Secured and Transparent Computerized Voting System accessible everywhere

Enas Elbarbary [1], Ghada Abdelhady [2], Hussam Elbehiery [3], Abdelhahim Zekry [4]

[1]VACSERA, Department of Electrical Engineering, Egypt
[2]Ahram Canadian University (ACU), Faculty of Computer Science and Information Technology, Egypt
[3]Misr University for Science and Technology (MUST), Faculty of Information Technology, Egypt
[4]Ain Shams University, Faculty of Engineering, Egypt
Hussam.elbehiery@gmail.com

Abstract: Aiding the user to have secured voting system is a must. Early regular voting systems have many drawbacks like the overcrowding of people in the polling stations and hence the traffic problems. The need for great amount of documents that are vulnerable, exposed to forgery, also the difficulty of achieving votes counting, analysis are considered as drawbacks for regular voting systems. This work presents a new smart system for voting process to be secured and transparent. We will call it "Secured and Transparent Computerized Voting system (STCVS)". "STCVS" system could eliminate counterfeiting, hacking. Also, while accessing it from any location, this would save the time spent for voting processes and countries economic performance would be better. Finally, "STCVS" system assures that user's vote will be his own opinion, not influenced by any others.
[Enas Elbarbary, Ghada Abdelhady, Hussam Elbehiery, Abdelhahim Zekry. **Secured and Transparent Computerized Voting System accessible everywhere.** *J Am Sci* 2014;10(1):151-157]. (ISSN: 1545-1003). http://www.jofamericanscience.org. 24

Keywords: E-Voting; Cryptography; Asymmetric Encryption; Elgamal; PHP; Javascript; MySQL

1. Introduction

Secured and Transparent Computerized Voting system (STCVS) is characterized by the use of computerized devices for voting procedures, votes counting and analysis. Compared to paper based ballots, its advantages are the faster, flexible, cost effective and accessibility suitable ballot procedures. Also, traditional polling stations using electronic equipments has an extra cost for the voting equipments and the voting process is supervised through government representatives.[1,8&9]

This is not required in case of using "STCVS" system as all voters use their own computerized communicator devices (smart phone, PC, laptop, tablet, etc…) and can even be abroad at the moment of voting.

In this research paper, we introduce an approach for implementing computerized voting concept in a secured, verifiable manner via the Internet. [10&11]

This is achieved by combining Elgamal cryptography algorithm with hash-based data structures. Voters can get verifying their own vote by receiving a feedback from the proposed computerized voting system. Feedback is an acknowledgement SMS sent to the voter's registered cell-phone.

The reliability of the introduced voting system against attacks is an important aspect to be considered. To eliminate the risk of attacks, voting data is encrypted from the client-side and along all channels. [14,15&17]

Elgamal encryption algorithm used for our proposed "STCVS" system had not been broken. Some internet voting systems use RSA (Ronald Rivest, Adi Shamir and Leonard Adleman) cryptosystem that had been broken, hence the later system is attacked. [3&18]

Also, recent electronic voting systems require the presence of huge number of electronic voting machines. This would definitely increase the voting system cost. Using special electronic voting machines is not required for our proposed "STCVS" system. [2,8&13]

2. Cryptography

Cryptography is the science of using mathematics to encrypt and decrypt data. Cryptography enables you to store sensitive information or transmit it across insecure networks (like the Internet) so that it cannot be read by anyone except the intended recipient. So, Cryptography is the science of secret writing with the goal of hiding the meaning of a message. [4]

Asymmetric encryption is a form of cryptosystem in which encryption and decryption are performed using the different keys, one is a public key and another is a private key. It is also known as public-key encryption. Asymmetric encryption transforms plaintext into ciphertext using a one of two keys and an encryption algorithm. Using the paired key and a decryption algorithm, the plaintext is recovered from the ciphertext. Asymmetric encryption can be used for confidentiality, authentication, or

both. Public-key algorithms are based on mathematical functions rather than on substitution and permutation, much of the theory of public-key cryptosystems is based on number theory. [5]

Modern symmetric algorithms such as (AES or 3DES) are very secured, fast and are in widespread use. However, there are several shortcomings associated with symmetric-key schemes, as discussed below:

1) Key Distribution Problem:

The key must be established between Sender and Recipient using a secured channel. The communication link for the message is not secured, so sending the key over the channel directly which would be the most convenient way of transporting it can't be done.

