Journal of Computer and Communications, **2014, 2, 97-100**
Published Online January 2014 (http://www.scirp.org/journal/jcc)
http://dx.doi.org/10.4236/jcc.2014.22017

Development of a General-Purpose E-Voting Server

De Su, Yuichi Goto, Jingde Cheng

Department of Information and Computer Sciences, Saitama University, Saitama, Japan.
Email: sude@aise.ics.saitama-u.ac.jp; gotoh@aise.ics.saitama-u.ac.jp; cheng@aise.ics.saitama-u.ac.jp

Received November 2013

ABSTRACT

Voting is a general and indispensable method, and widely used to express a choice or preference, to elect a person, or to choose an opinion by ballot in education, enterprise, medicine, and government. Until now, various E-voting schemes are proposed in the world but they are different from each other. There is no system that can provide users with E-voting services anytime and anywhere such that one can use E-voting servers without even thinking about them. Therefore, an E-voting system for general-purpose is demanded. To support any kinds of vote, we divide voting system into components, and make different assembly of those components for different kinds of voting.

KEYWORDS

Component; E-Voting

1. Introduction

Vote is a general and indispensable method and widely used for a group to express a choice or preference, to elect a person, or to choose an opinion by ballot in education, enterprise, medicine, and government.

E-voting is an important application of cryptography in which a variety of cryptographic technologies as the theoretical basis, through the computer and the network to complete the entire election process [2].

Until now, various E-voting schemes are proposed in the word but they are different from each other. There is no system that can provide users with E-voting services anytime and anywhere such that one can use E-voting servers without even thinking about them [6].

On the other hand, an E-voting system for general-purpose can be developed; there are already many established electronic voting schemes. We just need to analyze existing electronic voting schemes, and divide voting system into components, and make different assembly of those components for different kinds of voting. After that we can say we implemented a general-purpose voting system.

The rest of this paper is organized as follows: Section 2 presents the requirement of electronic voting. Section 3 presents an architecture of a general-purpose E-voting server. Section 4 presents analyses of existing E-voting schemes. Some concluding remarks are given in Section 5.

2. The Basic Requirements of Electronic Voting

Generally speaking, a secure electronic voting scheme should satisfy the following seven requirements:

- Completeness that all legal votes should be the correct statistical.
- The legitimacy that a malicious voter cannot disrupt the elections.
- Confidentiality of the contents of that vote is confidential and cannot get the ballot papers by the voters of information.
- Cannot be repeated that any legal voter can only cast one vote.
- Has the legitimacy that only the right to vote polling personnel are eligible to vote.
- The fairness of that election results can not disclose the middle.
- Verifiable that voters can verify their votes are correctly included in the counting results.

3. The Architecture

To satisfy all the requirements, we indented to design and implement a general-purpose E-voting server as a persistent computing system [3] and a web application. A persistent computing system is a system that functions continuously anytime without stopping its reactions even when it needs to be maintained, upgraded, or reconfigured, or it is attacked. A web application is an informa-

tion system that can be used anywhere easily via the web, and can be used easily only a web browser.

Figure 1 shows the architecture of a general-purpose E-voting server. All components with measuring, recording, monitoring, controlling functions are connected by several Soft System Buses (SSB) [4] with data/instruction preserving functions. To easily maintain, upgrade, and reconfigure without stopping its services, the E-voting server has several same components and databases. In order to provide high security, we use three SSBs rather than only one SSB to connect components and databases.

In addition, the component can get data only from accessible databases. Therefore, the E-voting server can be maintained and reconfigured easily anytime and anywhere without stopping its services and the E-voting server can be implemented and managed in a style of information hiding/protection such that any developer/administrator cannot get unauthorized information [8].

The E-voting server consists of four groups of components, *i.e.*, central control components group, user interface group, database management group, and data processing group.

Central Control Components (CCCs) group includes a central measurer, a central recorder, a central monitor, and a central controller/scheduler. Central control components measure, record, monitor, and control other components.

User interface group consists of Web page Generator Components (WGCs) to generate web page data by interactions with this server's users. By the component, users can change messages from the E-voting server to languages they speak or desire.

Database management group consists of databases to store and manage data. These databases are: Vote databases (VOSs) to manage vote data, Answer Vote databases (AVSs) to manage answer vote data, Administrator databases (ADMs) to manage administrator data, Voter databases (VORs) to manage voter data, Verifier databases (VERs) to manage verifier data, Candidate databases (CANs) to manage candidate data.

Data processing group consists of Vote Management Components (VMCs) to deal with vote data, Verification Components (VCs) to verify the vote, Cryptography Management Components (CMCs) to encrypt vote data, Vote Open Components (VOCs) to deal with answer vote data, Account Management Components (AMCs) to deal with user account data.

