A Novel in E-voting in Egypt

DR.MOHAMED ABO-RIZKA, HEBA REFAAT GHOUNAIM

Department of Computer Science
Arab academy for science and technology
Cairo-Egypt

Summary
Election is fundamental instruments of democracy that provide an official mechanism for people to convey their views to their government by democratic means. E-voting becomes the most important application in e-government and e-democracy. Now days, some countries start to test and use electronic voting system, advantage like quick tallies, the possibility for remote reduction are among the main reason for it, however there are some problem need to be solved.
Many e-voting schemes have been proposed and claim simplicity and added security.
Some of these systems used and implemented by government, the most famous one is the DRE system. There is a list of security requirements that constitutes a must for voting, and without these requirements, fraud and corruption may occur: confidentiality, integrity, authentication, and verifiability. Unfortunately no e-voting schemes have proved to be secure enough. By using electronic voting, cheating, bribe and, coercion will be reduced and provide more security, unlike conventional voting systems, the voter can choose any voting booth that is safe to him/her.
In this paper I will discover my scheme the (EVSE) Electronic Voting System in Egypt, this scheme designed to be fitting for the environment and the conditions in Egypt, trying to solve problems in the old system, conventional system.

Key words:
E-voting, Biometric smart token, EVSE system

1. Introduction

The essence of democracy is to allow people to vote freely so the result of the election must be accepted by the voters; electronic voting is a technology that used to support the citizen to participate in democratic decision making, electronic voting is used mainly to support the anonymous voting, by provide the security to the voter so no one can know he/she was vote to.
There is a list of security requirements needs for voting, and without these requirements, fraud and corruption may exist: confidentiality, integrity, authentication, and verifiability. Secure e-voting scheme must also satisfy completeness, privacy, unreusability, eligibility, fairness, robustness, and also receipt- freeness and uncoercibility. Conventional voting exhibits a great deal of potential weaknesses. There is an inherent possibility of cheating; as the system doesn't provide sufficient anonymity, tampering with the results during and after voting may take place, and finally the possibility of bribing voters by candidates is possible. Furthermore, the time taken to count the votes is far too long.
Many improvements have been proposed and indeed tried over the years, such as the Mechanical Lever Machine and the Computer-Assisted Counting but they were not completely foolproof.
DREs (direct recording electronic systems) are the first completely computerized voting system, it was introduced in 1970s. The popularity of DREs, especially the touch screen, has grown in recent years, many governments devote billions to enhance e-voting, and HAVA (Help America Vote Act) authorized $ 3.65 billions over four years to replace the punch card system and the lever machine system and to apply other administrative improvements.

1.1 Requirement of E-voting:

The requirement in conventional voting (paper vote) are also apply for e-voting, the requirements can expected to be universal, any system must try to apply these requirements:

Free election: the citizen must be able to vote without being coerced by the government to vote for certain candidate. The vote must be reach the election authority without the chance of manipulation.
Secret voting: no one can know the vote of another person, by protecting the vote form being attack by another third party.
Equal voting right: each vote must have the same weight. No vote must become invalid by predictable technical problems or must be lost on its way to the voting authority. Also, the right to vote must not be made dependent on factors other than those enumerated in the Law (e.g., a criminal conviction).
Reliability: the process of the voting system must work robustly, so no vote are lost, even if failure occur like loose of internet connection.
Flexibility: the system should be configurable for many different election scenarios (like different ballot question formats or multiple languages etc.) and on a technical

Manuscript received November 5, 2007
Manuscript revised November 20, 2007

level compatible with multiple operation system platforms as well.
Uniqueness: No voter should be able to vote more than once.
Integrity: votes as such should not be modifiable, forged or deleted without detection and the possibility to repair the manipulation.
Convenience: election systems should not require extra skills to be usable and without unreasonable need for equipment.

2. Voting in Eqypt:

Voting in Egypt is like any other country; most of countries still using the conventional voting technique in government election, but now Egyptian government think to electronic voting system rather that conventional voting to avoid the problems they faced on it.

There is a lot of problem in conventional voting in Egypt:

1- There is no good relationship between the government and popular, popular can't trust the government and depend on it, voter here is like a blind person that must rely on the other person to vote for him.
2- Sometimes, government coerced and carries on the voters to vote for a particular candidate, and eliminate them from voting freely.
3- Some candidates trying to win by buy the votes from the voters.
4- Government can cheat by substitute the original ballot by derivative ones.

So there must be another way to solve these problems or reduce it as possible, and give the voters the confidence to believe of the system, form this point we think to use a new technology to improve the election by building a new system that is convenience for environment of our country Egypt. Depending on the other research on the E-Voting scheme and the implemented system that is already used in the government election like the DREs (Direct Recording Electronic Voting system) which is the most famous implemented system, we build here a scheme called EVSE (Electronic Voting System in Egypt).

