Empowering E-governance with E-voting

Amarjeet Singh[1], Ramakanth Kumar P[2], Nagaraj G Cholli[3]
[1]Vivekananda Institute of Technology, Jagatpura, Jaipur (Rajasthan) India-303012
[2]Dept of Information Science & Engg, R V College of Engineering, Bengaluru, Karnataka, India

Article Info

Article history:

Received Dec 23, 2017
Revised Jan 10, 2018
Accepted Jul 25, 2018

Keywords:

E-governance
Encryption
E-voting
Security

ABSTRACT

Advances in Information and Communications Technology (ICT) have impacted the society in many ways. Be it education, healthcare, media or governance, the transformation is visible. As individual entities like education or healthcare systems have already implemented ICT to certain extent, e-governance is yet to make a significant progress even though several initiatives are undertaken. E-governance means activities like voting, administration, financial transaction etc., are enabled using automation systems. This paper discusses one part of the e-governance; e-voting. As e-voting empowers government, there are lot of challenges in implementing the e-voting system considering security threats and confidentiality involved in it. Online voting (e-voting) needs to be deployed as more convenient, relatively secure and less resource consuming system. E-voting system should ensure convenience for people to be able to access the system from personal or public computer with security and confidentiality. The presence of e-voting system with all the necessary security measures and convenience can be a potential solution for low voter turnout at the polls. The presented work demonstrates an online e-voting prototype system called SecureV. The proposed model achieves specific tasks namely, maintaining the anonymity of the voter, encryption of the vote, integrity check and avoids second time voting.

Corresponding Author:

Amarjeet Singh,
Vivekananda Institute of Technology,
Jagatpura, Jaipur (Rajasthan) INDIA-303012.
Email: amar.66.07@gmail.com

1. INTRODUCTION

In the current election process, a voter casts vote in voting stations. The voter is allowed to vote after physical verification of necessary documents. Once, the documents are verified, the person is a given a ballot which cannot be reused. The ballot does not reveal the actual identity. The traditional methods are established and trusted by parties as the disruption is not easy. In the existing voting process, it is not easy to attack as there is a greater chance of being caught and there will be physical evidence. As the new generation voters prefer electronic voting, it has become the need of the hour. This is revealed in the survey done by the Public Policy Institute of California. Internet voting is the choice of more than 50% respondents in the age group of 18-44 as per the surveys conducted. Security is the main concern as the network and internet related attacks are untraceable at several occasions. Also, there are chances that attacks may be all around the world. Educating voters is another issue with e-voting as. Users are not computer proficient and can’t use the e-voting system easily. Educating the voters in using e-voting system is another issue. It cannot be assumed that all voters are computer proficient and they will use the e-voting systems with ease. E-voting should be designed in such a way that it should be easy to use.

E-voting delivers fast, convenient and cost Effective Service Delivery if all the security concerns are addressed. E-voting increases the participation of people which is now drawback in the democracy. Current systems use several security measures such as cryptography for secure communication. Technical and secure attributes of a good e-voting system include accuracy, verifiability, privacy, convenience, flexibility and mobility [1]. A system can be called reliable and accurate if there is no chance for alteration of casted vote. The system should also ensure that the validated vote cannot be eliminated. A System is verifiable if anyone can independently verify that all votes have been counted correctly. A system can be called democratic if it denies the voting by non eligible voter, provides voting option for eligible voter only once.

Growing interest has been observed in recent years in e-voting as it provides a way to make voting more convenient and also increases the participation percentage in election process. Traditional systems have to be replaced by e-voting systems in future. E-voting is the quickest, efficient, economical and efficient way to conduct elections. In this work a new approach has been proposed for development of e-voting system which is more secured and reliable. Figure 1 depicts the existing voting modes.

