Implementation of Digital and Security probing Voting Machine

Srinjoy Chatterjee, Pinaki Pratim Acharjya
Department of Computer Science and Engineering
Durgapur Institute of Advanced Technology and Management
Durgapur, West Bengal, India
srinjoychatterjee2013@gmail.com, ppacharjya@gmail.com

Abstract — ***This research is generally based on implementation of new type of security probing Voting Machine which can make the entire system easy and smooth. Moreover, our main objective is maintaining the security which is being utilized by a special type idea and innovative techniques. The prototype model can be utilized through web-oriented services (Software, Applications, Websites) or by Hardware oriented models.***

Keywords - security probig, voting machine.

I. INTRODUCTION

Voting machine is an important aspect in each and every democratic country of our world. Each and every government or ruling authority has the right to VOTE or ELECT their suitable candidate who may serve the best for the people, of the people, by the people [1-4]. Our voting system in India started with Ballot Box (Hard copy paper), then to EVM (Electronic Voting Machine). But the EVM seems to be unsecure to conduct an election in the 21st century. The non-availability of authentication system makes it totally unsecured [5-12]. Nowadays when all systems are getting automated and security probed [13-17], the voting machine must also. The Prototype model we are going to introduced not only enabled with authentication system but also a new strategy to implement vote casting.

II. IMPLIMENTATION AND DISCUSSION

The Random generation of security code for each and every vote is being briefly explained. For each and every voter, the system will generate a list of security codes for each and every candidate nominated. The list of randomly generated security code will defer from each and every voter. This strategy will reduce the vote rigging up to 80%.

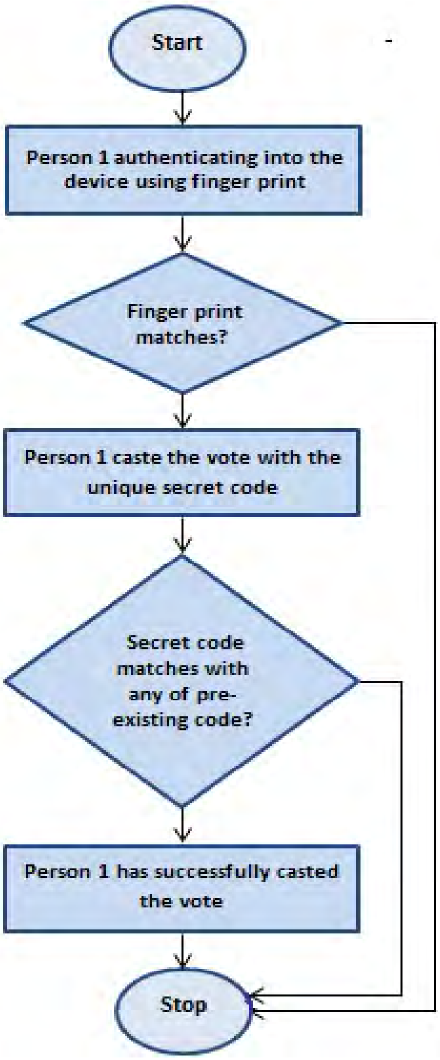
Start
Person 1 authenticating into the device using finger print
Finger print matches?
Person 1 caste the vote with the unique secret code
Secret code matches with any of pre-existing code?
Person 1 has successfully casted the vote
Stop

Figure 1. Example of a figure caption. (figure caption)

The table illustrated below (Table 1) shows the random generated security code for a voter to vote. The table will vary from each and every voter (Table 2). Both the tables given below shows that the nominated candidates are same but security codes are different. These codes will be entered by the voter in the system (Figure 1) to generate free and fair vote followed by election.

