VOTING VIA DIGITAL MEDIA

Prof. Pushpa Mahapatro

Assistant Professor, Vidyalankar School of Information Technology.

Abstract :

This paper presents a method to conduct Voting via Digital Media. It also discuss about the infrastructure needed for this. It also talks about the main concerns for such virtual elections. Digital Signatures and encryption can be used for conducting virtual elections in a secure and unbiased manner. With the technique proposed in this research paper, we can achieve Confidentiality and Authentication. Replay attack is not possible and there is limited association between the Digital Signature of the user and vote cast by the user. So, it cannot be identified that who has voted for whom. Hence this research paper provides a secure and efficient way of conducting elections on internet.

Keywords: *Public key, private key, Digital Signature, Authentication, Integrity, Fabrication.*

INTRODUCTION

A voting system or electoral system is a method by which voters make a choice between options, often in an election. A voting system enforces rules to ensure valid voting, and how votes are counted and aggregated to yield a final result [1]. Common voting systems are majority rule, proportional representation with a number of variations and methods such as first-past-the-post or preferential voting [2]. The study of formally defined voting systems is called social choice theory or voting theory, a subfield of political science, economics, or mathematics.

With majority rule, those who are unfamiliar with voting theory are often surprised that another voting system exists, or that disagreements may exist over the definition of what it means to be supported by a majority. Depending on the meaning chosen, the common "majority rule" systems can produce results that the majority does not support. If every election had only two choices, the winner would be determined using majority rule alone [3]. However, when there are three or more options, there may not be a single option that is most liked or most disliked by a majority. A simple choice does not allow voters to express the ordering or the intensity of their feeling. Different voting systems may give very different results, particularly in cases where there is no clear majority preference [4, 5].

PROBLEMS FACED:

1.Is it technically possible to have elections on the internet? How? What sort of infrastructure would be needed for this?
2. What would be the main concern in such a virtual election?
3. What would be the use of digital signatures and encryption in virtual elections? [8, 9]

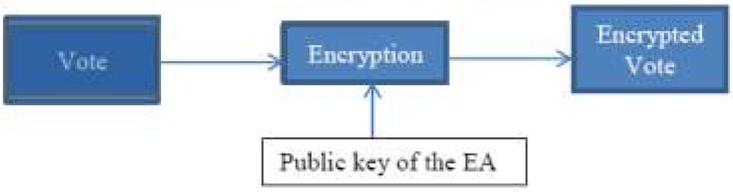
OBJECTIVE:

Cryptography is very useful in conducting voting via Internet. Computerized voting would become quite common in next few decades. As such, it is important that the protocol for virtual elections should protect individual privacy and should also disallow cheating.

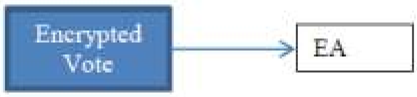
RESEARCH METHODOLOGY:

Consider the following protocol in order that voters can send their votes electronically to the Election Authority (EA) [6, 7]:

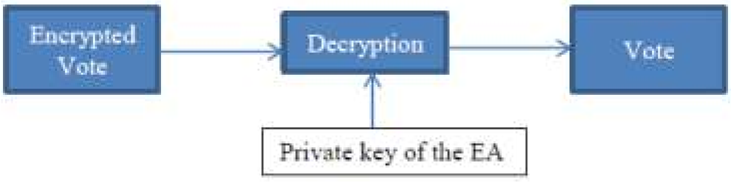
1. Each voter cast the vote and encrypts it with the public key of the EA.



2. Each voter sends encrypted vote to the EA.



3. The EA decrypts all the votes to receive the original vote, tabulates all the votes and announces the result of the election.



FINDINGS:

Is this protocol secure and does it provide comfort both to the voters as well as to the EA? The answer is that it does not because it has the following problems:

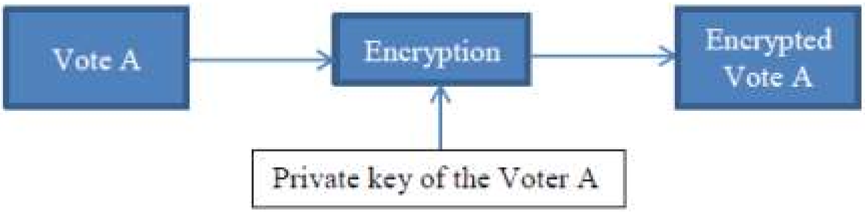
1. The EA does not know whether the authorized voters have voted or it has received fake (bogus) votes.
2. Secondly, there is no mechanism to prevent duplicate voting. It is also known as Replay attack wherein the hacker sends the same message again and again.

What is the advantage of this protocol? Clearly, no one would be able to change another voter's vote, because it is first encrypted with EA's public key and is then sent to the EA. However if we observe this scheme carefully, an attacker need not change someone's vote at all. The attacker can simply send duplicate votes.

