

Mobile voting (chance or challenge)

Somayeh Izadi¹ Saeed Zahedi², Kamran Morovati³, Reza Ebrahimi Atani⁴

¹ Department of Information Technology The University of Guilan, Rasht, Iran

² Department of Information Technology The University of Guilan, Rasht, Iran

³ Department of Computer Science University of Pune, PhD candidate in security, Pune, India

⁴ Department of Computer Engineering The University of Guilan, Rasht, Iran

Abstract : - Traditional election has many obscurity and people trust it difficult. Governments try to get dependence in society and it has no way except move to E-democracy. But there is many challenges in it. There are some security requirements such as Performance, Comfortable, Availability, Privacy, Eligibility that provide with Mobile voting simply.

Keywords: - E-Government; E-Democracy; M-Voting; Mobile infrastructure; Mobile requirements security

I. INTRODUCTION

E-Democracy is base of E-Governments. Dependency of people to government is like root and leads the society to national alliance. Voting is the best form and symbol to displaying democracy. But there was many ways to fluctuation in traditional voting. We discuss about E-government and democracy and then expression Electronic voting with disadvantages. So introduce Mobile voting as a good way to implement democracy. We notify voting requirements for mobile voting.

II. ELECTRONIC GOVERNMENT

E-government describes the use of technologies to facilitate the operation of government and the dispersement of government information and services. E-government, short for electronic government, deals heavily with Internet and non-internet applications to aid in governments. E-government includes the use of electronics in government as large-scale as the use of telephones and fax machines, as well as surveillance systems, tracking systems such as RFID tags, and even the use of television and radios to provide government-related information and services to the citizens.

The ultimate goal of the E-Government is to be able to offer an increased portfolio of public services to citizens in an efficient and cost effective manner. E-government allows for government transparency. Government transparency is important because it allows the public to be informed about what the government is working on as well as the policies they are trying to implement. Simple tasks may be easier to perform through electronic government access. Many changes, such as marital status or address changes can be a long process and take a lot of paper work for citizens. E-government allows these tasks to be performed efficiently with more convenience to individuals. E-government is an easy way for the public to be more involved in political campaigns. It could increase voter awareness, which could lead to an increase in citizen participation in elections. It is convenient and cost-effective for businesses, and the public benefits by getting easy access to the most current information available without having to spend time, energy and money to get it.

E-government helps simplify processes and makes access to government information more easily accessible for public sector agencies and citizens.

Bertot and Jaeger [1] point introduce some ways to achieve cost savings in a citizen-centered government through e-government services; governments should get wishes of e-Government services. So we do these:

- Governments should evaluate information, service and technology.
- Government learns the technology to citizen. Of course it's a duplex operation and government members should understand new technology.
- Usability, functionality and accessibility assessment permanent.

III. E-DEMOCRACY

E-democracy is concerned with the use of information and communication technologies to engage citizens, support the democratic decision-making processes and strengthen representative democracy

Citizens are the heart of democracy. Democracy is kind of system of government that is depends on citizen satisfaction.

The freedom to connect – the idea that governments should not prevent people from connecting to the internet, to websites, or to each other. The freedom to connect is like the freedom of assembly, only in

cyberspace. It allows individuals to get online, come together, and hopefully cooperate. Once you're on the internet, you don't need to be a tycoon or a rock star to have a huge impact on society [2].

A. The dimensions of electronic democracy

Information: There is clear information from government to citizen.

Communications: Interaction between people and government.

Participation: develop opportunities for people to develop partnerships.

Freedom: including freedom of speech, free press, of assembly and free voting.

B. Processes and Goals

E-democracy has three processes:

1. Information Rotation
2. Ideas
3. Decisions

The electronic democracy has two goals:

1. Electronic participation that is a prerequisite of decision. (Processes 1 and 2).
2. Electronic voting. (Process 3).

IV. E-VOTING

Electronic voting systems are increasingly replacing the traditional paper-based voting systems. These systems can make the voting process more convenient and may, therefore, lead to improved turnout. Electronic recording and counting of votes could be faster, more accurate, and less labor intensive [3].