2) Number of Keys:

Even if we solve the key distribution problem, we must potentially deal with a very large number of keys. If each pair of users needs a separate pair of keys in a network with "n" users, there are "n(n−1)/2" key pairs, and every user has to store "n−1" keys securely.

3) No Protection against Cheating by "Sender or Recipient":

Sender and Recipient have the same capabilities, since they possess the same key. As a consequence, symmetric cryptography cannot be used for applications where we would like to prevent cheating by either of them as opposed to cheating by an outsider hacker. For instance, in e-commerce applications it is often important to prove that the sender actually sent a certain message, say, an online order for a flat screen TV. If we only use symmetric cryptography and the sender changes his mind later, he can always claim the recipient, the vendor, has falsely generated the electronic purchase order.

Also, since we need to get the decryption key (secret key) available only with the recipient ("Higher Committee for Elections" and the "Human Rights Association" in our work), so we used the asymmetric encryption. [16]

2.1 Asymmetric encryption:

The are many asymmetric encryption algorithms, we will discuss them as follow:

RSA Cryptosystem is a protocol used for both encryption and digital signatures. It was developed by Rivest, Shamir, and Adleman and uses the multiplication of large prime numbers for encryption. It uses a large key space. Thus, the larger the number of bits, the better. However, because the calculations involved, both in key generation and in encryption/decryption, are complex, the larger the size of the key, the slower the system will run. We need to be careful in choosing a key size for RSA. For the near future, a key size in the range of "1024 to 2048 bits" seems reasonable. Finally, RSA algorithm is also already broken. So, the move to a different algorithm resulted in a tremendous speedup and more security. [6]

Diffie-Hellman is a key exchange protocol used for generating and securely exchanging symmetric encryption keys. It should be noted that a protocol that uses the basic version of the DHKE is not secured against active attacks. This means if an attacker, can either modify messages or generate false messages, he can defeat the protocol. This is called man-in-the-middle attack. [7]

ElGamal algorithm can be viewed as an extension of the DHKE protocol. The protocol consists of two phases, the classical DHKE which is followed by the message encryption and decryption. In contrast to the DHKE, no trusted third party is needed to choose a prime and primitive element. The recipient generates them and makes them public, by placing them in a database or on his website. The actual Elgamal encryption protocol rearranges the sequence of operations from the Diffie–Hellman inspired approach. The reason for this is that the sender has to send only one message to the destination, as opposed to two messages in the earlier protocol. It is important to note that, unlike the schoolbook version of the RSA scheme, Elgamal is a probabilistic encryption scheme, i.e., encrypting two identical messages does not yield two identical cipher texts. [4&5]

ECC (Elliptic Curve Cryptography) is an approach to cryptography that uses a finite set of values within an elliptic curve (an algebraic set of numbers). Elliptic curve cryptography is a more efficient algorithm than other asymmetric algorithms (for example, a key size of "60 –bit" is equivalent to a "1024-bit" key used with RSA). Elliptic curve methods have been deployed for encryption, digital signatures, and key exchange. ECC provides the same level of security as RSA or discrete logarithm systems with considerably shorter operands (approximately "160–256 Bits" versus "1024–3072" Bits). ECC is based on the generalized discrete logarithm problem, and thus Discrete Logarithm (DL) protocols such as the Diffie–Hellman key exchange can also be realized using elliptic curves. In many cases, ECC has performance advantages (fewer computations) and band-width advantages (shorter signatures and keys) over RSA and Discrete Logarithm (DL) schemes. However, RSA operations which involve short public keys are still much faster than ECC operations. [19]

Elgamal Digital Signature Scheme is similar to the case of RSA digital signatures, it is also possible that an attacker generates a valid signature

for a random message. The attacker impersonates the recipient. The native Elgamal signature algorithm is rarely used in practice. Instead, a much more popular variant is used, known as the Digital Signature Algorithm (DSA). It is a federal US government standard for digital signatures (DSS). Its main advantages over the Elgamal signature scheme are that the signature is only "320 Bits" long and that some of the attacks that can threaten the Elgamal scheme are not applicable. DSA standard has a bit length of "1024 Bits". Longer bit lengths are also possible in the standard. [6&7]

