ISSN No. 0976-5697

Volume 3, No. 5, Sept-Oct 2012

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Advances In Mobile Voting

Somayeh Izadi*, Saeed Zahedi
Department of Information Technology Engineering
The University of Guilan
Rasht, Iran
ecom.izadi@yahoo.com*, zahedi@msc.guilan.ac.ir

Kamran Morovati
Department of Computer Science University of Pune,
PhD candidate in security Pune, India,
kamran@cs.unipune.ac.in

Reza Ebrahimi Atani
Department of Computer Engineering
The University of Guilan
Rasht, Iran
rebrahimi@guilan.ac.ir

Hadi Foroutan Jazi
Department of Computer Engineering
Islamic Azad University of Doaltabad
Dolatabad, Isfahan, Iran
foroutan1382@yahoo.com

Abstract: E-Government appearance, leads the society to implement electronically all jobs. One of them is voting. Voting is a kind of democracy scheme. After introducing e-voting, many challenges appeared. Such as security requirements which often attacked to them. We introduce M-voting as a tool for increase performance and comfortably whereas will result in increased social participation. Here we express main e-voting disadvantages vs. m-voting advantages. We will disuse about attacks on security requirements.

Keywords: E-Democracy; M-Voting;; Mobile requirements security; Blind Signature; mix net.

I. INTRODUCTION

Because of many problems involved in traditional voting, such as vote counting, fraud, Loosing of time and money, so government goes to e-voting. But today, after years of working on of electronic voting and numerous implementations, there are still a lot of problems.

From the main problems can be pointed to attacks which did on all introduced protocols. We will see the largest number of attacks have been on robust, second, receipt freeness.

II. 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.

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 [1].

A. The Dimensions of Electronic Democracy:

- ***a. Information:*** There is clear information from government to citizen.
- ***b. Communications:*** Interaction between people and government.
- ***c. Participation:*** develop opportunities for people to develop partnerships.
- ***d. Freedom:*** including freedom of speech, free press, of assembly and free voting.

B. Processes and Goals:

E-democracy has three processes:

a. Information Rotation
b. Ideas
c. Decisions

The electronic democracy has two goals:

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

III. ELECTRONIC VOTING AND DEMOCRACY

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 [2].

Electronic voting scheme consists of three main stages: initialization stage, voting stage, and counting stage. The stage can consist of more phases.

A. Initialization stage:

At this stage, authorities set up the system. They announce the elections, formulate the question and possibilities for an answer, create a list of eligible voters, and so on. They generate their public and secret keys, and publish the public values.

B. Voting stage:

Voters are casting their votes. The voter communicates with authorities through the channels he can use, forming a ballot containing his vote. Finally he sends his ballot to its destination.

C. Counting stage:

Authorities use their public and secret information to open the ballots and count the votes. They publish the result of elections.

In Democracy the governmental power is transferred by counting secret votes during elections. To accept such transfer people and parties must be 100% sure that electoral results are fair and square: doubts about the legitimacy of the winner can damage the political life of the country and even bring riots and revolutions.

Votes must be forever secret from everybody because otherwise voters could undergo illicit pressure to vote according to somebody else's will. Criminals (and/or governments and/or politicians) have enough power to compel people to vote in a certain way.

Electoral procedures are obviously setup and managed by large organizations which span all over the country and give contracts to private and public companies.

Many people and/or organizations are interested in falsifying electoral results to maintain or to get the governmental power. They can be highly motivated, well financed, sophisticated, and could be outsiders as well as insiders with full knowledge of the election system. These attackers could be political operatives, voters, vendor personnel, polling place workers, election administrators, foreign countries, international terrorist organizations, or just pranksters.

Sitting governments are in charge of guaranteeing the accuracy of electoral results and the secrecy of votes, but the social groups & the economical powers which are the base of any government have the obvious interest in falsifying electoral results and violating the secrecy of votes to preserve the power. They could also succeed thanks to the complete control they have over the electoral process [3].

Figure 1. Electronic voting models

IV. MOBILE VOTING

Mobile voting systems have the potential to improve traditional voting procedures by providing added convenience and flexibility to the voter. Numerous electronic voting schemes have been proposed in the past, but most of them have failed to provide voter authentication in an efficient and transparent way. On the other hand, GSM (Global System for Mobile communications) is the most widely used mobile networking standard. There are more than one billion GSM users worldwide that represent a large user potential, not just for mobile telephony, but also for other mobile applications that exploit the mature GSM infrastructure [4].

V. INTERNET VOTING

Two types of Internet voting are possible, and both were used in voting trials in 2000. One method, the more basic from a technical stand point, is Internet voting at a traditional polling site, with computer voting machines connected to the Internet and where election officials authenticate voters before ballots are cast. The other method, more technically advanced, is to cast ballots over the Internet from remote locations using electronic authentication and computer security technologies.