3. EVSE (Electronic Voting System in Egypt):

Before talking about the EVSE scheme we need to define the biometric token and the feature of it, and why we use it in our system, and how can it be useful for the voters in the election.

3.2 Requirement of E-voting:

In e-voting, smart token is used as a storage media to store the information of the voters, card holders, other personal data and the identification number and unique number (token).
But why smart token, why it is the best for e-voting? Because it is a temporarily store media, and an anonymous media, which provide a secure way to save the information of the card holders.
In EVSE system we will use biometric with smart token and we will use the finger print as a template, to verify the voter in the election.
The voter present his token to the to the poll machine, and then put his finger on the finger print sensor, if the presented finger print matches the finger print templates in smart token, the voter will be verified for the system.
With the Match-On-Card technology the fingerprint is verified inside the secure environment of the Smart token. In this case the fingerprint template stored on the Smart token cannot be extracted. It can only be used internally by the Smart Card itself. Signing contracts or documents is only one application where the biometric verification in Smart token can be used. Other applications might be for example ID cards, where the user proves the validity and ownership of the ID card by biometric verification.[10].

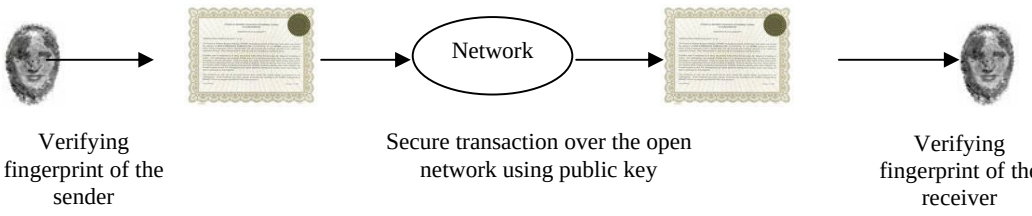

Fig 1: The figure shows an example of the usage of fingerprints for verification.
The fingerprint is used to verify the ownership of the smart token, to be able to use the cryptographic keys for digital signatures and encryption.

But how fingerprint template generated, there are three basic elements to create the template,

- Enrollment.
- Templates.
- Matching.

Enrollment is the process of collecting biometric sample (fingerprint sample) from the person to generate template. The device takes number of sample of fingerprint and averages them to generate template. Templates are the data representing a sample from the enrollment process. The small size of the templates allows it to be easy stores on smart token. Matching is the process of comparing a submitted biometric sample against one (verification) or many (identification) templates in the system's database.

4. The hierarchal of the system:

First, we will consider the e-voting process and discuss the possibility to build a system suitable for use in Egypt. Then we examine the hierarchal of such a system.

This figure describes the hierarchal of the e-voting system and the voting process itself. The system offers a certain degree of flexibility and convenience to the voter to ensure a maximum contribution in the democratic process. If the voter is registered for voting in a particular constituency, e.g. ALX but works in another, e.g. Agouza, then he/she can vote in the Agouza polling station near his/her work place. However, he/she will only have access to the Ballot Server of ALX to participate in the local election of his/her constituency.