Elliptic curves have several advantages over RSA and over DL schemes like Elgamal or DSA. In particular, in absence of strong attacks against elliptic curve cryptosystems (ECC), bit lengths in the range of "160–256 Bits" can be chosen which provide security equivalent to "1024–3072 Bits" RSA and DL schemes. The shorter bit length of ECC often results in shorter processing time and in shorter signatures. For these reasons, the Elliptic Curve Digital Signature Algorithm (ECDSA) was standardized. [12][16][19]

3. Elgamal Algorithm (Suggested Algorithm)

From the previous sections, we suggested Elgamal Encryption scheme for our "STCVS" work for the following reasons:

1) It is an effective algorithm, still not attacked (broken) "RSA is already broken".
2) It do not need large memory "as EC to deal with longer keys", so could be compatible with the most of the devices used for E-Voting and also with the use of a database. Also, it would allow lower system cost.
3) It do not share a private key, i.e. exchanging symmetric encryption keys "as Diffie-Helmann", since we have to apply public-key algorithm, so encryption would be done by a public key, while decryption would be done by private key (available with the Higher Committee for elections, Human Rights Association).
4) It could save the processing time because it is a somewhat simple algorithm "compared with the EC which would be too complex with many calculations".
   This could be important for our system to get a fast response (online acknowledgement SMS for the voting process).

Elgamal algorithm steps are described as shown in "Figure 1". A prime number is randomly generated with the value (10^6 to 10^7) via the host server "Supervision Site". Primitive root is also randomly generated.

Private (Secret) key is an assumption owned by the host server. Public key would be calculated by the host server knowing the prime number, the primitive root and the private key. Public key would be automatically changed per vote.

Cipher texts (encrypted voting data) would be calculated by the host server also via several calculations using many randomly generated constants.

Encryption is done using "Javascript", so voting data would be sent encrypted from the client-side (voter device) and along the entire path till reaching the server-side (supervision site "host server"). Thus, voting data fraud would be eliminated.

Decryption would be done by several calculations made on the server-side using "PHP" to recover the voting data.

Hence, the voting data would be available only with the supervision site ("Higher Committee for Elections" and the "Human Rights Association") that would be the owner of the host server for the proposed "STCVS" proposed system.

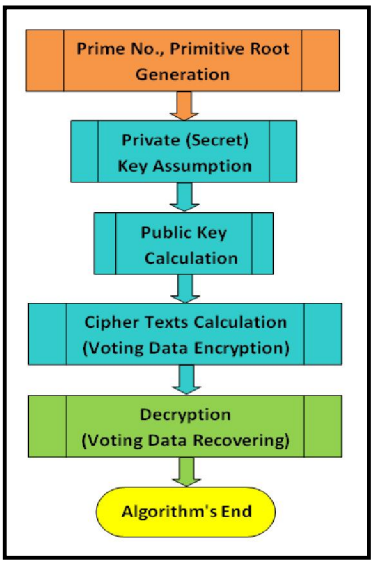

Figure 1. Elgamal Algorithm Flow Chart

4. Suggested Computerized Voting System Structure

"Figure 2" illustrates the way to achieve a secured computerized voting: In the "Start Stage". The user (Voter) would access the suggested computerized Voting system website using a smart phone, laptop, PC, tablet or any computerized communicator device. He would enter his full-name, pass-code as stored in the voting database to access voting.

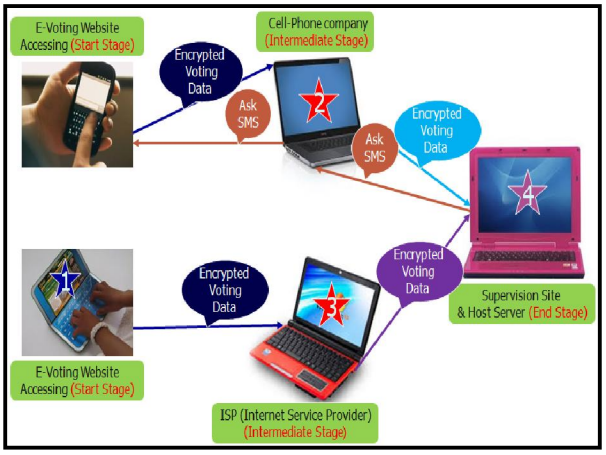

Figure 2. STCVS Block Diagram

"Voting Data" will be encrypted using "Asymmetric Encryption Algorithm" (Public-Key) to prevent its attack while being sent from any computerized communicator device via (cell-phone company / ISP) "Intermediate Stage" to the Host Server (Supervision Site) "End Stage". The later will be the ("Higher Committee for Elections" and the "Human Rights Association" in our work). As we stated in section "1", it will decrypt the voting data using (Private-Key).

