ISSN 0002-306X. Proc. of the RA NAS and NPUA Ser. of tech. sc. 2021. V. LXXIV, N1

UDC 004.8

COMPUTER SCIENCE AND INFORMATICS

S.V. BABAYAN

AN ELECTRONIC VOTING SYSTEM WITH DISTRIBUTED RESPONSIBILITY

Electronic voting (e-voting) helps to increase citizen involvement, reduce the costs of running election processes and improve the accuracy of the results. This paper provides a mechanism to build an electronic voting system based on open-source software technologies. The system uses private/public key cryptography and distributes authorities between independent servers. The system can be easily configured depending on the elections for which it will be used.

Keywords: e-voting, distributed responsibilities, multi-tiered web-based application, open-source software.

Introduction. Electronic voting systems are crucial for democratic organizations and represent a new technology that allows electors to cast their ballots in elections using computerized systems. There are different types of voting machines and systems such as punched cards, optical scan systems, Direct-Recording Electronic Voting machines, and Internet voting system [1].

Electronic voting gives an opportunity to solve some of the old electoral problems, but it also causes new problems. A large range of advantages is provided by electronic voting systems, such as accuracy in the voting process, speed of implementation, accessibility for disabled voters, and lack of complexity. However, despite these benefits, electronic voting systems have a range of security drawbacks and can lead to electoral fraud. As a result, e-voting usually creates more opposition and criticism and is more contentious than any other information technology (IT) election application.

In order to make the voting process equal and clear, the goal of electronic voting is transparency and consistency in recording the votes of voters. The main purpose of using electronic voting systems is the possibility of providing the following operational features:

1. *User participation.* By allowing them to vote everywhere the e-Voting system increases the level of user involvement.

2. *Security.* By this, it is meant the overlap of security layers that are applied when talking about a secure election to ensure that the votes counted are in line with the will of the voters and that they have been provided by the voters permitted to participate in elections. In addition to the logical and physical protection layers,

mechanisms are developed in electronic voting processes to ensure the participation of only users approved by an official document, so that all security assurances are given that equate the electronic voting process with the classical electoral process.

3. *Accessibility*. Internet voting offers a secure and private platform that enables all users to participate on equal terms. Increased accessibility for residents overseas and people with travel problems or mobility impairments. This also has a beneficial effect on the final turnout and therefore on the validity of the elections.

4. *Auditability*. End to end, the entire voting process is verifiable. The system's architecture helps managers to guarantee users that their votes are correctly accounted for in compliance with their decision to vote.

5. *Efficiency*. For example, the decrease in organizational and execution costs significantly enhances the efficacy of election management compared to traditional paper voting.

6. *Accuracy*. Electronic voting avoids errors in the manual count, which leads to reliable and quick results being published.

Some governments have already put in place e-Voting systems and are using them for parliamentary elections. Estonia, for example, successfully uses e-Voting for all its elections for years. Other projects encountered, but they all had major security issues and were often cancelled. The fact that the Estonian e-voting system is still in use does not mean that this system is secure.

There are a few implementations of e-voting systems [2, 3]. Such electoral systems promise and deliver several advantages despite some difficulties in solving problems and risks [4] in relation to these operating properties of authentication, democracy, confidentiality, lack of coercion, precision, reliability, verification, linkability and neutrality.

1. *Authentication*: Only registered users on a closed election can vote. The finalized list of voters has to be drawn up before the start of the election process.

2. *Democracy*: Every vote is counted only once at the elections. The rules should be clear for all voters.

3. *Confidentiality*: The vote will not be linked to the voter. Confidentiality is a very important right that the voter must have in order to ensure his or her self security.

4. *Lack of coercion*: Voting cannot be traded for any reason. The vote cannot be verified by the elector or others after it has been cast and the choice has been made.

5. *Precision*: All valid votes are correctly counted in the final tally. A valid vote may not be removed from the final count.

6. *Reliability*: All incorrect, false or other invalid votes are excluded from the final tally. It is not possible to include a non-valid vote in the final tally.

7. *Verification*: Any voter can verify that his or her vote is counted and that the counting has been carried out correctly. Voters can verify that their votes have been correctly taken into account.

8. *Linkability*: Two ballots from the same voter shall be connected, but not to the voter.

9. *Neutrality*: The election process must be fair both to the voters and candidates. While voting is still going on, the results should remain secret.

Design principles of the e-voting system. Since democracy depends very much on citizen participation, the majority of the citizens involved in the process of electing members of their governing bodies is important in our modern system of representative democracy. Consequently, the system of support that facilitates the voting process must be guided by these design principles:

- Usability
- Reliability
- Fairness
- Manageability

Certainly, these four design principles must include the operating properties listed above.

