iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 2 **Issue:** XI **Month of publication:** November 2014

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

A General E-Voting Scheme and Its Consequences

Ashish Jain*[1],Dhanraj Negi*[2],Dheeraj Dixit*[3]
[1,2,3] (B.Tech 3rd sem) Dept. of Computer Science and Engineering,
Dronacharya College of Engineering, Gurgaon 122001, India

***Abstract:** This paper introduces on electronic voting scheme, that have security context or known as e-trusted voting scheme. In this study, the prototype builds based on secured and trusted framework for electronic voting In this paper a new electronic voting scheme is described which guarantees coercion- resistance as well as privacy, eligibility, unreusability and verifiability. . In order to test whether the system had been fully functioning and meets the user's requirement, we have to apply the system to a sample of 20 persons and finally the prototype occur the objective and give us a general prototype system that provides security and trusted electronic voting.*

I. INTRODUCTION

The research on electronic voting is a very important topic for the progress of democracy. If a secure and convenient electronic voting system is provided, it will be used more frequently to collect people's opinion for many kind of political and social decisions through cyber space. Traditional paper-based voting can be time consuming and inconvenient. Electronic voting not only accelerates the whole process, but makes it less expensive and more comfortable for the voters and the authorities as well. It also reduces the chances of the errors. Electronic voting schemes should provide all basic features that conventional voting does, further should furnish more services in order to make the process more trusted and secure. Formerly when elections were made traditionally, organizers determine who is eligible to vote. This may involve a formal registration period or an announcement that anyone who is a member of a certain group as of a certain time may vote. This way could involve asking voters for identification cards or passwords. Generally, this procedure also involves keeping track of who has already voted so that eligible voters may vote only once. Moreover, the traditional way of voting generates mores constraints; election fraud could be prevented by using physical security measures, audit trails, and observers representing of all parties involved. But the prevention of election fraud was very difficult. Contrarily to the traditional way of voting, electronic voting is essential because it considers ways in which the polling tasks can be performed electronically without sacrificing voter privacy or introducing opportunities for fraud. In order to determine whether a system performs these tasks well, it is useful to develop a set of criteria for evaluating system performance. The criteria to be developed are such as accuracy, democracy, convenience, flexibility, privacy, verifiability and mobility. The aim of this paper is to develop a general prototype system that provides security and trusted electronic voting system.

A. Primary Features

In order to be functional in practice, an electronic voting scheme has to satisfy not only all the standard features of the conventional paper-based voting methods, but also should provide more efficient voting services. E-voting comparing to the traditional election allows adversaries to intrude the voting process in an easier way, even if there is a small security gap in the design.

Eligibility: Only eligible voters can cast votes.

Privacy: All votes remain secret. No coalition of participants not containing the voter himself can gain any information about the voter's vote.

Unreusability: Every eligible voter can cast only one vote.

Fairness: No participants can gain any knowledge about the partial tally before the counting stage. Knowledge of any intermediate result about the election can influence the voters.

Robustness: No voter can disrupt the election, any invalid vote will be detected and not counted in the final tally.

Individual verifiability: Each eligible voter should be able to verify that his vote was com- mitted as intended and

©IJRASET 2014: All Rights are Reserved

made into the final tally as cast.

Universal verifiability: Any participant or passive observer can check that the election is fair, the final result is exactly the sum of the votes.

Receipt freeness Uncoercibility: The voter cannot reveal his ballot to any adversary. Before the election someone can bribe the voter with a demand of casting his favorite vote. Receipt- freeness avoids vote-buying. Uncoercibility means that a voter cannot be forced into casting a particular vote by an adversary. During the election a coercer can observe the public information the communication between the voter and the authorities and can even order the voter how he should behave during the voting process with generating him the random bits.

Randomization attack: An attacker coerces a voter to submit randomly formed ballot. In this attack it is not possible to learn what candidate the voter cast a ballot for. The effect of this attack is to cancel the voter's vote with large probability.

Forced-abstention attack: An attacker forces a voter to abstain from voting. This attack happens if an adversary is able to follow who is eligible for voting and who has already voted. Being aware of this knowledge he threatens voters and effectively excludes them from the voting process.

Simulation attack: In this attack an adversary coerces or bribes the voter to reveal his private keying material and then pretends to be the voter and casts his own favorite vote.

A scheme is called coercion-resistant if it offers not only receipt-freeness, but also defense against randomization, forced-abstention and simulation attacks.

B. The Voting Scheme

The proposed election procedure consists of three distinctive stages:

1) *Authorizing, Voting and Tallying:* During the Authorizing stage the voter authenticates himself and receives his credentials, the Voting Authority gets the voter roll containing the corresponding public keys and all system parameters are generated.