VI. E-VOTING DISADVANTAGES

a. One had to stand in queue to cast his vote for many hours. This was very time consuming.
b. While counting of votes was usually manually so it needed many days to declare the results of election [3].
c. There is no documentary evidence and tangible results of the election.
d. 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.
e. It is possible for hackers to access and modify the results to their advantage.
f. It's possible to identify the voters. Privacy is weak.
g. Tallying is difficult without using the paper in voting process.
h. It was the worst limitation of previous voting processes. As we know that election's result can differ by the small margin of one or two votes and if there is error in counting the votes the entire result may change.
i. It was the big threat in previous voting processes. In recently conducted elections there was a great percentage of fake voting, and this type of frauds are not acceptable in democratic countries like India [3].
j. Security of these systems is difficult and almost no one can verify the health and assurance of election.
k. Initial costs for software and hardware infrastructure are high.
l. Control and protection of networks that connect users to the central server can be tricky.
m. Rules and standards for this work are still undefined.
n. As discussed earlier there was a great need of manpower to count the votes, also the security personnel need was necessary.

VII. M-VOTING ADVANTAGES VS. E-VOTING

a. There is no ballot to make fail possibility.
b. Reducing manpower requirements as well as polling places.
c. There is the possibility of counting the votes at any time.
d. There will be no queue.
e. Reduction of costs.
f. All of people in any classes and age have better access to mobile than. So there will be more welcome.
g. People trust to their own personal mobile phones is more than another devices and Internet.
h. The Voter can vote from any place in any time.,
i. 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 [5, 6, 11-13].

C. Accuracy:

A voting scheme must be error-free. Votes of invalid voters should not be counted in the final tally [5, 7].

D. Fairness:

No one should be able to compute a partial tally as the election progresses [6-8].

E. Robustness:

A scheme has to be robust against active or passive attacks and faults as well [7, 8, 11].

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 [6].

In some works, receipt-freeness means that the protocol does not require receipts, but in this paper, we consider receipt-freeness as uncoercibility because some voting protocols can give "receipts" to voters without the voter being able to use these to prove his vote whereas others need not supply voters with receipts in order for voters to be able to construct proofs of how they voted

G. Practicality:

A voting scheme should not have assumptions and requirements that may be difficult to implement for a real application [7].

H. Eligibility:

Only valid voters who meet certain pre-determined criteria are eligible to vote [5, 6, 11].

Prevention of Multiple Voting All eligible voters are allowed to cast the scheduled vote's number (function of the election system and his part in it) and not more, such that each voter has his intended power in deciding the outcome of the voting.

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 [5, 8 12].

- ***a. Perfect Privacy***: No coalition of participants (voters or authorities), not containing the voter himself, can gain any information about the voter's vote.
- ***b. n-Privacy***: No "n-coalition of participants", not containing the voter himself, can gain any information about the voter's vote. ("n-coalition of participants" means coalition of at most n authorities and any number of voters.)

J. Individual verifiability:

Each eligible voter can verify that his vote was really counted [8].

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 [7, 8].

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 [6, 11, 12].

M. Democracy:

No voter can vote more than once [5- 11].

N. On-line property:

A voter can join or leave the voting session at any time without losing the possibility to vote once [7].

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 [7].

P. Availability:

A voter eventually succeeds in casting a vote.

Q. Anonymity:

No one can't access to any vote [5- 11].

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. APPROCHES OF 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 [14].

There are three classical cryptographic techniques for electronic voting [15]:

a. Homomorphic
b. Blind Signature
c. Mix net

A. Homomorphic:

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 ⊕ b are votes, and is regular addition; the encrypted tally is obtained by applying 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 [15].

B. Blind Signature:

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 [8].

Formally, the blind signature scheme with message space 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. Mix net:

Anonymity is a sub discipline of information hiding, required in a number of applications, such as in electronic voting. For network communications, anonymity can be provided by a mix network (mixnet). A mixnet is a multistage system that uses cryptography and permutations to provide anonymity. The basic idea of a mixnet has evolved into a number of different classes. In addition to presenting the existing mixnet classifications, this paper classifies mixnets based on the verification mechanisms employed for robustness.

The construction of mixnets is presented under a common framework to provide insight into both the design and weaknesses of existing solutions. Basic forms of attack on mixnets and the corresponding robustness solutions are reviewed. Comparison with other solutions for anonymity and suggestions for interesting future research in mix networks are also provided[16].

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 [17]. 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[8].

The design of a mixnet is based on providing anonymity for a batch of inputs, by changing their appearance and removing the order of arrival information. the main component of a mixnet is the stage, also known as the mix, that performs mixing on a batch of inputs. Note that the inputs may arrive at the stage at different times. The mixing operation involves a cryptographic transformation using either decryption or encryption, which changes the appearance of inputs, followed by a permutation on the batch of transformed inputs. A mix network consists of several interconnected stages depending on the robustness of anonymity required. Each stage performs mixing on its inputs, and the mixed batch is then forwarded to the next stage in the mixnet or directly to their destinations. The interconnection of the stages determines the mixnet topology, and based on the topology of the mixnet, there can be a cascade mixnet or a free-route mixnet,

We review common E-voting protocols in using of approaches. Results show in table1.