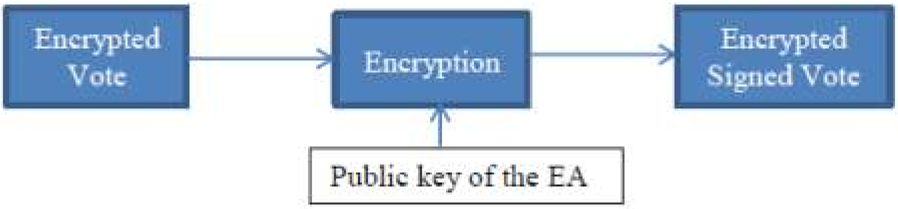
STRATEGY:

How can we improve upon this protocol to make it more robust? Let us rewrite it as follows:

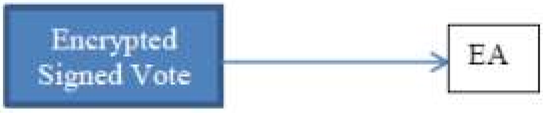
1. Each voter cast the vote and signs it with her private key.



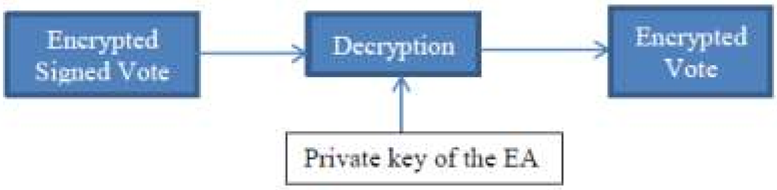
2. Each voter then encrypts the signed vote with the public key of the EA.

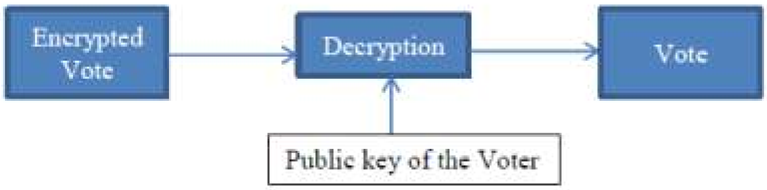


3. Each voter sends the vote to the EA.



4. The EA decrypts the vote with his private key and verifies the signature of the voter with the help of the voter's public key.





5. The EA then tabulates all the votes and announces the result of the election.

This protocol would now ensure that duplicate voting is disallowed. Because the voter has signed the vote (with his/her private key) in Step 1, this can be checked. Similarly, no one can change another voters vote. This is because a vote is digitally signed and any changes to it will be detected and exposed in the signature verification process.

Although this protocol is a lot better, the trouble with this scheme is that the EA would come to know who voted for whom, leading to privacy concerns. We shall now see how this problem can be solved.

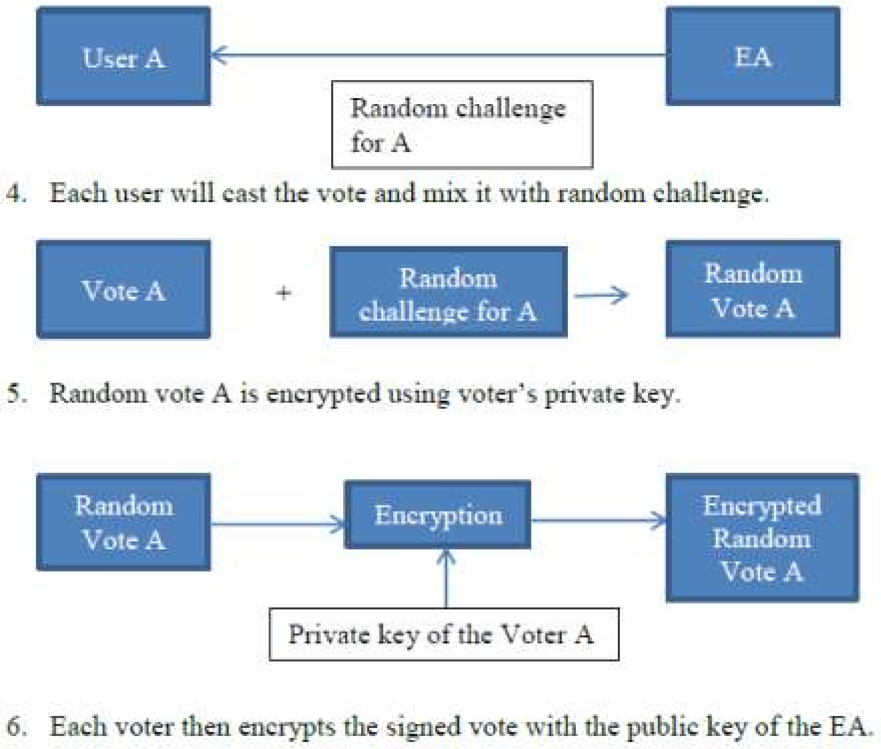
OUR REQUIREMENT IS THAT –

1. Verifying the sender's identity: The senders identity needs to be verified using digital certificate.
2. Hiding the sender's identity: The sender's identity should be hidden on internet.
3.Hiding the information that who has voted for whom: The EA should not be able to find that who has voted for whom.
4. A user can vote at his vote at his leisure.