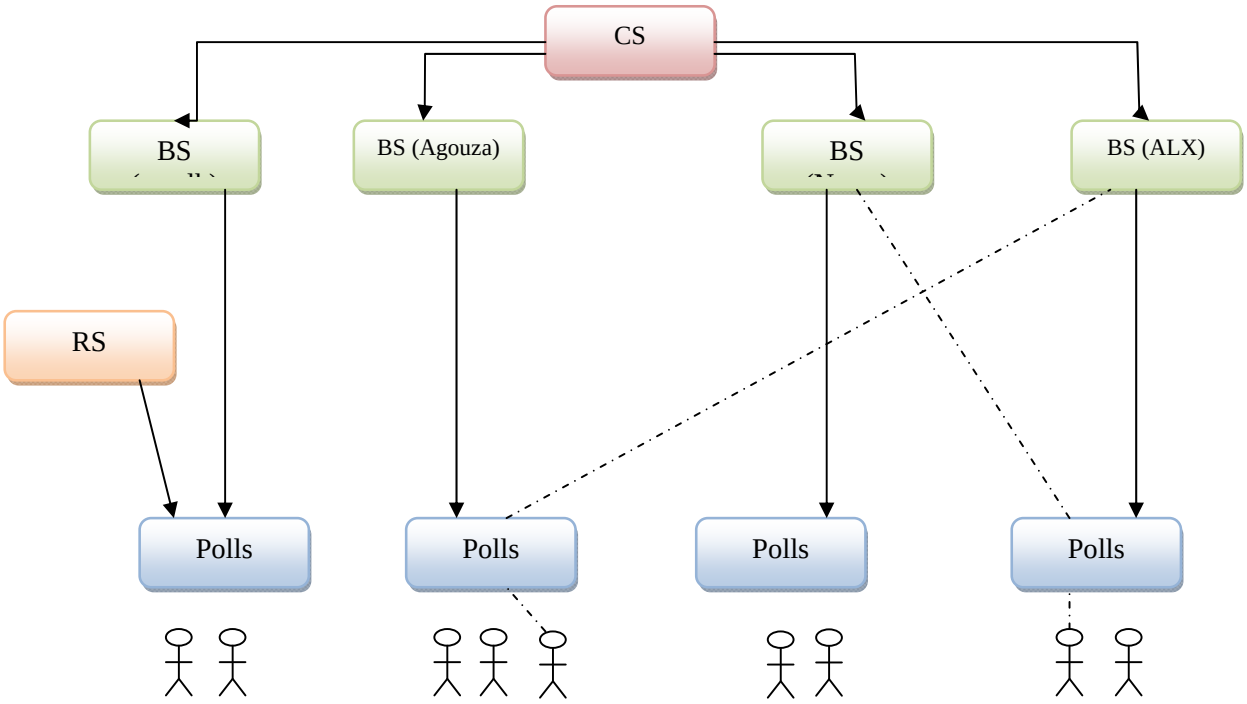

Fig 2

5. The hierarchal of the system:

5.1 System Design:

The frame work used for modeling analysis and construction of electronic voting system (EVSE) extends the Unified Modeling Language (UML) to model EVSE.

Figure 3 illustrate the use case diagram, which describe what system does from the standpoint of external observer, the emphases in on what a system does than how.

Figure 4 illustrate the proposed model in a collaborative diagram, which represent the first phase in electronic voting system (Registration phase), figure 5 will represent (Voting Phase), figure 6 will represent (checker phase) which is the last phase in the election.

Figure 7, 8, 9 illustrate the sequence diagram of EVSE system which is used to model interaction within the system, which presents the interactions and the sequence of events between the voters and the servers.