The user should get a feedback (acknowledgement SMS) from the (supervision site) on his registered cell-phone. This is regardless of using which computerized communicator device for the voting process.

(Vote Attack) could not be achieved since the voter pass-code is used once, it would be expired after each election, and so, it could not be used by another voter or by the same voter for a next election.

Finally, "voting duplication" would not be allowed since the user could achieve voting once only using this proposed system.

5. Methodology of STCVS

5.1 STCVS Use Case Diagram

As shown in "Figure 3", the use case diagram shows the interactions for the voter, supervisor (administrator) for each use in the "STCVS" system. The voter has firstly to login to the voting website successfully, then he could choose the candidates numbers. He gets a confirmation message (acknowledgement SMS) sent from the website to his registered cell-phone. The message is composed of his selected voting data.

The supervisor (website administrator) has more rights. He would login to the website, he could update the candidates numbers in the voting webpages for each new election. Vote's analysis, results charts are also controlled and could be shown by the supervisor. Adding voters and saving their data to the database is the supervisor's responsibility. Finally, a confirmation message is sent automatically by the host server owned by the supervisor.

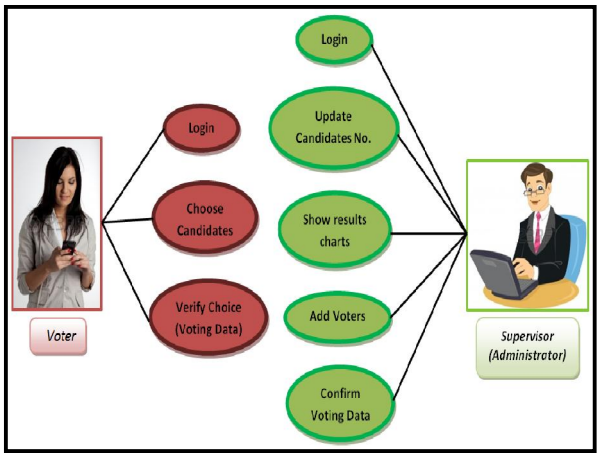

Figure 3. STCVS Use Case Diagram

5.2 STCVS Sequence/Process diagrams

"Figure 4" and "Figure 5" illustrate the voting sequence and process for the "STCVS" system respectively. As shown in figures, the voter has firstly to login to the "STCVS" voting website, voter's authentication is verified by comparing the login data (voter's name, pass-code) to that stored in the database. Status returned from the database indicates whether login is succeeded or not. So, if it is not succeeded, the process will be ended (activity ends).

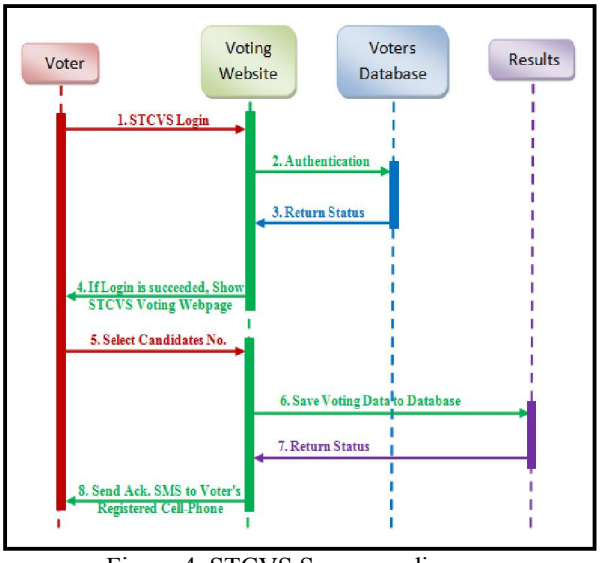

Figure 4. STCVS Sequence diagram

If it is succeeded, also, if this voter has not yet vote, the "STCVS" voting webpage will be shown to the voter, he could select the candidates numbers.

If login data is correct, but the voter has already voted, the process will be ended (activity ends).