TABLE I. THE GENERATED SECURITY CODE TO VOTER 1

Nominated Party standing for election	Security Code
XYZ	14578
QEL	25748
WQM	78459

TABLE II. THE GENERATED SECURITY CODE TO VOTER 2

Nominated Party standing for election	Security Code
XYZ	57842
QEL	87956
WQM	74958

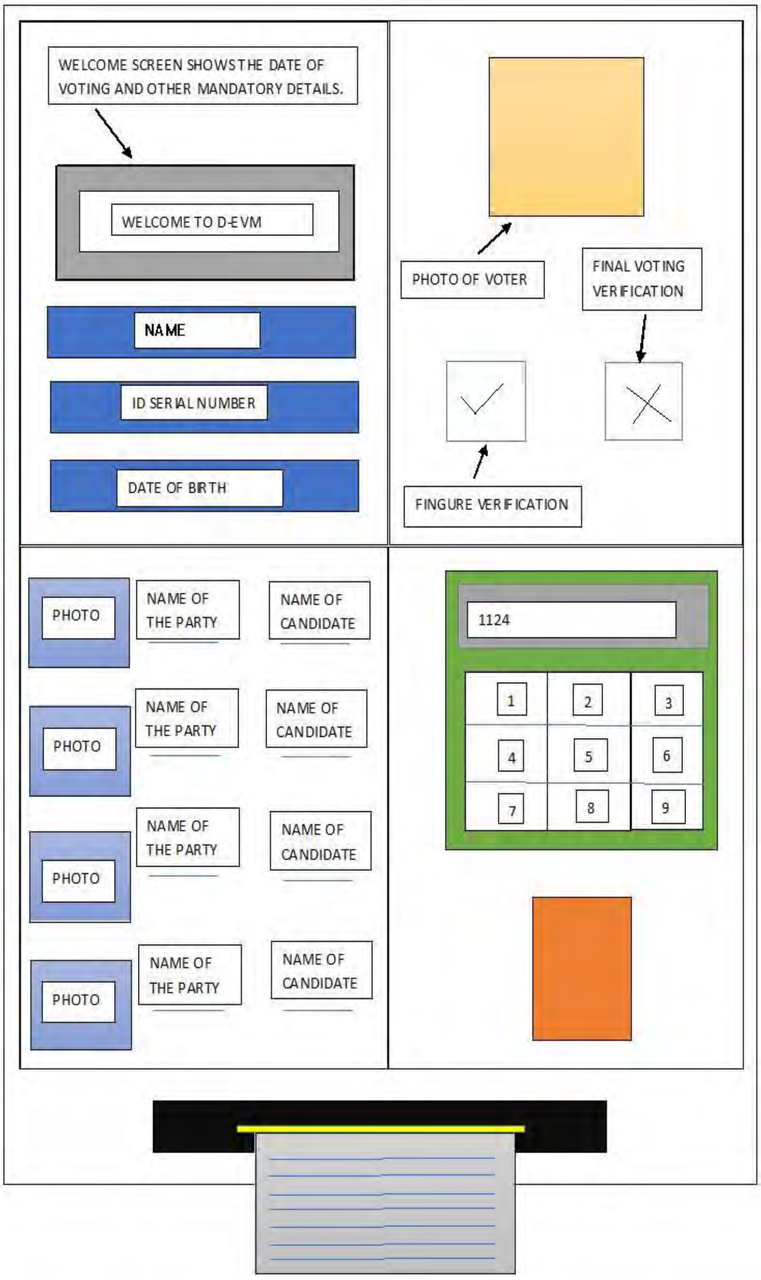

Figure 2. Prototype model of the system

III. CONCLUSION

This System of Election doesn’t need a huge number of work force or huge number of securities to control hacking of EVM. Less number of Paper works to be done by authority, it is fully digitalized, and larger number of papers are saved. No need of Booth slip. No need marking ink. Less number of hacking due to Security Code theory and Finger print Authentication. No One can force any one to cast a particular vote and third party can cast vote, neither excess number of votes can be casted.