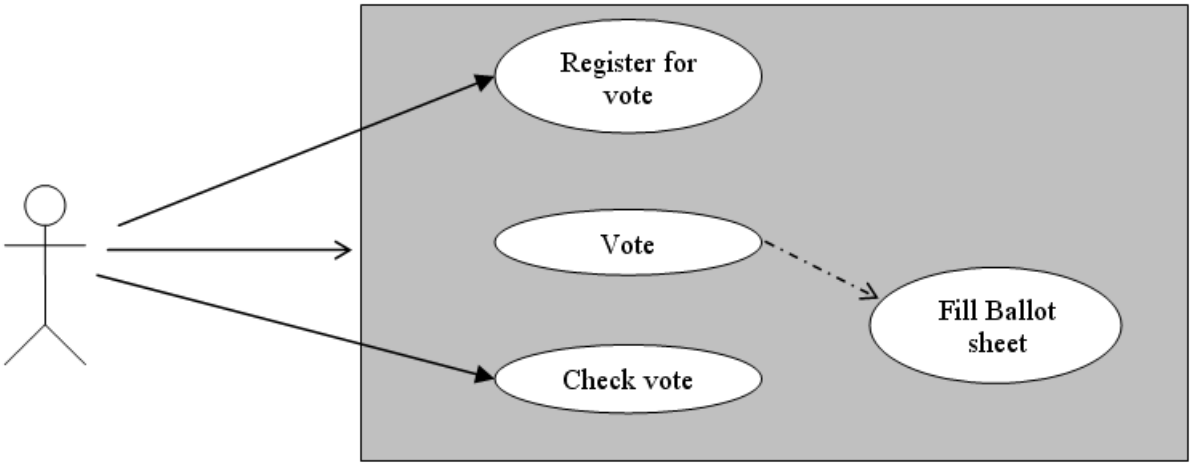

Fig 3 Use Case of voting system

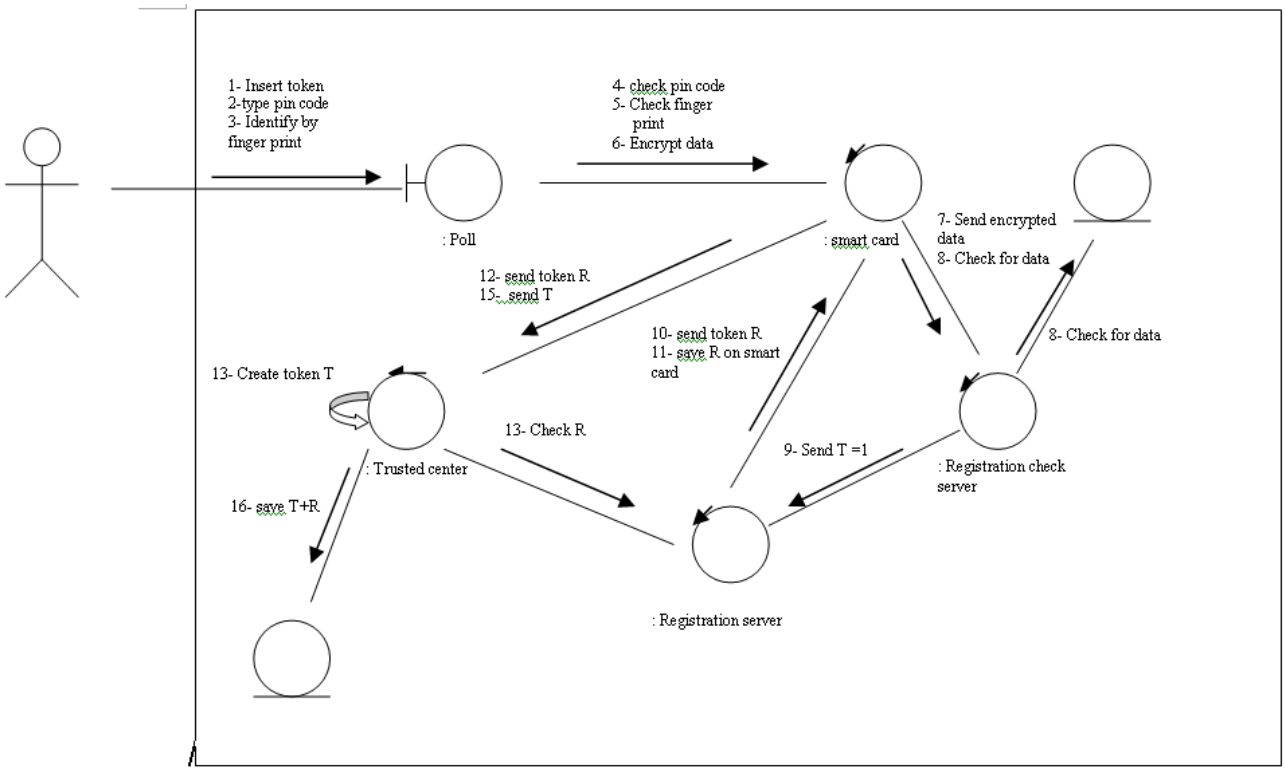

Fig 4 collaborative diagram for registration phase

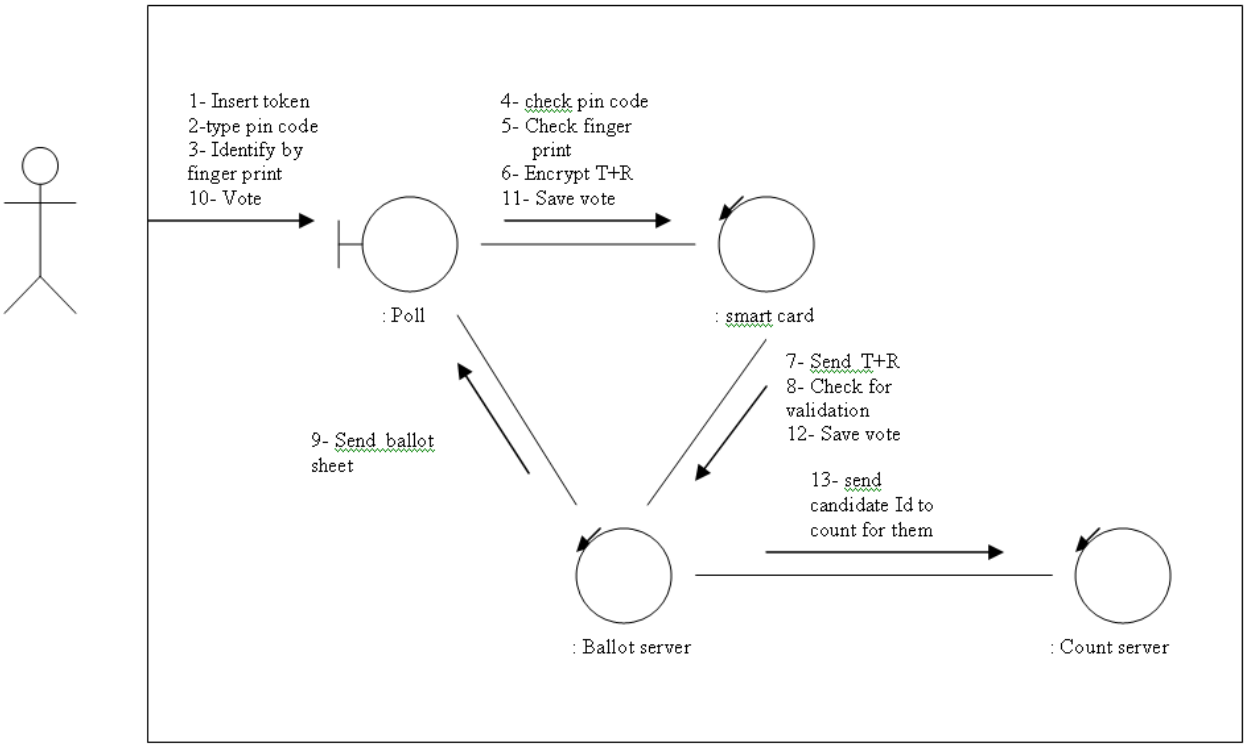

Fig 5 collaborative diagram for voting phase

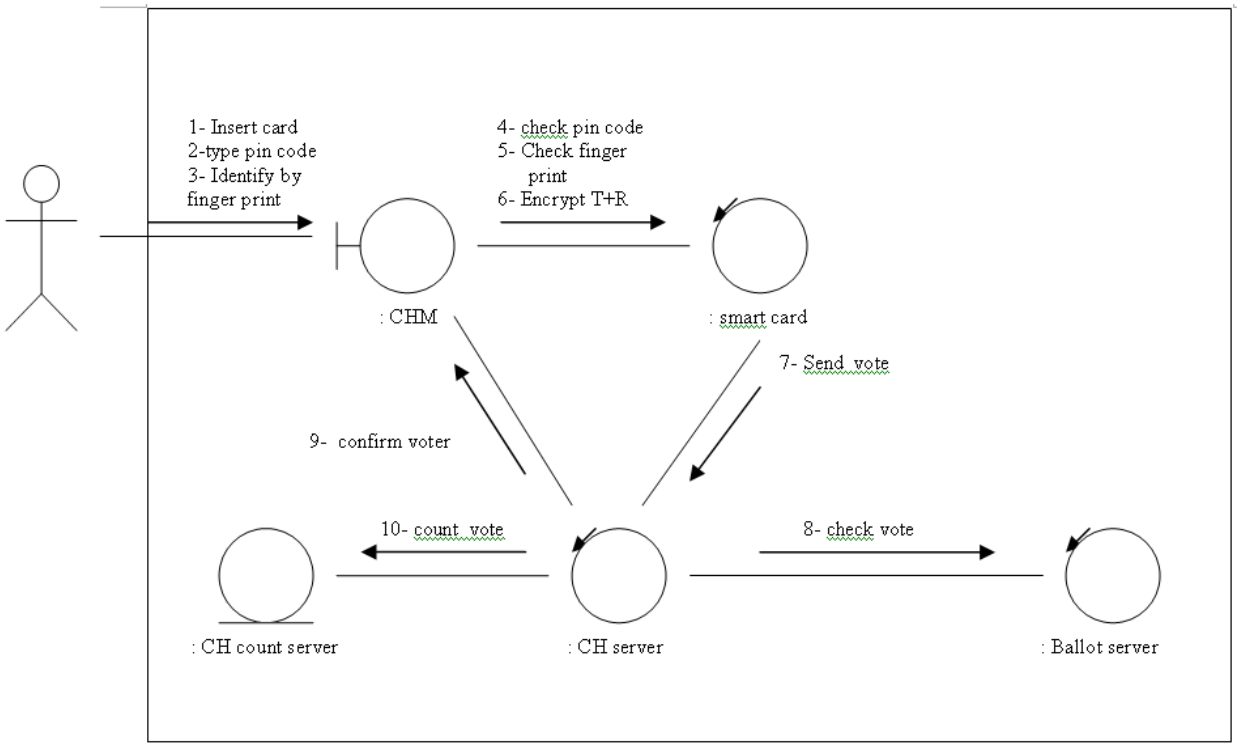

Figure 6 collaborative diagram for checker phase

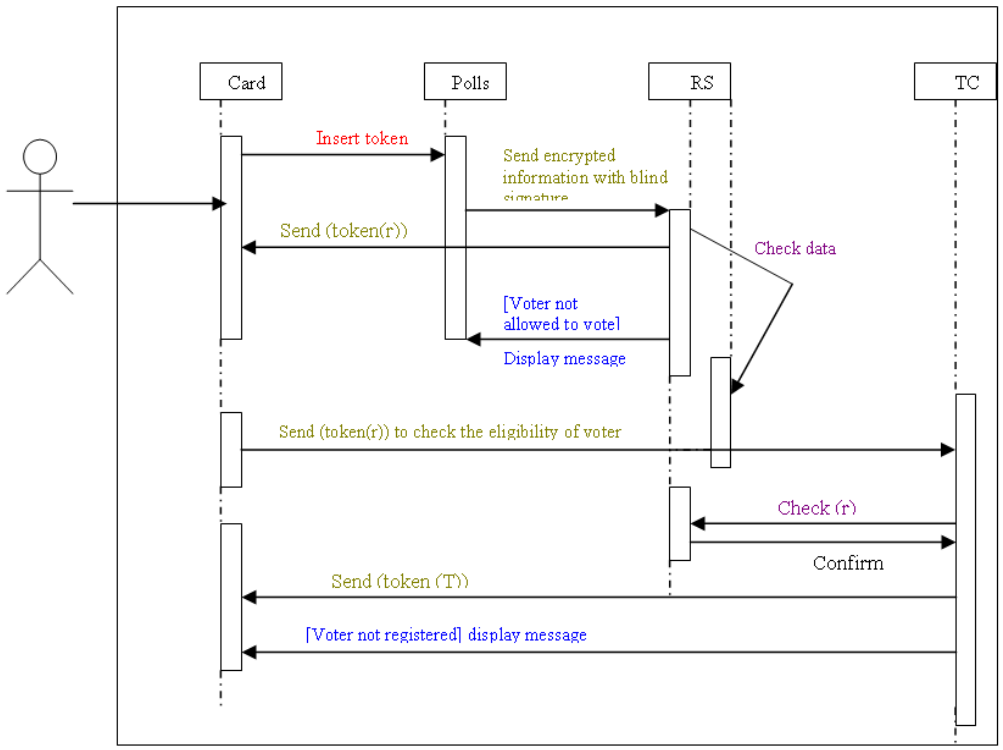

Figure 7 sequence diagram for registration phase

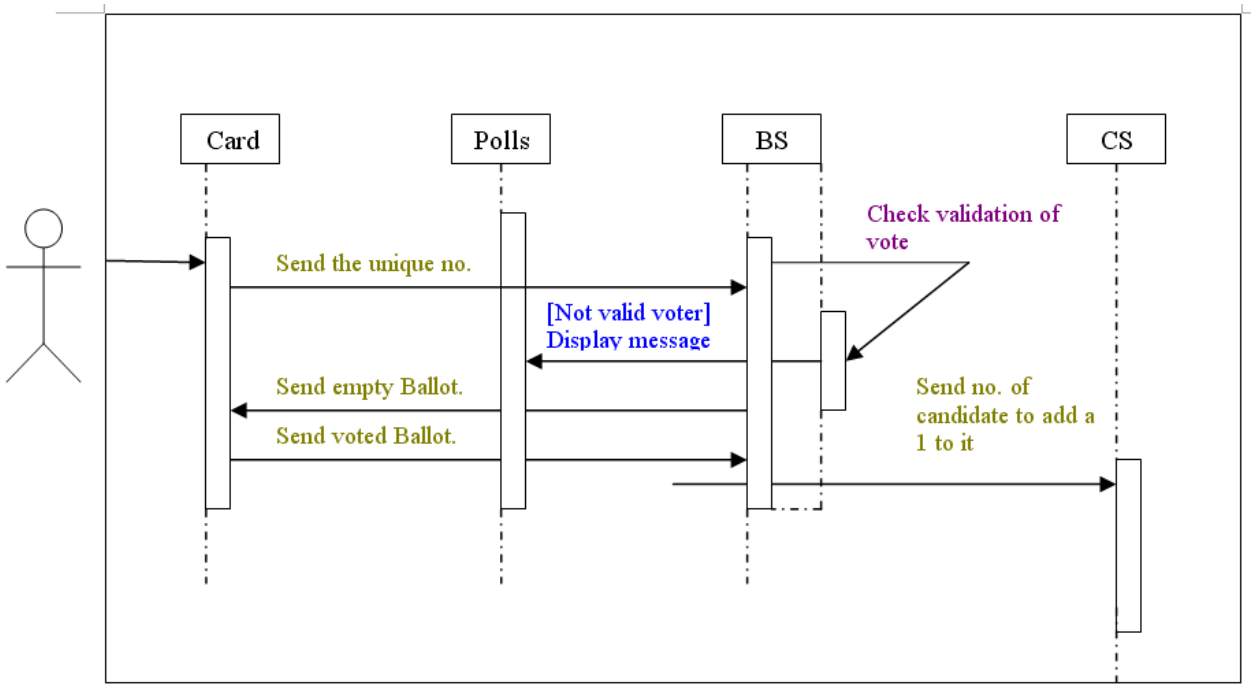

Figure 8 sequence diagram for voting phase

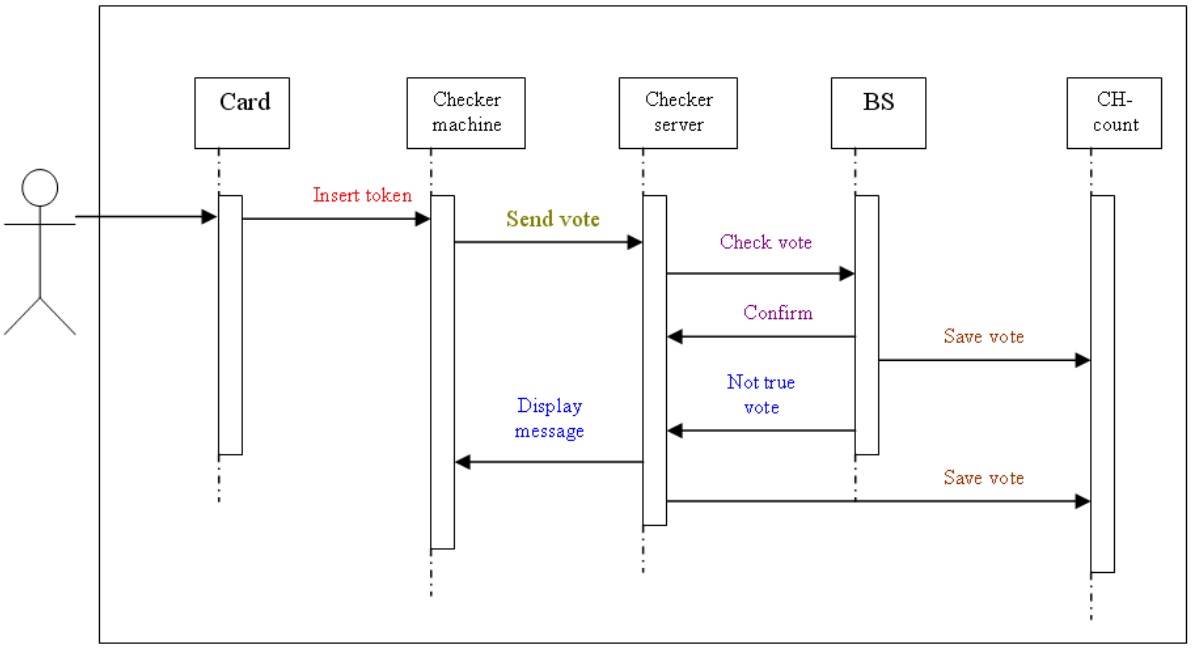

Figure 9 sequence diagram for checker phase

6. Chaum's Electronic coins scheme

Blind signatures were proposed by Chaum in *Untraceable Electronic Cash* as a technique realizes untraceable electronic coins. The scheme relies on the bank creating a number system where