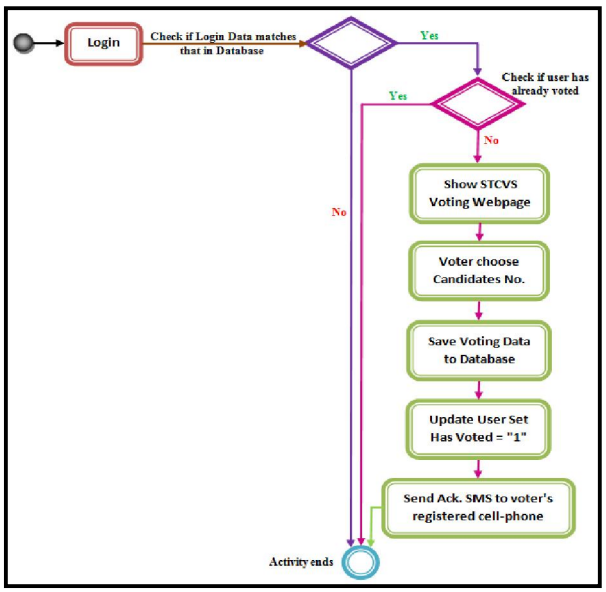

Figure 5. STCVS Process Diagram

The "STCVS" flowchart is represented in "Figure 6".

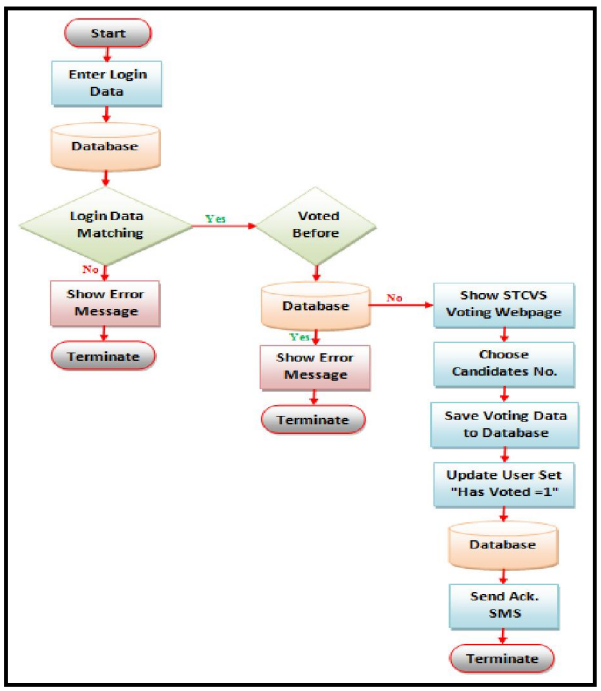

Figure 6. STCVS Flow Chart

Voting data will be saved to the database. The status for this voter will be saved as "has voted", that will be returned to the website to prevent voting duplication. Finally, a feedback (acknowledgement SMS) will be sent from the website to the voter's registered cell-phone as confirmation.

5.3 STCVS Webpages

The voter would access the voting website by entering his full-name, pass-code as shown in "Figure 7". Supervision Login could also been accessed from this webpage.

Figure 7. STCVS Login Webpage

According to each voter's postal-code stored in the database, a voting web-page as shown in "Figure 9" would be accessed where candidates numbers belonging to his round could be selected. The voter would use the form shown in this figure to select "1" (Presidential candidate), "2" (Parliamentary candidates [Individual]), "1" (Parliamentary candidate [Menus]), "2" (Local candidates [Individual]) and "1" (Local candidate [Menus]).

Error messages are shown as alerts in case of any incorrect choice procedure, so that the voter can correct it to complete his voting procedure. The voting data would be saved in the supervisors database tables. The supervisors represent the ("Higher Committee for Elections" and the "Human Rights Association" in our work).

Also, by accessing the supervision login from "Figure 7", "Figure 8" would be shown where the supervisor would enter his name and password to login.

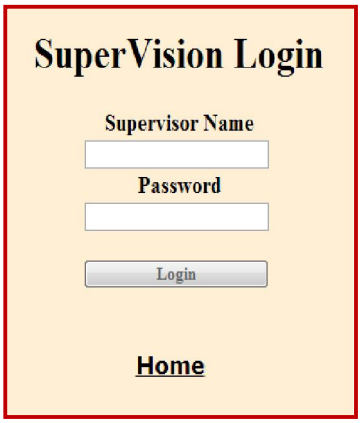

Figure 8. STCVS SuperVision Login Webpage

Figure 9. STCVS Voting Webpage

The supervisor would then be able to get the voting percentage for each candidate by the charts shown in "Figure 10". Hence, our aim to protect the voting data would be achieved since it would be available only with the supervision site ("Higher Committee for Elections" and the "Human Rights Association") that would be the owner of the host server for the proposed "STCVS". The later would have the code, the keys, would encrypt and decrypt the voting data.