During the Voting stage voters create their ballots. Voting Authority checks eligibility of the voters and if they have already voted before. Voters receive their encrypted ballots signed by the Voting Authority, if a fraud is detected the voter makes a claim. At the end voters pass the corresponding decrypting keys of the encrypted ballots to the Registry. Ballots and bulletin board information are passed through an anonymous channel.

During the Tallying stage the Voting Authority sends encrypted ballots to the Registry. The ballots are being decrypted and the final results with the votes are listed on the bulletin board. Voters confirm that their ballots are on the bulletin board. If his ballot is not listed correctly, he makes a claim.

C. Consequences

1) Media effects of the voting technology: We will offer different voting/polling media, in order to be able to investigate the effect of media on participation and articulation of opinion. In the three 'real communities', the voting will be done by dividing the population into three groups all using a different medium: traditional paper based voting; electronic voting in various special voting kiosks and online voting from home. In the two virtual communities, the online voting from home or work is one of the two modalities; the second is on-line voting from the. This variety of used media enables us to investigate whether the medium influences participation and the opinion of the voter, as theories of social identity suggest.

2) Learning effects: The fact that someone is confronted with e-voting technology for the first time may influence the willingness to use it, the attitude (trust, fear for monitoring behavior), and the effect on social identity. As we have three ballots over a period of 4 months in the various test sites, and of course some change in group of people participating, we are able to investigate the effects of learning and experience on the use and effects of the e-voting system.

D. Security Analysis

The proposed e-voting scheme is secure, i.e. it satisfies eligibility, privacy, un- reusability, fairness, robustness, individual and universal verifiability and coercion-resistance.

Proof: Eligibility: During the Authorizing stage a voter is registered only after identifying him- self. Only eligible voters receive credential material. Voting Authority ensures eligibility before accepting the ballot by running function if eligible. The Voting Authority cannot impersonate an eligible voter without the official credential issued by the Registry. Therefore, the proposed scheme satisfies eligibility.

©IJRASET 2014: All Rights are Reserved

Unreusability: Each voter possesses different secret key. If a voter tries to vote with the same credential again the Voting Authority detects it since all the necessary values are stored. Since he cannot generate any other voter's credential, every eligible voter can cast a vote only once.

Fairness: Only in the Tallying stage votes are decrypted, and final results are posted, thus during the voting phase no one has information about any intermediate results.

Robustness: Invalid votes cast by malicious voters are detected in the Tallying stage, after decrypting ballot. No coalition of voters can disrupt the election.

Randomization attack: The randomization attack is prevented, since adversary cannot coerce a voter to cast a different, randomly formed, invalid vote. The adversary cannot verify if the coerced voter has cast the prescribed vote or not.

Simulation attack: Even if a voter provides his private keying material (V_{ID}, SK_V) after the Authorizing stage and before the Voting stage, he cannot be coerced by an adversary. An attacker is not able to verify the correctness of the received private keying material.

The proposed scheme satisfies receipt-freeness and protects against randomization, forced-abstention and simulation attack; therefore it is coercion-resistant.

II. CONCLUSIONS

The proposed system fulfills requirements for electronic election schemes, such as eligibility, privacy, unreusability, fairness, robustness, individual and global verifiability and coercion-resistance. It is offered to employ it in a small-scale practical environment (e.g. companies), where the authorities participating do not collude and the voting authority do not collaborate with voters.

REFERENCES

[1] D. Chaum, Elections with unconditionally secret ballots and disruption equivalent to breaking RSA, *In Advances in Cryptology - EUROCRYPT '88, LNCS* Springer-Verlag, 1988; 330, pages 177-182.

[2] C. Boyd, A new multiple key cipher and an improved voting scheme, *In Advances in Cryptology - EUROCRYPT '89, LNCS* Springer-Verlag, 1988; 434, pages 615-625.

[3] A. Fujioka, T. Okamoto, K. Ohta, A practical secret voting scheme for large scale elections, *In Advances in Cryptology - ASISACRYPT '92, LNCS* Springer-Verlag, 1992; 718, pages 244-251.

[4] K.R. Iversen, A cryptographic scheme for computerized general elections, *In Advances in Cryptology - CRYPTO '91, LNCS* Springer-Verlag, 1992; 576, pages 405-419.

[5] C. Park, K. Itoh, K. Kurosawa, Efficient anonymous channel and all/nothing election scheme, *In Advances in Cryptology - EUROCRYPT '93, LNCS* Springer-Verlag, 1993; pages 248-259.

[6] Cetinkaya, O. & Cetinkaya, D. (2007) "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, pp. 903-907.