How can we improve upon this protocol to make it more robust? Let us rewrite it as follows again.

PROPOSED ALGORITHM:

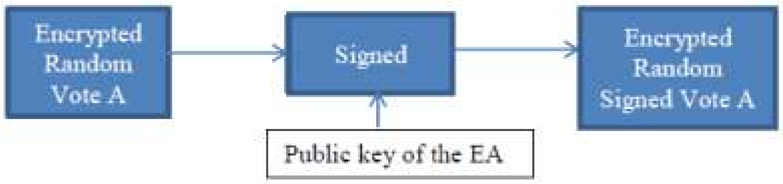
1. Each voter will have his digital certificate to prove his identity on internet.
2. A fixed time slot will be allotted to the users during which they can cast their vote.
3. EA will generate a random challenge for each user and send it to them on internet.



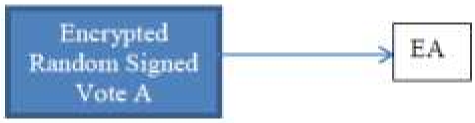
4. Each user will cast the vote and mix it with random challenge.

5. Random vote A is encrypted using voter's private key.

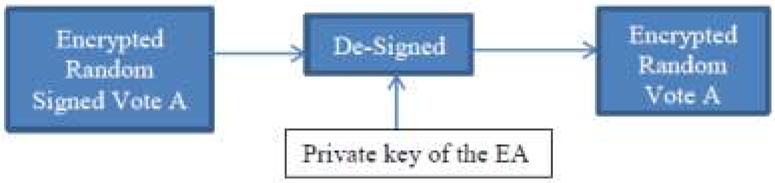
6. Each voter then encrypts the signed vote with the public key of the EA.

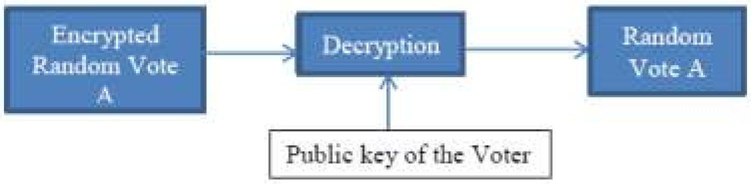


7. Each voter sends the vote to the EA.

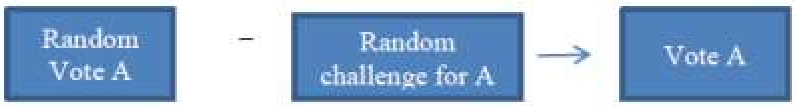


8. The EA decrypts the vote with his private key and verifies the signature of the voter with the help of the voter's public key.





9. The EA then separates the random challenge from the vote.



10. The EA then tabulates all the votes and announces the result of the election.

CONCLUSION:

With the technique proposed in this research paper it can be concluded that we can achieve confidentiality because encrypted vote is send on internet. Authentication is achieved using digital signature. Replay attack is not possible because the user to whom random challenge is send will cast the vote only once. There is limited association between the Digital Signature of the user and vote cast by the user. So, it cannot be identified that who has voted for whom.

Hence this research paper provides a secure and efficient way of conducting elections on internet.

BIBLIOGRAPHY:

1.The Virtual Polling Station, Transferring the Sociocultural Effect of Poll Site Elections to Remote Internet Voting by Philipp Richter, Allee 64-66, 34109 Kassel, Germany.
2. A Virtual Election in a Fantasy Chechnya, By Svante E. Cornell.
3. A Fast Distributed and Efficient Virtual Backbone Election in Large Scale MANETs by Wasim El-Hajj,

College of Information Technology, UAE University, United Arab Emirates and Mohsen Guizani, College of Information Technology, UAE University, United Arab Emirates.

4. Power Aware Reliable Virtual Machine Coordinator Election Algorithm in Service Oriented Systems by Danial Rahdari, Mahdi Golmohammadi, AbasPirmoradi
Department of Computer Science, ShahidBeheshti University, Tehran, Iran.

5.Secure Virtual Election Booth with Two Central Facilities by Janga Sireesha, So-In Chakchai, Department of Computer Science Washington University in St. Louis, USA.

6.Introduction to the Virtual Issue: Election Fraud and Electoral Integrity by Ines Levin, Department of Political Science, University of Georgia, Athens, GA 30602 and R. Michael Alvarez, Division of Humanities and Social Sciences, California Institute of Technology, Pasadena, CA 91125.

7.Virtual Election Booth, 8th February 2003, This project implements the secure election protocol described in [SCHN96], p. 127 (Voting with Two Central Facilities).

8.You Go to Elections with the Voting System You Have: Stop-Gap Mitigations for Deployed Voting Systems by J. Alex Halderman (Princeton University), Hovav Shacham (University of California), and David Wagner (University of California).

9. Cryptography and Network Security by AtulKahate, 2nd Edition, Tata McGrawHill.

10. Cryptography and Network Security by William Stallings, Fifth Edition, Pearson Education.

11. Cryptography: Theory and Practice by Douglas Stinson, CRC Press, CRC Press LLC.