6. Requirement Analysis

6.1 Constraints, Obstacles, and Barriers

- The voter can vote only once during the elections time.
- The voter must enter his pass-code saved in the database to verify his identity.
- The used PC's must have at least "1 GB" RAM, Core2Duo "2.4 GHz".

6.2. Performance Requirements

- The error rate must not exceed "1%"
- The voting operations after entering the voter name, pass-code must not take more than "1 min".

6.3. Logical Database Requirements

- The system shall use the MySQL Database which is open source and free.
- The system's database is assumed to be already created and including (Voters Names – Pass-codes – Postal-codes – Addresses).

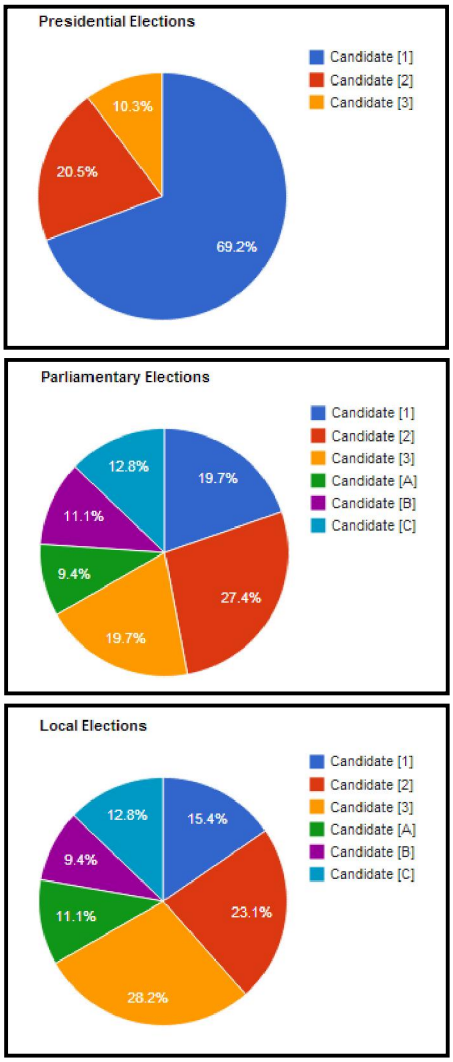

Figure 10. STCVS Charts

7. Interfaces

7.1 Software Interface

The Operating Systems can be any version which supports TCP/IP protocols:

- Application: PHP version : 5.3.13
- Data Base: MySQL version: 5.5.24
- Web Server: Wamp Apache version : 2.2.22

7.2. Communication Interface

The communication interface is a World Wide Web (WWW). The voter must connect to the internet to access the "STCVS" system. This access could be done using cell-phone or (PC / Laptop / Tablet …) to accomplish the voting process.

8. Conclusion

The proposed "STCVS" system is "Multipurpose" since it could be used for (Presidential, Parliamentary and Local) elections. Also, from everywhere and using a smart phone, laptop, PC, tablet or any computerized communicator device, voting process could be achieved.

It saves the cost of a huge number of electronic voting machines that are needed for recent electronic voting systems. Also, the overcrowding of people in the polling stations, and hence the traffic problems would be eliminated.

It protects the "Voting Data" since the later would be sent "Encrypted" from the "Client-Side" where the user would achieve his voting and till the "Host Server" representing the "Supervision side". Encryption is done using asymmetric cryptography algorithm (Elgamal) via "Public-Keys". "Decryption" for the voting data would be done by the "Host Server" using "Private-Key".

System supervisors ("Higher Committee for Elections" and the "Human Rights Association") would use their accounts to display the elections charts showing the voting percentage get for each candidate.

Finally, for more security, an "acknowledgement SMS" would be sent from the "Host Server" to the registered voter cell-phone. It consists of his voting data (i.e. candidates numbers he selected), thus cheating would be eliminated.