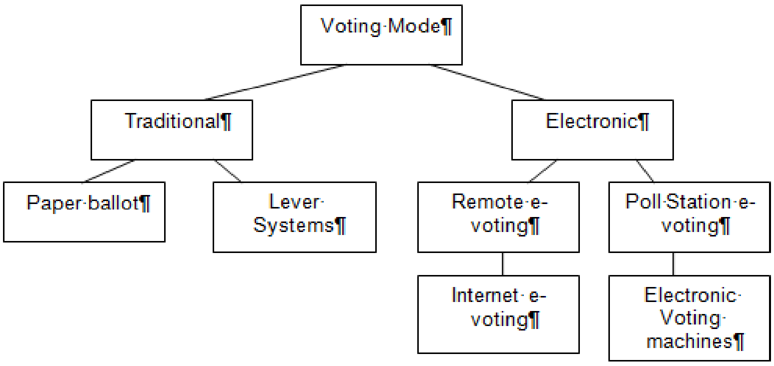


Figure 1. Voting Modes

2. RELATED WORK

In the last decades, an enormous amount of literature on electronic voting has been developed. As electronic voting concept is gaining momentum, efforts have begun to develop real-world solutions [2], [3]. Electronic voting poses new challenges as the use of insecure Internet results in security breaches [4]. These security concerns and challenges have to be resolved to increase the trust worthiness of e-voting.

Universal verifiability concept was introduced by Sako et al., [5] that emphasizes the importance of election audit by categorizing the verifiability. The e-voting studies apply 2 categories; individual variability and universal verifiability. In individual verifiability, a sender can verify the reachability of his message to destination but not of other voters. Universal verifiability is the category in which participants can broadcast information that can be used by third party for verification whether the election was performed properly or not.

It is not simple to implement e-voting in reality. Mercuri et al., [6] worked on the issues like conflicts that arise between secrecy and accuracy requirements. Problems also pop up from the procedure that is followed in current voting systems. There is still no voting system which can be called as safety-critical in development and deployment as opined by some researchers [7]. Because of the proprietary nature of system components and other factors, serious issues have been created in legally binding elections. As e-voting needs network infrastructure, threats exist in various forms leading to untrustworthy systems. Threats such as DOS (Denial of Service), malwares, worms, Trojan horses etc., have destructive impact on the availability of the system. These can affect the availability of e-voting systems forcing the governments to conduct re-elections. Worm replaces the portions of the data with random data and hence it is dangerous [8]. This can bring down the integrity of voting system as there is a chance of it may affect the results of voting. Trojan horses are destructive computer programs that delete or modify important files from computer. There are also chances of password stealing and planting harmful viruses. This leads to fraudulent schemes.

Hari K. Prasad et al., [9] analyzed the security of electronic voting machines in India. The authors opined that there is a need to reconsider mechanisms to achieve secured and transparent voting system that suits national values and requirements. VVPAT (Voter verifiable audit trail) was suggested that is in use in other countries. VVPAT combines electronic record stored with a paper vote record that can be audited by hand. Electronic Voting Machines do not have updatable software but still VVPAT can be added by interposing on the cable between ballot unit and the control unit. There exists another option in the form of

PCOS (precinct-count optical scan) where the ballot paper ballots are filled by voters, scanned by a voting machine at the polling stations before they are placed in a ballot box.

The outcome of the literature survey is that there exists a solution for security concerns of electronic voting but also indicate more secured, trust worthy system is needed for the present political conditions.

3. PROPOSED MODEL: SecureV

3.1. System Model

The proposed model achieves four points: Anonymity of the voter, encrypted vote, integrity check and restricting the eligible voter to cast the vote only once. There are mainly two user types for voting portal usage. One as administrator and other as voter. The administrator tasks include creation of candidate list and registration of voter. The anonymity of vote casting is maintained for all voters. Secret ballot is a voting method in which a voter's choices in an election or a referendum are anonymous. In the proposed work, this is achieved by sending a secret key to voter. This key is used for logging to voting portal. Once the voter logs in, the voter is provided with the list of candidates. Once the vote is casted, the vote is encrypted and stored. The voter cannot cast the vote again as the portal does not permits. Table 1 depicts additional information of the process followed.