The voting process flow. The simple flow chart scheme is presented in Fig. 1. The 3 major voting processes are designed to ensure the operational and administrative independence of each other. Administrative responsibilities will be assigned to three non-collaborative teams. These administrators will not share information about organizational secrets and data.

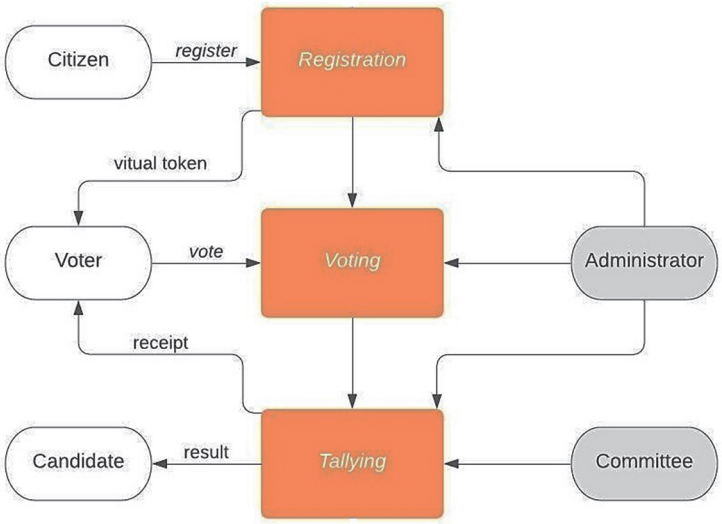

Fig. 1. Voting process flow

System infrastructure. The system is divided into three servers, which perform different functions at different stages of the election. Servers communicate with each other using JSON-RPC (Fig. 2). Each server has at least two identical copies, so if any of the servers fail, no data will be lost and one of the copies will replace the main server. The databases also have at least two replicas.

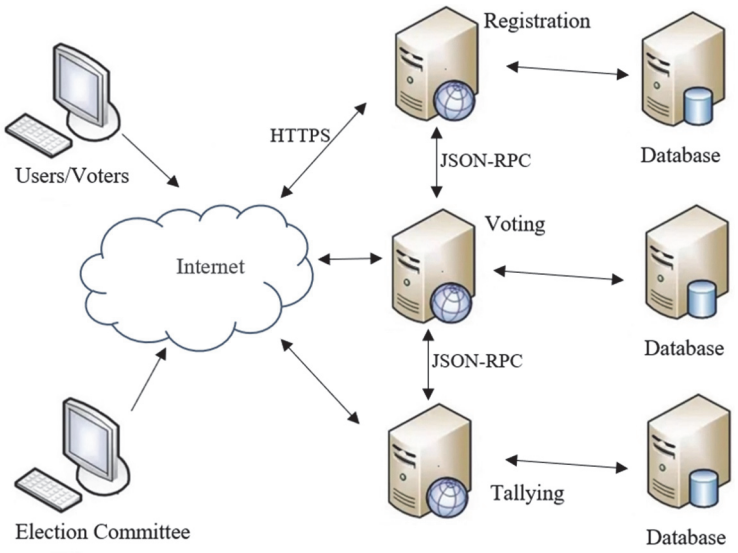

Fig. 2. The system infrastructure

The software used for the e-voting system. The system is built based on design principles and using open-source software. The front end is developed using Angular. Angular is an application design framework and development platform for creating efficient and sophisticated single-page apps [5]. To set up a connection a server and the browsers of users, Apache Web server [6] is used. Server-side code is written in Python [7]: an interpreted, object-oriented, high-level programming language. PostgreSQL [8] is used as a database.

The system uses two common cryptography algorithms, private/public key (RSA) [9], [10] and hash functions [11]. Hash functions return the fixed-size value for an input, which is called their hash value or hash.

Encryption and decryption keys are different in RSA. The encryption key is public, the decryption key is private. Anyone can encrypt messages using the public key, but they can only be decoded by someone who knows the private key:

$$cipher = rsa\_encrypt(message,\ k_{public}),$$

$$decrypted = rsa\_decrypt(cipher,\ k_{private}).$$

The election process. Elections are held according to the voters' list. The voters' list is saved in all three servers. To be able to vote, users need to be in the list of voters and be registered in the registration server (**R**). Users authenticate by their *userId* and *password*. After they successfully authenticate for election, they get a unique number (*voterId*) which is in the voters' list. Voting server (**V**) generates voting token (*tokenId*) for any user with valid *voterId*. The voting token must be authenticated with a *PIN*. The **V** saves the hash of the *PIN*.