REFERENCES

[1] A. K. Agarwala, D. T. Shahani, and P. V. Indiresan. Report of the expert committee for evaluation of the upgraded electronic voting machine (EVM). Sept. 2006. http://www.scribd.com/doc/6794194/ Expert-Committee-Report-on-EVM, pages 2-20.

[2] R. Anderson and M. Kuhn. Tamper resistance: A cautionary note. In Proc. Second USENIX Workshop on Electronic Commerce, Oakland, CA, 1996.

[3] A. W. Appel. Certi_cation of December 1, 2008. http://citp.princeton.edu/voting/advantage/seals/ appel-dec08-certif.pdf.

[4] A. W. Appel, M. Ginsburg, H. Hursti, B. W. Kernighan, C. D. Richards, G. Tan, and P. Venetis. The New Jersey voting-machine lawsuit and the AVC Advantage DRE voting machine. In Proc. Electronic Voting Technology Workshop/Workshop on Trustworthy Elections (EVT/WOTE), Montr_eal, Canada, Aug. 2009.

[5] A. Aviv, P. Cern_y, S. Clark, E. Cronin, G. Shah, M. Sherr, and M. Blaze. Security evaluation of ES&S voting machines and election management system. In Proc. USENIX/ACCURATE Electronic Voting Technology Workshop (EVT), San Jose, CA, July 2008.

[6] D. Bowen. \Top-to-Bottom" Review (TTBR) of voting machines certi_ed for use in California. California Secretary of State, Aug. 2007. http://sos.ca.gov/elections/elections vsr.htm.

[7] Santanu Santra, Pinaki Pratim Acharjya, “A Study and Analysis on Computer Network Topology for Data Communication”, International Journal of Emerging Technology and Advanced Engineering, Vol. 3, pp. 522-525, January 2013.

[8] Santanu Santra, Pinaki Pratim Acharjya, “Comparative Study of Proactive Routing Protocols for MANETs”, International Journal of Electronics and Computer Science Engineering,, Vol., pp. 375-383, January 2013.

[9] J. Brunner. Evaluation & Validation of Election-Related Equipment, Standards & Testing (EVEREST). Ohio Secretary of State, Dec. 2007. http://www.sos.state.oh.us/SOS/Text.aspx?page=4512.

[10] Bundesverfassungsgericht (German Constitutional Court). Judgment [...] 2 BvC 3/07, 2 BvC 4/07, o_cial English translation. Mar. 3, 2009. http://www.bverfg.de/ entscheidungen/rs20090303 2bvc000307en.html.

[11] K. Butler, W. Enck, H. Hursti, S. McLaughlin, P. Traynor, and P. McDaniel. Systemic issues in the Hart InterCivic and Premier voting systems: Reections on Project EVEREST. In Proc. EVT, San Jose, CA, July 2008.

[12] J. A. Calandrino, A. J. Feldman, J. A. Halderman, D. Wagner, H. Yu, and W. P. Zeller. Source code review of the Diebold voting system. Part of California TTBR, Aug. 2007.

[13] J. A. Calandrino, J. A. Halderman, and E. W. Felten. Machine-assisted election auditing. In Proc. EVT, Boston, MA, Aug. 2007.

[14] C. Castelluccia, A. Francillon, D. Perito, and C. Soriente. On the di_culty of software-based attestation of embedded devices. In Proc. 16th ACM Conference on Computer and Communications Security (CCS), Chicago, IL, pages 400-409, Nov. 2009.

[15] M. Chatterjee. Tribal voters in Jharkhand reckon with EVM technology. In Indo-Asian News Service, Nov. 20, 2009.

[16] D. Chaum. Secret-ballot receipts: True voter-veri_able elections. IEEE Security & Privacy, 2(1):38{47, Jan. 2004.

[17] D. Chaum, A. Essex, R. Carback, J. Clark, S. Popoveniuc, A. Sherman, and P. Vora. Scantegrity: End-to-end voter-veri_able optical-scan voting. In IEEE Security & Privacy, 6(3):40{46, May 2008.