only it can compute cube roots. A coin that Alice would want to spend starts off as a number *x* that acts like a serial number for a bill. The number *x* is a 100-digit number that Alice chooses at random, so there is very low probability someone else will pick the same serial number. [24].

This serial number needs to be digitally signed by the bank so that the bank will later recognize it as currency that someone was authorized to spend. However, in order to protect her anonymity, Alice will multiply *x* by the cube of another random number, *r*3. [24]

This extra random number is called the *blinding factor* because it "hides" the value of *x* from the bank. This blinding factor, according to Chaum, is unconditionally untraceable to Alice: "Even if the bank had infinite computing power, they couldn't find out because it contains just as much *r* information as *[x]* information.

Each coin is a pair (x, $f(x)$ 1/3 (mod n)) where f is a one-way function and n is some composite whose factorization is known only to the bank (Chaum88 319). Since only the bank knows the factorization of n, only it can compute cube roots modulo n, so the cube root acts as a digital signature from the bank. The basic coin issuing and spending protocol described in *Untraceable Electronic Cash* is:

1. Alice chooses a random x and r, and supplies the bank with $B = r3f(x)$ (mod n).
2. The bank returns the third root of B modulo n: $r * f(x)$ 1/3 (mod n) and withdraws one dollar from her account.
3. Alice extracts $C = f(x)$ 1/3 (mod n) from B [by dividing by the blinding factor r].
4. To pay Bob one dollar, Alice gives him the pair (x, $f(x)$ 1/3 (mod n)).
5. Bob immediately calls the bank, verifying that this electronic coin has not already been deposited. [25]

7. Preventing double voting

After registration in Registration Sever (RS) and Trust Center (TC), the RS and TC send tokens (R, T) to the voter's smart token. Then the two token will be combined to generate a token x, through using of XOR, this digit number x will be multiply by the cube of a random number r.

This extra random number is called blinding factoring because it hide from the RS and ballot Server (BS) and it generate a unique number no one know about, voter will use it to vote. Even if anyone tries to know about it, they couldn't because they do not have any information about ' r' or about 'x'.
Each voter has (x , $f(x)$ 1/3 (mod n), Where f is one way function and n is some composite factorization is known only to the voter.

