of the message to be signed, nor the signatures that the recipients obtain for their message. This kind of signatures is used in scenarios where the signer and the message creator are different entities.

In this technique the registrar, who has the authority to sign, has a set (n, d, e) based on RSA key scheme. He chooses a random number k where $1< k \leq n$. The voter blinds his ballot m to get blind ballot B where

$$B = (mk^e) \bmod n \quad ....(1)$$

where e is the public key.

The blinded ballot B is signed by an authority person with a private key d to get signed ballot S where

$$S = B^d = (mk^e)^d \bmod n = (md^k) \bmod n \quad ....(2)$$

The signed ballot is unblinded by dividing it over k

$$UB = S^{k-1} = m^d \bmod n \quad ....(3)$$

2. Homomorphic Encryption

Homomorphic encryption is a form of encryption which allows specific types of computations to be carried out on ciphertext and generate an encrypted result which, when decrypted, matches the result of operations performed on the plaintext.

$$D(E(m_1, r_1).(E(m_2, r_2) \bmod n^2) = m_1 + m_2 \bmod n$$

The Paillier cryptosystem, named after and invented by Pascal Paillier in 1999, is a probabilistic asymmetric algorithm for public key cryptography. The scheme is an additive homomorphic cryptosystem It is an algebraic property that allows to apply mathematical operations on sets of encrypted ballots without need of decrypting them which improves privacy. For example, in additive homomorphic encryption, the product of two ciphertexts is a third ciphertext that encrypts the sum of the two original plaintexts. Paillier algorithm is one of the homomorphic cryptosystem which is widely used in most voting systems.

The Pallier cryptosystem works as follows [4]

- Key generation:

In this step both the public keys (n, g) and private keys (μ) are generated.

Choose two large prime numbers p and q
where,
gcd (pq, (p–1) (q–1)) =1
Compute $n = p \times q$ and $\lambda = lcm (p-1, q-1)$
where,
$\lambda = (p-1)(q-1) / gcd ((p-1)(q-1))$
Select random integer g
where,
$gcd [((g^\lambda \bmod n^2 - 1)/ n), n] = 1$
Compute $\mu = (L(g^\lambda \bmod n^2))^{-1} \bmod n$
where, $L(u) = (u-1) / n$

- Encryption

Select a random number r
C (ciphertext) $= g^m r^n \bmod n^2$
where,
m is the plain message.

- Decryption

m (plaintext) $= L(c^\lambda \bmod n^2) . \mu \bmod n$

III. PROPOSED SYSTEM

Our proposed system will adopt Android phone as voting machine for the voter which will collect the vote and sends it to the Central Tabulation Facility (CTF).The workflow of the system is depicted in fig. 1.

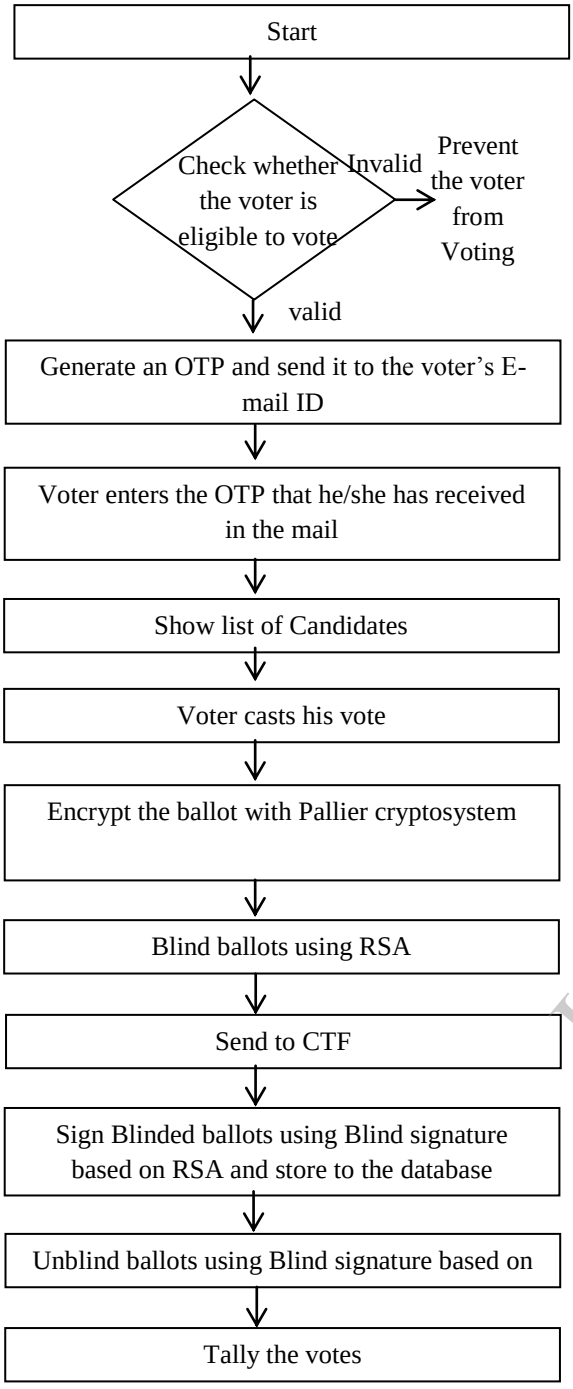

Fig. 1: The Proposed system

Our project will function in following phases: Validation and Authentication phase, Voting phase, Encryption and transmission phase, Decryption and counting phase. We will be discussing each phase in detail in the following section:

A. Validation and Authentication phase

The voter will use his device on which the E-voting application will be installed. Using this device, the voter will enter his voter ID, which will be sent to the server or the CTF as a request to cast his/ her vote.

Now, the CTF maintains the database of voter details and also a database of voters who have already voted. The CTF will check whether the voter has already voted; if yes, the voter will not be allowed to vote again. If the voter has not voted before, the CTF will check the validity of voter. If the voter is a valid voter the an One Time Password (OTP) will be generated by the CTF using the voter ID and the timestamp. This OTP will be sent to the voter's E-Mail address that has already been registered in the database. When the voter receives this OTP he can use it to log into the system to cast their vote.

B. Voting phase

After logging in, the user enters the Voting phase, which is perhaps the most important part of this system. A list of candidates will be displayed on the screen of the voter's device. The user can select any of the candidates and further confirm their vote for the candidate. Now as the voter casts his vote a ballot is created.

C. Encryption and transmission phase

If a voter casts his vote his ballot will be constructed by storing a prime number representing vote YES in a cell intersects with the selected nominee while the rest L-1 cells have another prime number that represents vote NO [4]. This will be further encrypted or blinded using RSA and transmitted to the CTF. At CTF, blind signature based on RSA will take place, now this is done if we have multiple CTFs and we need to transmit the ballots to the Central Counting Facility. The blind signature enables the Central Counting Facility to understand that the ballots are authenticated ones.

D. Decryption and counting phase

Counting phase involves unblinding of ballots and use of additive property of Pallier cryptosystem to tally the votes. The unblinded ballots can be represented as follows:

TABLE I: TABLE OF UNBLINDED BALLOTS

Prime No. Representing Yes Vote=5, No Vote=7

	Candidate 1	Candidate 2	Candidate 3
Voter1	5	7	7
Voter2	5	7	7
Voter3	7	5	7

The counting of votes can be done easily using a simple formula:

$n = (y - Nr_2) / (r_2 - r_1)$

where,

r_2 is the prime number representing "Vote No."

r_1 is the prime number representing "Vote Yes".

n is the number of "Vote Yes" for each nominee.

N is the total no. of ballots

y is the decryption result of each nominee.

For example, we can calculate Yes votes for Candidate2 using the formula:

$n = (y – Nr_2) / (r_2 – r_1)$
n=(19-(3x7))/(7-5)= 1 vote

TABLE I. RESULT TABLE

	Candidate1	Candidate2	Candidate3
Yes Vote	2	1	0
No Vote	1	2	3

IV. CONCLUSION

In this paper, we have presented a new E-voting system , that enables 'on the fly' voting. The paper facilitates the use of modern mobile platform to provide this service to the users.The project implements a client running on mobile device of the user and CTF server. We have used OTP, Blind signature based on RSA and Pallier cryptosystem. Our attempt has been to design an E-Voting system that fulfills the philosophy of Uniqueness, Secrecy, Privacy and Integrity

V. REFERENCES

1. Amir Omidi and MohammadAbdollahiAzgomi, ''An Architecture for E-Voting Systems Based on Dependable Web Services'', Innovations in Information Technology, 2009. IIT '09, pp. 200 – 204,Dec. 2009.
2. Mohsen Rezvani, S. M. HosseinHamidi, "MIZAN: A Secure E-voting Schema with Vote Changeability",Information Society (i-Society), 2010 International Conference, June 2010, pp. 548 – 552.
3. Gina Gallegos-García, Roberto Gómez-Cárdenas, Gonzalo I. Duchén-Sánchez, "Identity based Threshold Cryptography and Blind Signatures For Electronic Voting", WSEAS Transactions on Computers archive, Volume 9 Issue 1, January 2010, pp. 62-71
4. HanadyHussien, HussienAboelnaga, "Design of a Secured E-Voting System"Computer Applications Technology (ICCAT), 2013 International Conference, Jan. 2013, pp. 1 – 5
5. Thomas Rössler, Herbert Leitold and ReinhardPosch, 'E-Voting: A Scalable Approach using XML and Hardware Security Modules' The 2005 IEEEInternational Conference on e-Technology, e-Commerce and e-Service, pp. 480 – 485, 2005.