The components are controlled by central control components. Central control components can make different assembly of those components for different kinds of voting. If some new kinds of voting are proposed in the world, we just need to add new components and make new assembly for new kind of voting.

4. Analysis of Existing E-voting Schemes

We had analyzed 10 voting schemes about internet voting. A distinction between voting system, there are four types below:

- Blind signature scheme.
- Mixnet scheme.
- Homomorphic encryption scheme.

4.1. Blind Signature Scheme

"Blind signature scheme", the voters will send their votes

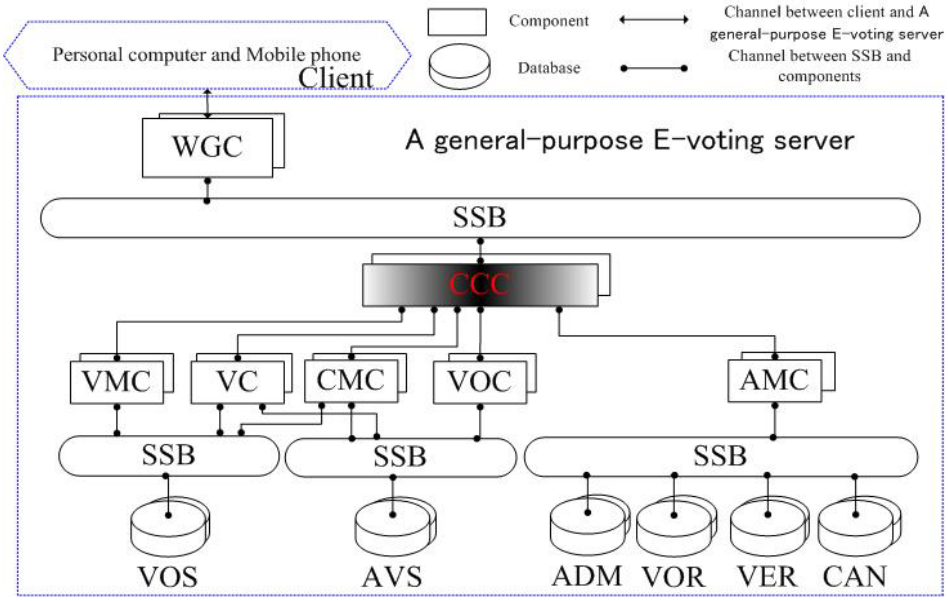

Figure 1. The architecture of a general-purpose E-voting server.

with the name of a trusted control center. Management Center will not look at the contents of the votes with the name, ownership may conduct a check of double voting, signing back with a ticket if they pass the Administration Center. Voters, the Center sent an anonymous aggregate vote signed center aggregation to aggregate and verify the signature [5].

To require anonymous communication channel, it cannot be used without the normal communication channels like the Internet. Configuration has the disadvantage of increasing the instrument [7].

Blind signature of anonymity because the electronic voting system constructed blind voters vote centre the identity of a blind signature is an important application. In 1992, Fujioka proposed a blind signature based voting program, which the algorithm is easy to implement, low network traffic, in the non-governmental sector has been widely used. However, this solution in terms of safety there are some shortcomings:

1) The lack of voter control. In this way, a malicious voter may send a large number of anonymous votes, the electoral process interference and damage.

2) Fails to effectively prevent the issuer's fraud. Since the legitimacy of the voting phase of the signature entirely by the issuer to verify, so people can forge a valid visa votes if voters abstained, so he can be someone else's vote.

3) No effective supervision of tellers, tellers failed to prevent the intermediate results of the vote disclosure, thus affecting the elections.

Currently, many papers and programs on the electronic voting program Fujioka has been improved, but the safety and efficiency to varying degrees, still there are some problems. This departure from the practicality and safety, the use of blind signatures, put forward an electronic election scheme, which can effectively address the issue.

Models of blind signature scheme have the following five:

Sensus scheme.
EVS scheme.
SEAS scheme.
DynaVote scheme.
Receipt-free scheme.

The above model using the blind signature scheme can effectively protect the privacy of voters.

4.2. Mixnet Scheme

I will not be able to vote by correspondence with the content and the close vote in the first ciphertext by making a mixnet that guarantees the anonymity of the vote.

This method, however, to increase the accuracy to prevent unauthorized centers, it is necessary to increase the number of centers and to increase the number of system components, to achieve fairness and tallied after the deadline for voting, aggregate you must have a problem on the ballot may essentials.

Mixnet system model has the following three:

Clarke Tax scheme
Voter-Resolved scheme.
Model Mixnet-based scheme.

4.3. Homomorphic Encryption Scheme

Voters sent to administrators and the public key to encrypt the contents of the votes. Administrator to aggregate the votes without looking at the contents of the table, send their votes to the ballot and then aggregated. The ballot will be announced at a private key to decrypt the votes. But look what's on ballot for each vote. The anonymity of the vote is guaranteed.