Table1. Using approaches in common E-voting protocols

Homomorphism	Blind Signature	Mix net
Cohen and Fischer 1985	FOO 1992	Chaum 1982
Benaloh and Yung 1986	Radwin 1995	Rjaskova 2002
Benaloh and Tuinstra 1994	Juang and Lei 1997	Lee, Boyd, Dawson,Kim, Yang,Yoo 2003
Cramer ,Gennaro and Schoenmakers 1997	Mu and Varadharajan 1998	Prêt-à-Voter 2005
Hirt and Sako 2000	Juang, lei and Yu 1998	Weber 2006
	Ohkubo,Miura,Abe ,Fujioka,Okamoto 1999	
	K.Kim, J.Kim, Lee, Ahn 2001	

We have some security requirements for mobile voting. Based on survey in attacks on protocols in [8], we can draw diagram1. It shows than most attacks have been on the robustness requirement.

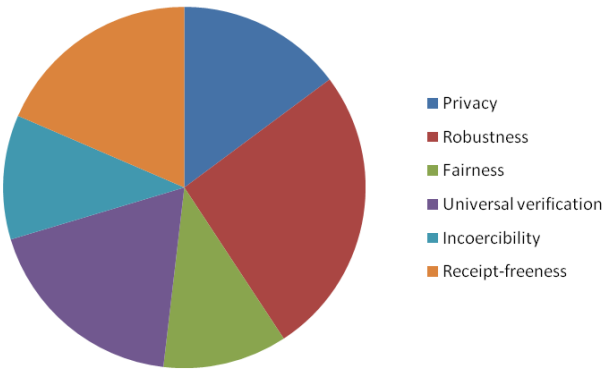

Figure: 2 Diagram1. Review on attack

X. CONCLUSIONS

As seen, Mobile voting has challenges less than E-voting. Because many of security requirements are not necessary for mobile and we can centralization on them.

Of course, it can enhance the participation of people in elections. Because of mobile access is more than computer and internet.

XI. REFERENCES

[1] H. Cilinton, "Remarks on Internet Freedom." U.S. Department of State. 21 Jan. 2010. Web. 15 Mar. 2011. http://www.state.gov/secretary/rm/2010/01/135519.htm.

[2] K. Weldemariam, R. A. Kemmerer, A. Villafiorita, "Formal Specification and Analysis of an e-Voting System", International Conference on Availability, Reliability and Security, 2010.

[3] http://www.electronic-vote.org/ (september 2011).

[4] http://seminarprojects.com/Thread-mobile-voting--15026#ixzz26KzPrdLT.

[5] B. Lee, C. Boyd, E. Dawson, Kwangjo Kim, Jeongmo Yang, and Seungjae Yoo. "Providing receiptfreeness in mixnet-based voting protocols". In Jong In Lim and Dong Hoon Lee, editors, ICISC, volume 2971 of Lecture Notes in Computer Science, pages 245–258. 2003.

[6] D. Chaum, Peter Y.A. Ryan, and Steve A. Schneider. "A practical, voter-verifiable election scheme". Volume 3679 of Lecture Notes in Computer Science, pages 118–139, 2005.

[7] F. Koenders, "Ad hoc voting", Master's thesis, Department of Mathematics and Computer Science, Eindhoven, 2009.

[8] L. Fouard, M. Duclos, and Pascal Lafourcade, "Survey on Electronic Voting Schemes", supported by the ANR project AVOTÉ, 2007.

[9] M. Ion, Ionuț Posea, " An Electronic Voting System Based On Blind Signature Protocol", CSMR, VOL. 1, NO. 1,2011.

[10] M. Wrighty, M. Adlery, B. N. Leviney, Clay Shields, "An Analysis of the Degradation of Anonymous Protocols", supported by grant DT-CX-K001 from the U.S. Department of Justice, O_ce of Justice Programs, 2000.

[11] M. Ohkubo, F. Miura, M. Abe, Atsushi Fujioka, and Tatsuaki Okamoto. "An improvement on a practical secret voting scheme". In Masahiro Mambo and Yuliang Zheng, editors, ISW, volume 1729 of Lecture Notes in Computer Science, pages 225–234, 1999.

[12] R.Jaye Chen, "Blind Signatures and Their ApplicationsI", CRYPTO, 2010.

[13] S. Weber. "A coercion-resistant cryptographic voting protocol - evaluation and prototype implementation". Master's thesis, Darmstadt University of Technology, 2006.

[14] K. Weldemariam, R. A. Kemmerer, A. Villafiorita, "Formal Specification and Analysis of a e-Voting System", International Conference on Availability, Reliability and Security, 2010.

[15] S. Poveniuc, "A Framework For Secure Mixnet-Base Electronic Voting", Phd thesise, Washington University, 2009.

[16] K. Sampigethaya, R. Poovendran, "A Survey on Mix etworks and Their Secure Applications", Proceedings of the IEEE | Vol. 94,No. 12, December 2006.

[17] David L. Chaum. "Untraceable electronic mail, return addresses, and digital pseudonyms". Commun. ACM, 24(2):84–90, 1981.