1- Voter will generate a random number x and r, uq = $r3f(x)$ (mod n)
2- The Smart Token will return the third root of uq modulo n: $r * f(x)$ 1/3 (mod n)
3 – Then ST will extract C = $f(x)$ 1/3 (mod n) [By dividing by the blinding factor r]
4- The C will be encrypted using the private key of the voter, and start to send this code to the ballot server.
5- The BS, will receive the token and decrypt the message it's receive form the voter, and start to check if the voter can vote by make a comparison between the tokens in the TC and the tokens in smart token.
6- If the BS confident the tokens are true, BS will encrypt the ballot sheet using the private key of BS and send it to the voter.
7- The voter will decrypt the ballot sheet by the public key ballot server and start to fill the sheet.
8- Then the voter will send his/her vote with his/her unique number.

8. Security analysis:

In this section, we will show that this scheme is secure; and satisfies the following crucial criteria: completeness, privacy, unreusability, eligibility, fairness, robustness, receipt-freeness, and uncoercibility.

Completeness: all ballots are counted correctly and fully in an e-voting scheme.
Since the independent agency double checks the results on the voting server to those on the checker server by counting the ballots in the checker count server, then are making a comparison between CHS and CS, so the probability of incorrect count will be reduced.
Privacy: all ballots are secret.
Since the ballot server transmits encrypted ballots to the smart card via a public key and this ballot can decrypted only by the smart card while still in the card reader. In addition, the vote is sent back to BS encrypted using a private key.
Unreusabaility: no voter can vote twice.
When the voter casts his vote the BS retains the ballot plus the voting unique number for the period of the election, to prevent the voter from voting more than once.
Eligibility: only eligible voter can vote.
No one can vote without going through the correct procedure for registration to obtain the token from RS, so if the voter does not register, he/she cannot vote.
Fairness: no one can know the result of the voting process, before announcement of it.
After the voting, if any one try to know the result will not be able to know it, there must be a permission from the government to broadcast the result.
Robustness: no voter can disrupt the voting process.
Receipt-freeness: ensures that the voter can be convinced that his/her ballot is counted without getting a receipt. Through checker server the voter can be sure that vote was taken and saved correctly in BS (Ballot server) and it's counted by CS (count server). This electronic method minimizes the possibility of bribes and is environmentally friendly by making a paperless process.
Uncoercibility: no voter will be coerced to casting for particular candidate.
The only way to coerce voters is to know the content of the ballot sheet, and because there is no receipt, no one can know which candidate voter vote to, so there is no coerce.

References

[1] Jeremy M. Sharp, Middle East Policy Analyst, Foreign Affairs, *Defense, and Trade Division: Egypt: 2005 Presidential and Parliamentary Elections***,** CRS Report for Congress, September 21, 2005

[2] http://news.bbc.co.uk/1/hi/world/middle_east/4417204.stm.
[3] Kenneth Clark: *Can E-Voting Software Be Secured To Ensure the Accuracy of the Election*?, 21st Computer Science Seminar.
[4] Songini, Marc L.. ComputerWorld: *E-voting May Face Recall in Florida County*. April 18, 2005.
[5] Schultz, Eugene: Computers and security: *E-voting in recent US election gets mixed in reviews*. Feb2005.
[6] Rothke, Ben. eWeek: *E-voting: it's security stupid*. August 23, 2004
[7] A SSP LITRONIC White Paper: *introduction to smart card*
[8] http://www.smartcardalliance.org/alliance_activities/identity_faq.cfm
[9] Chapter two: *A PRIMER ON BIOMETRIC TECHNOLOGY*
[10] Magnus Pettersson, Mºarten Ä Obrink: *Ensuring integrity with fingerprint verification*. Precise Biometrics AB, Dag HammarskjÄolds vÄag 2, SE 224 67 Lund, Sweden. 16th November 2001.
[11] Robert Kofler, Robert Krimmer, Alexander Prosser1, *Electronic Voting: Algorithmic and Implementation Issues*. Department Production Management, Vienna University for Business Administration and Economics. 2002
[12] http://people.cs.uct.ac.za/~flifson/things/security/node8.html
[13] Sonia Arrison and Vince Vasquez. *Upgrading America's Ballot Box:The Rise of E-Voting.*2005
[14] Wei-Chi Ku and Chum-Ming Ho: Department of computer science and information engineering, Fu Jen Catholic University, Taipei, Taiwan: *An e-Voting scheme with improved resistance to Bribe and coercion*.
[15] http://www.calvec.org/site/c.9dJDLJNkGkF/b.1120043/k.AF53/HAVA.htm
[16] http://guidelines.kennesaw.edu/vvsg/vg1/v1ad.htm
[17] Eric A. Fischer, and KEvin J. Coleman- CRS Report For Congress: *The Direct Recording Electronic Voting Machine (DRE) Conterversy* :FAQ and Misperceptions. December 2005
[18] Eric A. Fisher- CRS Report For Congress: *Election Reform and Electronic Voting System (DREs): Analysis of Security Issues*. NOV 2003
[19] http://odl-skopje.etf.ukim.edu.mk/uml-help/html/02day12.html
[20] http://www.agilemodeling.com/artifacts/sequenceDiagram.htm