Survey Paper on Variant of New JCJ Protocol

Prachi Kataria.
DYPIET, Ambi.
Dr. D.Y. Patil Educational
Academy, Ambi
Talegaon-Pune.

Bhagyashri Lokhande.
DYPIET, Ambi.
Dr. D.Y. Patil Educational
Academy, Ambi
Talegaon-Pune.

Amol Jadhav
Professor at DYPIET, Ambi.
Dr.D.Y.Patil Educational
Academy,Ambi ,
Talegaon-Pune.

ABSTRACT

Paper, pens, and ballot-boxes, appropriate procedures were used in traditional voting schemes to reassure voters that the result of the tally is correct [1]. Most viable approach to address voter coercion and vote selling in Internet voting is still the basic concept [4]. Its unrealistic computational requirements of the quadratic-time tallying procedure.is one of the main open issues [4]. In this paper, they examine authorization of votes which is the main cause of the issue and the most recent proposals to perform this step in linear time will be summarized. Based on anonymity sets we explain the key underlying concepts of these proposals and introduce a new protocol. However at the negative side, high transparency will generally make it easier for voters to reveal how they voted [1]. Relevant information is published so that the voter may verify that her vote is included in the final tally and that accepted votes have been cast using proper voting material. With the purpose of internet voting protocol it is practically impossible for vote buyers or coercers to elicit the voters' behavior. The efficiency is compared efficiency with existing work under equal degrees of coercion-resistance using an appropriate measure. Internet voting enjoys wide interest from both researches as well as practices [2]. The main purpose of the new protocol is to move computational complexity introduced in recent works from the voter side to the tallying authority side.

Keywords

Quadratic-time tallying, coercion-resistance, computational complexity

1. INTRODUCTION

E-voting elections are far from being a consensus [3].The traditional way of voting over the Internet gains increasing attention as many governments aim at providing their citizens with electronic voting services [3]. They propose a coercion-resistant Internet voting protocol to which they refer as the JCJ protocol. Their protocol has been discussed and analyzed in the literature, and its basic theory till now seems to be the most viable solution to address the voter coercion and vote selling issues. In one way, many people believe that the current technology is enough for deploying such elections in large scale whereas on the other hand, a number of voting researchers and experts do not recommend them nowadays. Therefore, the coercion-resistance property is the most effective one nowadays to fight coercion.

2. AIMS AND OBJECTIVES

1. To give a secure E-voting protocol to the users.

2. To give transparency in the advanced voting system.

3. Efficiency in the counting of vote.

4. Provides accuracy in the vote counting.

3. FIGURES/CAPTIONS

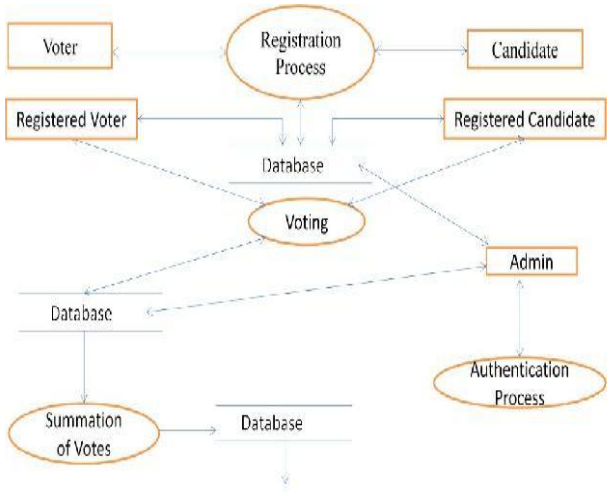

Fig 1: E-voting system working

4. LITERATURE SURVEY

4.1 Towards Practical and Secure Coercion-Resistant Electronic Elections [2010]

Roberto Ara´ujo, Riadh Robbana, Narjes Ben Rajeb, Jacques Traor´e, and Souheib Yousfi

In this paper, they first show that Schweisgut's scheme is insecure. Therefore, they describe an attack that allows a coercer to check whether a voter is followed or not his instructions. They later proceed by presenting a new coercion-resistant election scheme with a linear complexity that overcomes the disadvantages of these previous proposals that has taken place [3].

They have introduced a new coercion-resistant scheme instead of quadrate work factor. In the previous solutions their solution has a linear work factor which has a similar structure like the membership certificate. In the short signature scheme without random oracles. This security is based on the strong Diffie-Hellman inversion assumptions. From the previous schemes, but differently, new credentials are used in one or more elections. By this, there is no need for a new credential to be issued, every time a new election is being taken place.

4.2 Efficient Vote Authorization in Coercion-Resistant Internet Voting [2011]

Michael Schl¨apfer, Reto Koenig, Rolf Haenni; and Oliver Spycher.

In this paper, they examine the cause and effect of this issue, namely the authorization and analyzing of votes, and summarize the most recent proposals to perform this step in linear time. They explain the key underlying or most important concepts of these proposals and introduce a new protocol based on anonymity sets [4].

They have presented improvement of the JCJ protocol which allows authorization of vote efficiency with less computation power on the side of voter basically. It is a mix between SELECTIONS and Spycher et al. Election setup-with comparison to SELECTIONS. Their protocol does not require any election setup.

Vote casting-with comparison to the Spycher et al. protocol, they do not require the authorities to build up take votes during the phase of vote casting and therefore they have reduced the efforts .In this phase for the authorities the advantage of this approach is the fact that of which is the security parameter does not have the client side at all .In this approach β only can affect the server side which is scalable with respect to the computational power.