The voter gets an empty ballot from the **V** using his *tokenId* and *PIN*. After voting, the **V** encrypts the ballot using the public key of the tallying server (**T**) and sends the encrypted ballot to the **T**. The **T** provides the voter with a receipt after validating voter's ballot.

When voting ends, the **R** and **V** servers turn off. The **T** opens the voters' list and reads each *voterId* and the related ballot. Tallying follows the rules and requirements set out by organizers and finally decides the winners of the elections.

It is necessary to keep the backups of databases after elections. Backups must be deleted sometime after the elections according to the regulations.

Conclusion. The represented system is effective and appropriate for electronic voting. It uses common, secure cryptographic algorithms to achieve privacy and anonymity by distributing trust. Security is modelled on servers and communication between servers only.

The main issues with electronic voting systems are data protection and the difficulty of preventing data loss due to electronic malfunction or denial of service attacks. The distributed design of this system solves the problems mentioned above.

REFERENCES

1. **Adeel M.J.** Electronic Voting System Security// SSRN Electronic Journal.- 2014.
2. i-Voting — e-Estonia. https://e-estonia.com/solutions/e-governance/i-voting/, 2021 (last accessed)
3. BigPulse Online Voting. https://www.bigpulsevoting.com/product/, 2021 (last accessed
4. Security Considerations in e-Cognocracy/ **J.M. Moreno-Jiménez**, **J.J. Piles**, **J. Ruiz**, **J.L. Salazar**, **A. Turón** // Springer-Verlag.- Berlin, Heidelberg, 2006.- P. 735-744.
5. Angular. https://angular.io/, 2021 (last accessed)
6. Apache, The Apache Software Foundation, HTTP server. http://www.apache.org/, 2021 (last accessed)
7. Python Programming Language. http://www.python.org/, 2021 (last accessed)
8. PostgreSQL, The world's most advanced open source relational database. http://www.postgresql.org/, 2021 (last accessed)
9. **Rivest R.**, **Shamir A.** & **Adleman L.** A Method for Obtaining Digital Signatures and Public-Key Cryptosystems// Communications of the ACM.- 1978.- P. 120-126.

10. **Jonsson J.**, **Kaliski B.** Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1.- RSA Laboratories.- 2003.
11. FIB PUB 180-3, SECURE HASH STANDARD (SHS)// Federal Information Processing Standards Publication.- 2008.

National Polytechnic University of Armenia. The material is received on 03.02.2021.

Ս.Վ. ԲԱԲԱՅԱՆ

ԲԱՇԽՎԱԾ ՊԱՏԱՍԽԱՆԱՏՎՈՒԹՅԱՄԲ ԷԼԵԿՏՐՈՆԱՅԻՆ ԸՆՏՐԱԿԱՆ ՀԱՄԱԿԱՐԳ

Էլեկտրոնային քվեարկությունն օգնում է՝ մեծացնելու ընտրական գործընթացներում քաղաքացիների ներգրավվածությունը, նվազեցնելու դրանց վարման ծախսերը և բարելավելու արդյունքների ճշգրտությունը: Դիտարկվում է բաց կոդով ծրագրային ապահովման տեխնոլոգիաների վրա հիմնված քվեարկության էլեկտրոնային համակարգ կառուցելու մեխանիզմ: Նկարագրված համակարգն օգտագործում է բացահայտ բանալիների գաղտնագրում և բաշխում է պարտականությունները մի քանի անկախ սերվերների միջև: Համակարգը կարող է հեշտությամբ կազմաձևվել՝ կախված այն ընտրություններից, որոնց դեպքում կօգտագործվի:

Առանցքային բառեր. էլեկտրոնային քվեարկություն, բաշխված պարտականություններ, բազմամակարդակ վեբ ծրագիր, բաց կոդով ծրագրային ապահովում:

С.В. БАБАЯН

ЭЛЕКТРОННАЯ СИСТЕМА ГОЛОСОВАНИЯ С РАСПРЕДЕЛЕННОЙ ОТВЕТСТВЕННОСТЬЮ

Электронное голосование помогает повысить вовлеченность граждан, снизить затраты на проведение избирательных процессов и поднять точность результатов. В этом документе представлен механизм построения системы электронного голосования на основе программных технологий с открытым исходным кодом. Описанная система использует криптографию с открытым ключом и распределяет обязанности между несколькими независимыми серверами. Систему легко настроить в зависимости от того, на каких выборах она будет использоваться.

Ключевые слова: электронное голосование, распределенная ответственность, многоуровневое веб-приложение, программное обеспечение с открытым исходным кодом.