It puts only 1 or 0 in this method the contents of the table is a small range of applications.

Homomorphic encryption scheme model has the following two:

Re-encryption scheme
Secret-ballot scheme

4.4. A Case Study of DynaVote

We make a case study to illustrate the feasibility of our server. We choose DynaVote [9] as a target, because this scheme is often discussed in the world. We make a table to proof our components can achieve this scheme. How our components can achieve DynaVote shows in **Table 1**.

DynaVote has the following actors: Voter, Ballot Generator, Key Generator, Counter, and PVID Authority.

5. Concluding Remarks

An E-voting system for general-purpose can be developed.

Table 1. Components in dynaVote.

Process	Component	DynaVote
Prepare Stage	AMC	Voter registration
	AMC	Voter applies PVID authority to obtain a PVID-list by using his real registration identity.
	VMC	Voter obtain a secret key
Voting Stage	VMC	In voting stage voter obtains a dynamic ballot and casts his candidate selection with the PVID.
	VC	Verifier verifies that the PVID belongs to a registered voter who has not yet voted. If the ballot is valid, the verifier signs the ballot and returns it to the voter.
	VMC	The voter then sends the signed ballot to the counter
Opening Stage	VOC	The counter checks the signature on the ballot, The counter then add the ballot to the tally.

There are already many established electronic voting schemes. We just need to analyze existing electronic voting schemes, and divide voting system into components, and make different assembly of those components for different kinds of voting. In this paper, we have presented a requirement analysis and architecture for a general-purpose E-voting server.

Now we are developing a general-purpose E-voting server based on ENQUETE-BAISE [1].

In this paper we only analyze some common voting schemes, but we have not analyzed special voting schemes. So in the future we will also analyze other special voting schemes and add them into ENQUETE-BAISE

REFERENCES

[1] Advanced Information Systems Engineering Laboratory, Department of Information and Computer Sciences, Saitama University, "ENQUETE-BAISE," Saitama, Japan, 2003-2013 http://www.aise.ics.saitama-u.ac.jp/enquete/index.html.

[2] J. Cheng, Y. Goto, M Koide, K. Nagahama, M. Someya, Y. Utsumi, and A. Shioneiri, "ENQUETE-BAISE: A General-Purpose e-Questionnaire Server for Ubiquitous Questionnaire," *Proceedings of* 2*nd IEEE Asia-Pacific Services Computing Conference*, December 2007, IEEE Computer Society Press, Tsukuba, pp. 187-194. http://dx.doi.org/10.1109/APSCC.2007.73

[3] J. Cheng, "Persistent Computing Systems as Continuously Available, Reliable, and Secure Systems," *Proceedings of* 1*st International Conference on Availability, Reliability and Security*, April 2006, IEEE Computer Society, Vienna, pp. 631-638. http://dx.doi.org/10.1109/ARES.2006.91

[4] J. Cheng, "Persistent Computing Systems Based on Soft System Buses as an Infrastructure of Ubiquitous Computing and Intelligence," *Journal of Ubiquitous Computing and Intelligence*, Vol. 1, No. 1, 2007, pp. 35-41. http://dx.doi.org/10.1166/juci.2007.004

[5] F Baiardi, "SEAS, a Secure e-Voting Protocol: Design and Implementation," *Computers &. Security*, Vol. 24, No. 8, 2005, pp. 642-652.

[6] Y. Goto and J. Cheng, "Information Assurance, Privacy, and Security in Ubiquitous Questionnaire," *Proceedings of* 4*th International Conference on Frontier of Computer Science and Technology* (FCST'09), December 2009, IEEE Computer Society Press, Shanghai, pp. 619-624.

[7] L. F. Cranor, "Sensus: A Security-Conscious Electronic Polling System for the Internet," *Proceedings of the Thirtieth Hawaii International Conference on System Sciences*, Vol. 3, 1997, pp. 561-570. http://dx.doi.org/10.1109/HICSS.1997.661700

[8] M. R. Selim, Y. Goto and J. Cheng, "Ensuring Reliability and Availability of Soft System Bus," *Proceedings of* 2*nd IEEE International Conference on Secure System Integration and Reliability Improvement* (*SSIRI*'08), July 2008, The IEEE Reliability Society and The IEEE Systems, Man, and Cybernetics Society, Yokohama, pp. 52-59.

[9] O Cetinkaya, "A Practical Verifiable e-Voting Protocol for Large Scale Elections over a Network," *The Second International Conference on Availability, Reliability and Security* (*ARSE*), April 2007, Vienna, pp. 432-442. http://dx.doi.org/10.1109/ARES.2007.15