- Processing time / Vote ≈ (1) min.
- Processing time / Voting Charts displaying ≈ (30) sec.

For better performance and more reliability, we would suggest integrating Biometrics (or Biometric Authentication) with the proposed computerized voting system for more security. Biometrics is used in computer science as a form of authentication and access control. Hence, voter fingerprint authentication, voter iris recognition could be integrated with the proposed system. This would surely increase the system cost since additional hardware and software would be needed.

Also, we could increase the private (secret) key size. This would provide more security for such elections system but necessities more advanced system specifications with definitely higher cost to support such larger key size.

References

1. "Australian Capital Territory Electoral Commission",http://en.wikipedia.org/wiki/Australian_Capital_Territory_general_election,_2001, 18th March 2013.
2. Angel Tchorbadjiiski, "Liquid Democracy Diploma Thesis", RWTH AACHEN University, Germany, March 2012.
3. Scott Wolchok, Eric Wustrow, Dawn Isabel, and J. Alex Halderman, "Attacking the Washington, D.C. Internet Voting System", Proceedings 16th Conference on Financial Cryptography and Data Security, Feb. 2012.
4. Christof Paar, and Jan Pelzl, "Understanding Cryptography A Textbook for Students and Practitioners", Springer-Verlag Berlin Heidelberg, Germany, 2010.
5. Hans Delfs, and Helmut Knebl Delfs, "Introduction to Cryptography Principles and Applications", Second Edition, Springer-Verlag, Berlin Heidelberg, New York, 2007.
6. Tom St. Denis, and Simon Johnson, "Cryptography for Developers", Syngress Publishing, Inc, 2007.
7. William Stallings, "Cryptography and Network Security Principles and Practices", Fourth Edition, Pearson Education, Inc, 2006.
8. Arthur M. Keller, Alan Dechert, Karl Auerbach, David Mertz, Amy Pearl, and Joseph Lorenzo Hall, "A PC-Based Open-Source Voting Machine with an Accessible Voter-Verifiable Paper Ballot", http://infolab.stanford.edu/pub/keller/2005/electronic-voting-machine.html, USENIX '05, FREENIX track, California, April 10-15, 2005.
9. Tadayoshi Kohno, Adam Stubblefield, Aviel D. Rubin, and Dan S. Wallach, "Analysis of an Electronic Voting System", IEEE Computer Society Press, May 2004.
10. David Chaum, "Secret-Ballot Receipts: True Voter-Verifiable Elections", IEEE Security and Privacy, January/February 2004.
11. Rui Joaquim, André Zúquete, and Paulo Ferreira, "REVS – A Robust Electronic Voting System", IADIS International Journal of WWW/Internet, Vol. 1, N. 2., pp. 47-63, Dec 2003.
12. Taher ElGamal, "A Public-Key Cryptosystem and a signature scheme based on discrete logarithms", IEEE Transactions on Information Theory, Vol. IT-31, No. 4, pp. 469-472, 6th January 2003.
13. Berry Schoenmakers, "Fully Auditable Electronic Secret-Ballot Elections", XOOTIC Magazine, July, 2000.
14. Jared Karro, and Jie Wang, "Towards a Practical, Secure, and Very Large Scale Online Election", Proceedings 15th Annual Computer Security Applications Conference (ACSAC'99), USA, 1999.
15. Lorrie Faith Cranor , and Ron K. Cytron, "Sensus: A Security-Conscious Electronic Polling System for the Internet", http://lorrie.cranor.org/pubs/hicss/hicss.html, Proceedings of the Hawaii International Conference on System Sciences, USA, 10th January 1997.
16. Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone, "Handbook of Applied Cryptography", Massachusetts Institute of Technology, Cambridge, USA, June 1996.
17. Atsushi Fujioka, Tatsuaki Okamoto, and Kazuo Ohta, "A practical Secret Voting Scheme for Large Scale Elections", Advances in Cryptology - AUSCRYPT '92, Computer Science, Vol. 718, pp. 244-251, Japan, 1993.
18. David Chaum, "Elections with Unconditionally-Secret Ballots and Disruption Equivalent to Breaking RSA", Advances in Cryptology, EUROCRYPT'88", pp. 177-182, 1988.
19. Whitfield Diffie, and Martin E. Hellman, "New Directions in Cryptography", IEEE Transactions on Information Theory, vol. IT-22, pp. 644-654, Nov., 1976.

12/12/2013