Table 1. e-voting process in SecureV Model

Activity	Role	Technical aspect
Voter Registration	Administrator	• Secret key is generated
Candidate List Preparation	Administrator	
Voting	Voter	• Vote is encrypted using public key and stored • Anonymity is maintained
Vote Counting	Administrator	• Vote is decrypted using secret key • Integrity check done • Corrupted / Manipulated vote not counted

The voting server has been built with the following strengths:

a) Access control mechanism allows access to the voting server if at least two different users are logged on.
b) Comprehensive audit data availability in the server.
c) No provision to know the voting process except number of votes casted so far.
d) Servers stops in case of irreversible problems.

The voter interface has the following functionality:

1) Identification and authentication of voter.
2) Initiating the polling possible only once.
3) Resume polling after recovery in case breakdowns.
4) Perform self-checks.

3.2. Technical Aspects of the Model

The model used asymmetric cryptography where the system uses pairs of keys: public keys and private keys. Public keys are disseminated widely and private key is known only to the owner. Vote encrypted with public key can be decrypted only with private key. The private key cannot be practically derived from the public key. Figure 2 indicate the asymmetric cryptography process.

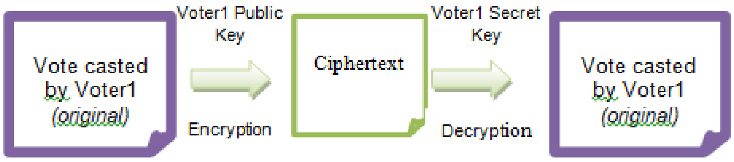
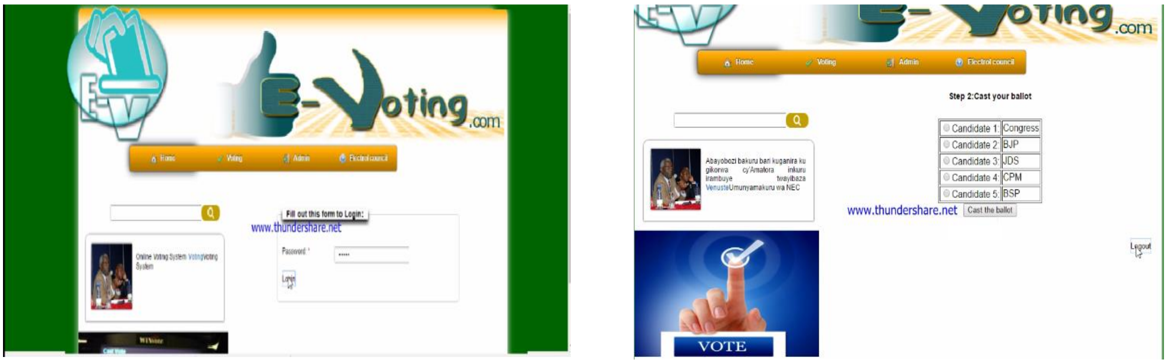

Vote casted by Voter1 (original)
Voter1 Public Key
Encryption
Ciphertext
Voter1 Secret Key
Decryption
Vote casted by Voter1 (original)

Figure 2. Asymmetric Cryptography

The voter cannot cast the vote for second time as the portal does not allow it. Once the voting process is over, the administrator decrypts the votes using secret key and vote counting is done. Prior to this, integrity check is done to ensure that no vote has been manipulated. An integrity check module has been integrated in the portal with built-in intelligence. Figure 3 provides the two screenshots of the application developed.



○ Candidate 1	Congress
○ Candidate 2	BJP
○ Candidate 3	JDS
○ Candidate 4	CPM
○ Candidate 5	BSP

Figure 3. Screenshots of the applicatios

3.2.1. MD5 Algorithm

Integrity check is done using MD5 algorithm. The MD5 function algorithm takes an input of arbitrary length and produces 128 bits long message digest. The digest is also called as "hash" or "fingerprint" of the input. MD5 is suitable for integrity check of the votes casted using voter interface.