There are three classical cryptographic techniques for electronic voting [4]:

A. Homomorphic scheme

Homomorphism is an algebraic property particularly useful in electronic voting schemes because it allows applying operations on sets of encrypted ballots without need of decrypting them. In a homomorphic voting system, the clear text ballots are never visible to anyone except the voter. The encrypted ballots are made public and are aggregated in encrypted form. The encrypted tally is then decrypted. These systems require special types of homomorphic encryption schemes, and homomorphic counters, which enable the computation of the encrypted tally from the encrypted votes. A function F is said to be an (\oplus, \otimes) homomorphism if $F(a) \oplus F(b) = F(a \otimes b)$. In particular, if F is an encryption function, and $a \oplus b$ are votes, and \oplus is regular addition; the encrypted tally is obtained by applying F to the encrypted votes. In a homomorphic encryption scheme anyone can check that the encrypted tally is computed correctly, as all the encrypted ballots are public [4].

B. Blind Signature

A blind signature allows somebody for instance an authority to sign an encrypted message without decrypting it. Once the message signed and resent to the sender, he has a signed version of his vote by the authority and a guarantee that his vote has not been seen [5].

Formally, the blind signature scheme with message space M is a 5-tuple $(\eta; \chi; \sigma; \delta; \Gamma)$, where

- a) η is a polynomial-time probabilistic algorithm, that constructs the signer's public key (pk) and its corresponding secret key (sk);
- b) χ is a polynomial-time blinding algorithm, that on input a message $m \in M$, a public key pk and a random string r , constructs a blind message m' ;
- c) σ is a polynomial-time signing algorithm, that on input a blind message m' and the secret key sk constructs a blind signature s' on m' ;
- d) δ is a polynomial-time retrieving algorithm, that on input a blind signature s' and the random string r extracts a signature s on m ;
- e) Γ is a polynomial-time signature-verifying algorithm that on input a message signature pair $(m; s)$ and the public key pk outputs either yes or no.

Blind signature is often used to get a token from the authority: The voter gets a signature from the authority of his ballot and then he is able to cast his ballot. It is used to achieve eligibility.

C. Mixnet

After finishing the voting, when all voters vote using a ballot box, votes come out in a different order. This ensures the anonymity of the voter. One possibility to realize it electronically is to use so-called mix-net first introduced by Chaum [6]. In these protocols mix messages by sending them through a network of authorities, where each authority shuffles the received list of messages before to send it to the next one, while keeping the permutation secret to send it to the next one, while keeping the permutation secret[5].

V. E-VOTING DISADVANTAGES

1. There is no documentary evidence and tangible results of the election.
2. Votes collect, store and be counted electronically, so it can not be proved that the results are consistent with the votes of the mass electorate.
3. It is possible for hackers to access and modify the results to their advantage.
4. It's possible to identify the voters. Privacy is weak.
5. Tallying is difficult without using the paper in voting process.
6. Security of these systems is difficult and almost no one can verify the health and assurance of election.
7. Initial costs for software and hardware infrastructure are high.
8. Control and protection of networks that connect users to the central server can be tricky.
9. Rules and standards for this work are still undefined.

VI. INFRASTRUCTURE OF M-VOTING

Mobile voting (m-Voting) can be seen as an additional platform to the electronic voting systems. It is an m- Government initiative with tremendous potentials to enhance democratic participation [9]. It will also serve as an enabler and a convenient way to involve citizens in political decision making. It is a cheaper, convenient, and a simple to administer voting alternative. Mobile phone users can subscribe to GSM operators that will incorporate an m- Voting system service which will enable them to participate in choosing political candidates into government seats. M-Voting is not a replacement for e-voting, but rather a complement [10]. The use of mobile devices in political participation simplifies and eases access to and the integrating of persons and institutions in political processes. With SMS, Multimedia Message Service (MMS), and emerging applications offered by mobile computing, m-Voting can enhance the citizen's input to political decision-making and increase their democratic participation.

A. *Technical infrastructure*

Holding a successful election, needs power technical infrastructure than should be secure in communications network. Mobile voting is product of a set of technical, scientific, legal software and hardware, and work is ongoing.

Implementation voting without infrastructure is a large risk for government and maybe can unrepeatable. Because of importance of voting and challenges which can start a war in countries, at first;

“Government should provide infrastructure.”

Challenges of employing electronic elections in the country are as follows:

Legal challenges are the existing laws inconsistent with the necessary electronics and new elections.

Political - social challenges: the impact of modern information and communication technologies on electoral systems.

Technical challenges are connection with the techniques of system security, voter's identity and privacy of votes.

Cultural challenges are a lack of equality of citizens' information literacy and lack of sufficient skills in using new technologies.