[7] Chaum, D. (1981) "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms", *Communications of the ACM*, Vol. 24-2, pp. 84-90.

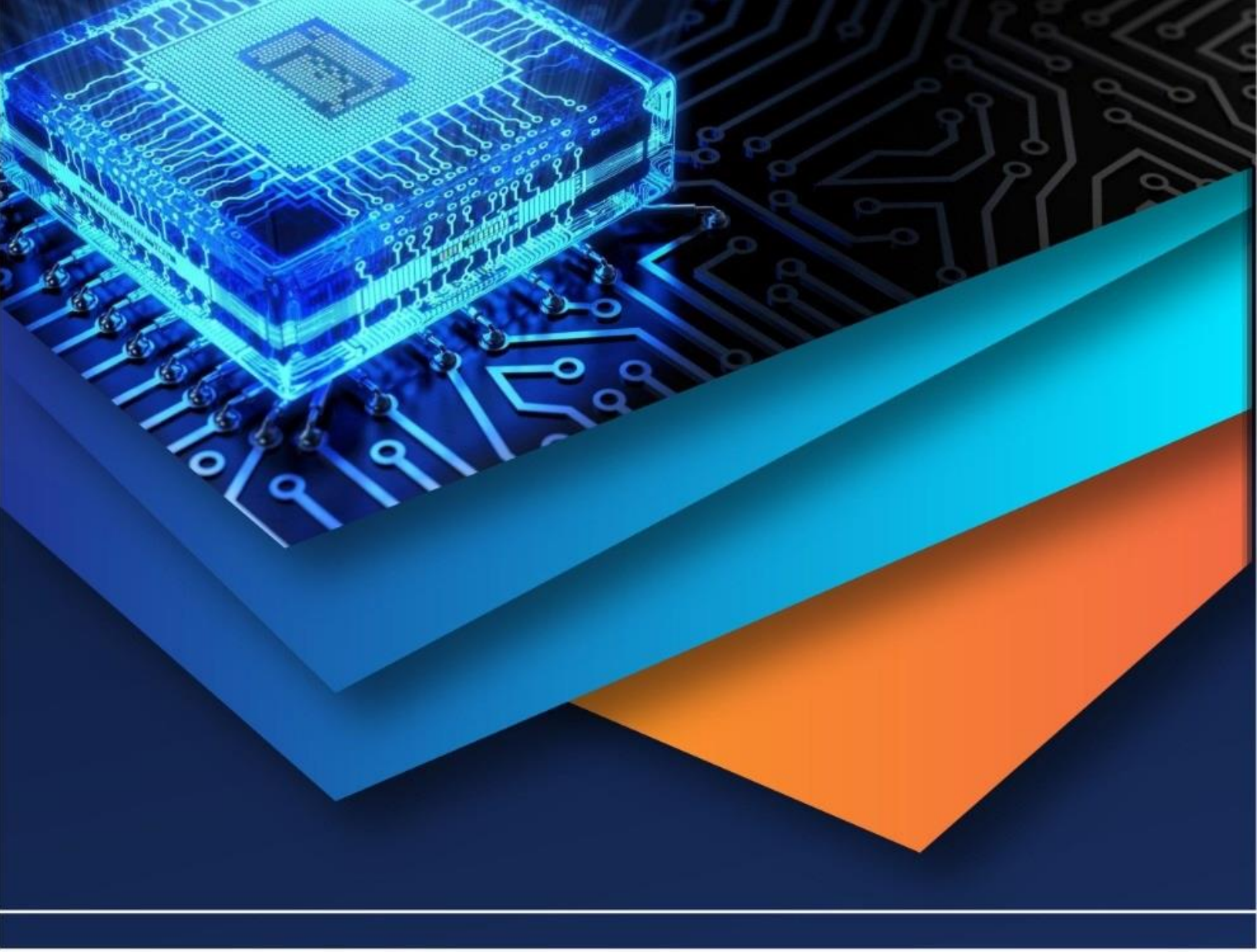
[8] Chaum, D. (1982) "Blind Signatures for Untraceable Payments", *In Proceedings of Advances in Cryptology CRYPTO'82*, pp. 199-203.

[9] Chaum, David (2000) Secret-Ballot Receipts and Transparent Integrity,. David Chaum, draft. Available at http://www.vreceipt.com/article.pdf

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

[11] Fujioka, A., Okamoto, T. and Ohta, K. (1992) "A Practical Secret Voting Scheme for Large Scale Elections", *Workshop on the Theory and Application of Cryptographic Techniques - In Proceedings of Auscrypt'92*, Gold Coast , Australia, pp. 244-251

©IJRASET 2014: All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)