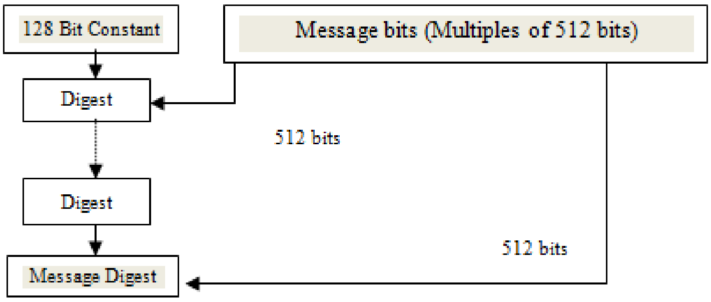


Figure 4. MD5 hashing algorithm

MD5 algorithm hashing process:

a) The message is padded to make its length 448 bits or 512 bits. Padding is also performed even if the message length is already 448 bits or 512 bits. This is achieved by adding “1” bit to the message and appending “0” bits so that the length becomes congruent to 448 mod 512. Minimum one bit and maximum 512 bits are appended.

b) MD5 uses 32 bits length words that constitute buffer which are named A, B, C & D. These words are initialized as
word A: 01 23 45 67
word B: 89 ab cd ef
word C: fe dc ba 98
word D: 76 54 32 10

c) MD5 uses a table K that has 64 elements. The following function is used to compute elements.
Ki = abs(sin(i + 1)) * 232 where Ki is the element number i.

d) MD5 also uses four auxiliary functions. Each of these functions takes 32-bit words as input and produces one 32-bit word as output. Logical operators AND, NOT, XOR and OR are used for processing.
F(X,Y,Z) = (X and Y) or (not(X) and Z)

G(X,Y,Z) = (X and Z) or (Y and not(Z))
H(X,Y,Z) = X xor Y xor Z
I(X,Y,Z) = Y xor (X or not(Z))

e) Buffers (A,B,C,D) content is mixed with the words of the input using auxiliary functions. After completion of all rounds, the buffers A,B,C D contain the MD5 digest of the original input.

3.2.2. Homomorphic Encryption

For encryption, homomorphic encryption has been used. In homorphic encryption, useful operations can be performed on encrypted values without decrypting them first. Given cipher texts that encrypt $\pi_1, \ldots,$ π_t , any one can generate ciphertext that encrypts $f(\pi_1, \ldots, \pi_t)$ for any desired function f, as long as that function can be efficiently computed. The original message would be the AES key encrypted under some public key pk1, the homomorphic function decrypts the AES key under pk1and encrypting it again under pk2. In this model, AES key, KK, is encrypted under public key pk1, that is, $Enc_{pk1}(K)$. If ff is designed to decrypt cipher texts using the corresponding secret key, that is, $f(sk_1,Enc_{pk1}(K))=K$, the equation indicate the transformation without affecting the original information.

$$f(Enc_{pk2}(sk_1),Enc_{pk2}(Enc_{pk1}(K)))=Enc_{pk2}(K) \quad (1)$$

Advanced Encryption Standard (AES) algorithm used in the model accepts the bock size of 128 bits and choice of three keys – 128 bits, 192 bits and 256 bits. The encryption consists of 10 rounds for 128 bits, 12 rounds for 192 bits and 14 rounds for 256 bits.

These technologies strengthen the proposed e-voting system with availability, integrity and confidentiality. Figure 5 indicate the building blocks of the proposed system.

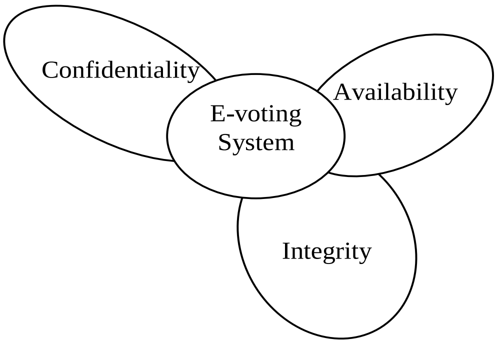


Figure 5. Building blocks of e-voting system

- Integrity implies protecting against data correction. In the proposed model, this is achieved MD5 hashing algorithm.
- Confidentiality implies securing individual protection and restrictive data. This is achieved using private key concept.
- Availability implies guaranteeing convenient and dependable access to, and utilization of data. The proposed model incorporates this using easy to use voter interface and secured server.

