

A High Secured, Cost Effectively E-Voting System

Essam M. HAMED, Mohammad Hosam SEDKY

College of Computing and Information Technology

Arab Academy for Science, Technology and Maritime Transport, Heliopolis,
Cairo, Egypt

essam.hamed@aast.edu, m.hosamsedky@hotmail.com

Abstract

Electronic voting is often seen as a tool for making the electoral process more efficient and increasing trust in its management. Properly implemented e-voting solutions can increase the security of the ballot, speed up the processing of results and make the voting process easier. However, the challenges are considerable. If not carefully planned and designed, e-voting can undermine the confidence in the whole electoral process. The main important obstacle in any e-voting system across the world is the security issue. Election's results may be modified when delivered to the Higher Elections Committee, unauthorized voter may vote instead of the eligible voter, a vote may not be calculated; also there may be an election's official reveal the candidate who some voter cast his ballot for. That makes E-voting system generally not trustful and convenient. This paper proposes a voting model system overcomes these obstacles. Security parameters evaluation experiments are performed successfully to the proposed system. The experiments are proving that the proposed Voting Model satisfies privacy, accuracy, un-readability, eligibility, integrity, and cost effectiveness.

Index terms: EVS, FDES, Security, E-Voting Systems, Data Integrity, Avalanche Effect

References:

- [1]. Fact Sheet June 2009, Estonia Today, "Estonian e-voting system", accessed on 05-04-2015 at http://vm.ee/sites/default/files/content-editors/web-static/095/e-voting_system.pdf.
- [2]. U.S. Election Assistance Commission, "A Survey of Internet Voting", Voting System Testing and Certification Division 1201 New York Avenue, NW, Suite 300 Washington, DC 20005, accessed on 05-04-2015 at <http://www.eac.gov/assets/1/Documents/SIV-FINAL.pdf>.
- [3]. Estonia.eu, "Estonian e-voting System", accessed on 05-04-2015 at <http://estonia.eu/about-estonia/economy-a-it/e-voting.html>.
- [4]. Geneve.ch, "The Geneva Internet Voting Project", accessed on 08-12-2014 at <http://www.geneve.ch/evoting/english/doc/final-livret-anglais.pdf>.

- [5]. Mägi. T, “Practical Security Analysis of E-voting Systems”, Master Thesis, TALLINN UNIVERSITY OF TECHNOLOGY, 2007, accessed on 05/04/2015 at <http://www.cs.nccu.edu.tw/~raylin/MasterCourse/http://www.cs.nccu.edu.tw/~raylin/MasterCourse/SelectedTopicsIS/Spring2009/master%20thesis%20e-voting%20security.pdf>.
- [6]. Gerlach. J, Gasser. U, “Three Case Studies from Switzerland: E-Voting”, Berkman Center Research Publication No. 2009-03.1, March 2009, accessed on 04-04-2015
- [7]. http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/Gerlach-Gasser_SwissCases_Evoting.pdf.
- [8]. Geneve.ch, “The Geneva Internet Voting System”, accessed on 08-12-2014 at <http://www.geneve.ch/evoting/english/securite.asp>.
- [9]. Digitalvote.wordpress.com, “E-voting in Brazil, step by step”, accessed on 05/04/2015 at <http://digitalvote.wordpress.com/2014/10/03/e-voting-in-brazil-step-by-step/>.
- [10]. M. Ali, “Critical thoughts from a government mindset”, Cartridge Books Oxford, Hexagon House Avenue 4, 2013, p 180-186.
- [11]. UAENEC.ae, accessed on 08/01/2015 Available at <http://www.uaenec.ae/ar/election-centers/overview.aspx>.
- [12]. National Institute of Standards and Technology. “An Introduction to Computer Security: The NIST Handbook”. Special Publication 800–12. October 1995, pp 5.
- [13]. Keshk. A. E, “Development of remotely secure E-Voting”, 5th International Conference on Information and Communications Technology, ICICT 2007, Page:235
- [14]. CES (2002), “E-voting Security Study, Communications and Electronic Security Group (CESG)”, accessed on 10-12-2014 at [“http://www.edemocracy.gov.uk/library/papers/study.pdf”](http://www.edemocracy.gov.uk/library/papers/study.pdf).
- [15]. G. Dimitris, “Secure Electronic Voting”, 7th Computer Security Incidents Response Teams Workshop Syros, Greece, September 2002, pp 9-10, accessed on 05-04-2015 at <http://www.terena.org/activities/tf-csirt/meeting7/gritzalis-electronic-voting.pdf>.
- [16]. A. Fujioka, T. Okamoto and K. Ohta, “A practical secret voting scheme for large scale elections”. LNCS 718, Advances in Cryptology: Proc. Auscrypt’92, Springer Verlag, Pages: 244-251.
- [17]. T. Wan, W. Liao, “Cryptanalysis on Polynomial-Based E-Voting Schemes”, 2010 International Conference on E-Business and E-Government, Page 436.
- [18]. ElectionAudits.org, “Principles and Best Practices for Post-Election Audits”, access on 15-11-2014 at http://electionaudits.org/files/best%20practices%20final_0.pdf.
- [19]. S. William, “Network Security Essentials: Applications and standards”, 5th Edition, Pearson Education, Inc., publishing as Prentice Hall, 1 Lake Street, Upper Saddle River, NY07458, 2011, p 77-78.
- [20]. Sarker, M.Z.H.; Parvez, M.S, “A Cost Effective Symmetric Key Cryptographic Algorithm for Small Amount of Data”, 9th International Multitopic Conference, IEEE INMIC 2005, Pages: 1-6

- [21]. Eff.org, "Frequently Asked Questions (FAQ) About the Electronic Frontier Foundation's "DES Cracker" Machine", accessed on 05-04-2015 at https://w2.eff.org/Privacy/Crypto/Crypto_misc/DESCracker/HTML/19980716_eff_des_faq.html.
- [22]. Essam M. Hamed, S. Mohammad Hosam, "A Modified Flexible Data Encryption Standard Algorithm", *European Journal of Scientific Research (EJSR)*, volume 126, Number 4, November 2014, Pages: 465-480.
- [23]. M. Akash, et. al, "Performance Evaluation of Cryptographic Algorithms: DES and AES", 2012 IEEE Students' Conference on Electrical, Electronics and Computer Science, IEEE SCEECS.
- [24]. "1.2 مليار جنيهه تكلفة انتخابات الرئاسة المصرية 1.2" available at: www.al-sharq.com/news/details/242069. Election.eg, "Egyptian Presidential Elections 2014", available at <https://pres2014.elections.eg/presidential-elections-2014-results>
- [25]. Election.eg, "Egyptian Presidential Elections 2014", available at <https://pres2014.elections.eg/presidential-elections-2014-results>