B. *Legal infrastructure*

Holding the mobile voting needs clear-cut rules that eliminate ambiguity to executing, observers, candidatures and voters. Before definition the rules, discussion is useless.

C. *Cultural infrastructure*

Failure to adopt between people and governors cause distance and cost for government. For remoteness of this cost should explain voting method to people and test it before main voting. So all people an organization which are involved in election, will justified.

VII. M-VOTING ADVANTAGES VS. E-VOTING

1. There is no ballot to make fail possibility.
2. Reducing manpower requirements as well as polling places.
3. There is the possibility of counting the votes at any time.
4. There will be no queue.
5. Reduction of costs.
6. All of people in any classes and age have better access to mobile than. So there will be more welcome.
7. People trust to their own personal mobile phones is more than another devices and Internet.
8. The Voter can vote from any place in any time.,
9. The possibility of voting is for the disabled and illiterate, very simple.

VIII. SECURITY REQUIREMENTS FOR MOBILE VOTING

In different protocols, according to kind of elections and applications, we need different stages and different requirements. In order to be usable in practice, electronic voting scheme has to satisfy some requirements.

A. Verifiability

A voter should be able to verify whether his vote was correctly recorded and accounted in the final vote tally. We distinguish between individual and universal verifiability. In the latter case not only the voter but anyone can verify that all valid votes were included and the tally process was accurate.

B. Dispute-freeness

A voting scheme must provide a mechanism to resolve all disputes at any stage.

C. Accuracy

A voting scheme must be error-free. Votes of invalid voters should not be counted in the final tally.

D. Fairness

No one should be able to compute a partial tally as the election progresses.

E. Robustness.

A scheme has to be robust against active or passive attacks and faults as well.

F. Receipt-freeness

A voter should not be able to provide a receipt with which he may be able to prove his vote to any other entity.

G. Practicality

A voting scheme should not have assumptions and requirements that may be difficult to implement for a real application.

H. Eligibility

Only valid voters who meet certain pre-determined criteria are eligible to vote.

I. Privacy

In a secret ballot, a vote must not identify a voter and any traceability between the voter and his vote must be removed.

J. Individual verifiability

Each eligible voter can verify that his vote was really counted.

K. Universal verifiability

Any participant or passive observer can check that the election is fair: the published final tally is really the sum of the votes.

L. Incoercibility

Say that the scheme is incoercible if the voter cannot convince any observer how he has voted. This requirement prevents vote-buying and coercion.

M. Democracy

No voter can vote more than once.

N. On-line property

A voter can join or leave the voting session at any time without losing the possibility to vote once.

O. Walk-away property

After a voter has cast his vote he can leave the voting session (“walk-away”) with the assurance that his vote is counted.

P. Availability

A voter eventually succeeds in casting a vote.

Q. Anonymity

No one can't access to any vote.

R. Performance

E-voting systems should can faced with any problem in high volume and can continue their activities and ultimately count the obtained valid votes, and then to inform the results with end of performance.

S. Comfortable

Any one even the handicapped and illiterate can vote.

IX. CONCLUSION

Presence of mobile in modern life is undeniable. It can replace for many devices, such as camera, video camera, phonebook and ..., So according to the requirements stated importance usage of mobile voting will be displayed more. Mobile provides performance, comfortable, democracy, privacy, availability more than E-voting.

REFERENCES

- [1] J. C. Bertot, P. T. Jaeger, "The E-Government paradox: Better customer service doesn't necessarily cost less, Government Information Quarterly", Volume 25, Issue 2, April 2008, pp. 149-154.
- [2] H. Cilinton, "Remarks on Internet Freedom." U.S. Department of State. 21 Jan. 2010. Web. 15 Mar. 2011. <<http://www.state.gov/secretary/rm/2012/01/135519.htm>>
- [3] K. Weldemariam, R. A. Kemmerer, A. Villaforita, "Formal Specification and Analysis of an e-Voting System", International Conference on Availability, Reliability and Security, 2010.
- [4] S. Ppoveniuc, "A Framework For Secure Mixnet-Base Electronic Voting", Phd thesis, Washington University, 2009.
- [5] L. Fouard, M. Duclos, P. Lafourcade, "Survey on Electronic Voting Schemes", VERIMAG, 2 avenue de Vignate, 38610 Grières, France.
- [6] D. L. Chaum. "Untraceable electronic mail, return addresses, and digital pseudonyms. Commun". ACM, 24(2):84-90, 1981.