4. CONCLUSION

In this work, a new approach has been developed for e-voting process that takes care of all required security concerns. The SecureV model has improved built in security measures that can improve the trustworthiness of e-voting process. The proposed model stands out among existing techniques in terms of reliability, usability, voter friendly and easy process flow. This can be cost effective also compared to other models. The proposed system can be a potential candidate for e-voting systems under consideration.

A future work is planned to include additional security measures and improving the user interface design. The planned work also includes voice input at voter interface end.

REFERENCES

[1] Abdalla Al-Ameen and Samani Talab, The Technical feasibility and feasibility of e-voting, *The International Arab Journal of Information Technology, Vol. 10, No. 4, July 2013*

[2] Cetinkaya, O. & Cetinkaya, D. *Towards Secure E-Elections in Turkey: Requirements and Principles*, International Workshop on Dependability and Security in e-Government (DeSeGov'07) - *In Proceedings of ARES'07*, Vienna, Austria,2007, pp. 903-907.

[3] Cranor, L. & Cytron, R. S*ensus: A Security-Conscious Electronic Polling System for the Internet*, In Proceedings of the 30th Annual Hawaii International Conference on System Sciences, Wailea, Hawaii, 1997

[4] Kohno T, Stubblefield A, Rubin AD & Wallach DS., *Analysis of an electronic voting system*. IEEE symposium on security and privacy, 2004

[5] Sako, K. & Kilian J. *Receipt-Free Mix-Type Voting Scheme: A Practical Solution to the Implementation of A Voting Booth*, In Proceedings of Advances in Cryptology EUROCRYPT'95, Malo, France, 1995, pp. 393-403.

[6] Mercuri, R., "Rebecca Mercuri's Statement on Electronic Voting", [Online], 2000, Available: http://www.notablesoftware.com/RMstatement.html

[7] Mcgaley, M., & GIBSON, J. P., *EVoting: A Safety Critical System*. Tech. Rep. NUIM-CS-TR-2003-02, NUI Maynooth, Computer Science Department, 2003, http://www.cs.may.ie /research/reports/2003/index.html#02.

[8] Falk H., "Computer Intrusions and Attacks," The Electronic Library, vol. 17, no. 2, pp. 115-119, 1999.

[9] P. Jagadeeswaraiah, M.R. Pavan Kumar, *SecureDBaaS Model for Accessing Encrypted Cloud Database,* TELKOMNIKA Indonesian Journal of Electrical Engineering, Vol. 16, No. 2, November 2015, pp. 333 ~ 340.

[10] L Ferretti, M Colajanni, M Marchetti. *Distributed, concurrent, and independent access to encrypted cloud databases*. IEEE Transactionson Parallel and Distributed Systems, 2013; 99: 2013.

[11] A. Ben Charke , M. Chabi , M. Fakir, *Contribution to the Security of the Information System,* TELKOMNIKA Indonesian Journal of Electrical Engineering, Vol. 16, No. 1, October 2015, pp. 154 ~ 166.

[12] Kenneth G Paterson. *A cryptographic tour of the IPsec standards,* Information security technical report. 2006. 11(2): 72-81

[13] Pierre-Alain Fouque, Gaëtan Leurent, Phong Q Nguyen, Full Key-Recovery Attacks on HMAC/NMAC- MD4 and NMAC-MD5, LNCS. 2007; 4622: 13-30.

[14] Syed Umar , P. Gayathri , N. Yongender Nath , N. Bashwanth , Royyuru Srikanth, *Data Integrity and Security [DIS] Based Protocol for Cognitive Radio Ad Hoc Networks*, Indonesian Journal of Electrical Engineering and Computer Science, Vol. 5, No. 1, January 2017, pp. 187 ~ 195

[15] Johnson J, Kaliski B. Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1. 2013. www.ietf.org. Network Working Group.