Vote authentication: the requirements of lower computation for the voters during the voting procedure .yield a lot of effort that is put in the vote authorization phase the security parameter βaffects the server side computational requirement as a linear factor. They have implicitly removed duplications using the linear approach and thy have enlarged the input of the mix-net by the factor. Hence, mixing in their protocol requires additional computational power as compared to other protocols.

4.3 Achieving Meaningful Efficiency in Coercion-Resistant, Verifiable Internet Voting [2012]

Oliver Spycher, Rolf Haenni, Michael Schläpfer. In this paper, they describe an Internet voting protocol that is verifiable and simultaneously makes it practically impossible for vote buyers or coercers to elicit the voters' behavior [1].

It is true that the JCJ protocol provides coercion resistance but only when the protocol is not implemented for large scale elections. Other solution that were proposed either compromise the verifiability or require an off trade between efficiency and coercion resistance during phases that are critical of tallying vote casting there proposal requires a lot of computation however they have proved that when it is compared with other schemes the factor that identifies the computation time is not large for relatively high degree of coercion resistance. Above all the expensive computations that are specific to coercion resistance while the polling is open that is when nobody is waiting therefore, they conclude that their protocol is efficient at both tallying and vote casting.

4.4 Towards A Practical JCJ / Civitas Implementation [7 Jan 2014]

Stephan Neumann, Christian Feier, Melanie Volkamer, and Reto E. Koenig

In this paper, they revise the ARES proposal from a performance view. Based on the proposed revisions herein, they are able to define that the revised ARES proposal is perfect to be used in real-world elections [2].

After years of research theoretically on the topic of E-voting, schemes of scientific internet voting schemes comes up with high security claims. This protocol overcomes the proposal presented by Neumann and Velkamer in 2012 that addressed challenges that were practical by the smart cards that were incorporated into the JCJ and hence this work did not center on the performance they have directed a work which causes this gap. The first part of their work, they have revised the NV12 scheme from a performance base and they were able to remove, outsource or replace smart card operation so as to improve the performance overall. Depending on these revisions, in the second part of their work, they have assessed the timing of smart card for operation that is basic from recent literature. Summarizing this, they calculated the running time of smart card of around 5 second for the voting phase of registration of the NV12 scheme. They were convinced that the outcome of the result proved the NV12 scheme lot feasible that could be applied within the real-world elections they also have discarded the client machine assumptions with respect to forced abstention the implemented NV12 scheme asks the voter not to forget or must type her PIN. This implementation may be too strong and should be considered in the future research.

5. EXISTING WORK

In the existing system, they have applied a new scheme for the following cryptographic primitives: the ones not employed by the JCJ protocol are identified accordingly. In justifying coercion resistance and verifiability in the duration of their exposition, they assume primitives to be ideal. In today's date we are having both manual voting and e- voting. Because of this scenario all citizens and public must be applied for voter id and by using this we can go for manual voting or remote voting. To do this operation every time voters must go to outlets and at the same time politicians also must go to outlets for processing nominations. This is the main drawback in present scenario. To overcome this problem they are going to introduce a web based application called "Automated ballot vote".

5.1 Disadvantages

1. Time consuming process.

2. Results will come very late.

6. PROPOSED WORK

Automated ballot vote is a management system that has been developed for automating the process of vote proceedings that take place between the people of the nation, and the government. The system needs consistent flow of information and data at different levels within the automated ballot vote system, any interruption in the flow of data can cause the final verdict to get stalled. These kinds of situations should be holding our automated ballot vote system.

Data maintenance becomes a vital component with proper relation at all different stages. The systems also becomes false proof for data and information attractions at any stage, because the whole control of information and data is kept in the hands of different administrations working at different levels of the work.. The authority of data manipulation is handled with proper authentication, but all the actions in the system can execute queries upon the system as per the substantial standardizations as we arise when the system is under the operational standards.

6.1 Advantages

1. It will save our valuable time.

2. Results will come very early

3. Removes invalid and duplicate votes.

4. Efficient for large e-voting system

7. CONCLUSION

Many e-voting techniques have been initiated in last decades**.** However, using these uncovered data or pattern in the field of e-voting is hard to implement and too much effective. In this research work, an effectual discovery technique has been established to overcome he low rate of misapprehension problems for e-voting, This proposed technique uses the election model and definition of coercion resistance produced by Juel et al.

8. ACKNOWLEDGMENT

Our special thanks to all those who have provided us valuable guidance towards the completion of this project. We hereby take this opportunity to record our sincere thanks and heartily gratitude **Project Guide Prof. Amol Jadhav and Coordinator Vibha Lahane** , without whom we would have not started authoring this paper and also for their useful guidance and making available their intimate knowledge and experience

9. REFERENCES

[1] Achieving Meaningful Efficiency in Coercion-Resistant, Verifiable Internet Voting Oliver Spycher, Reto Koenig, Rolf Haenni, Michael Schläpfer.

[2] Towards A Practical JCJ / Civitas Implementation Stephan Neumann1, Christian Feier1, Melanie Volkamer1, and Reto E. Koenig2

[3] Towards Practical and Secure Coercion-Resistant Electronic Elections Roberto Ara´ujo, Narjes Ben Rajeb, Riadh Robbana, Jacques Traor´e, and Souheib Yousfi

[4] Efficient Vote Authorization in Coercion-Resistant Internet Voting Michael Schl¨apfer, Rolf Haenni, Reto Koenig; and Oliver Spycher.