Secure Online Voting Scheme Using Steganography

Mariam Haroutunian
Institute for Informatics and Automation
Problems of NAS RA
Yerevan, Armenia
e-mail: armar@sci.am

Arsen Margaryan
MoodMap AI
Yerevan, Armenia
e-mail: margaryanarsen83@gmail.com

Karen Mastoyan
Institute for Informatics and
Automation
Problems of NAS RA
Yerevan, Armenia
e-mail: kmastoyan@yandex.com

https://doi.org/10.62343/csit.2024.12

***Abstract* — Distrust in voting is not a rare phenomenon even in developed countries. Electronic voting, however, appeared as an alternative, but is still not practiced on a large scale. This is due to the fact that despite the huge number of articles it is not yet possible to completely ensure security, verifiability and anonymity. It is hard to create a system or a protocol fulfilling all requirements, especially unconditionally. Designing effective voting systems is challenging because these aspects often conflict with each other. There are issues that need to be resolved. Our aim is to develop a secure online voting system in Armenia suitable for a variety of choices and easily adaptable to different cases. In this paper we suggest to use steganography to create an e-voting model with added security. This research proposes a novel architecture for an internet voting system that incorporates steganography techniques to enhance the security of the system. In the proposed architecture steganography is used to hide the voter's identity and voting preferences within the data packets transmitted between the storage, that keeps all the votes, and the counting server. The use of statistical steganography ensures that the encrypted vote is undetectable, while hypothesis testing ensures the integrity of the voting process.**

***Keywords* — e-voting, security, privacy, trust, steganography**

I. INTRODUCTION

In recent years, online voting has been offered as an alternative means of conducting elections. Today there are many e-voting schemes and systems, which allows their use in many areas of public administration. Internet voting offers many advantages compared to traditional types of voting. The main benefit is to ensure better accessibility and convenience of voting (including for people with disabilities, during pandemic or citizens abroad), which can lead to higher participation in elections. Another advantage of online voting is higher speed and accuracy of results data processing. Very positive are lower voting costs for both voters and organizers.

Internet voting systems have gained popularity and have been used for government elections, referendums, municipal elections in such countries as Estonia, Switzerland, Canada, the USA, France and others. Our aim is to develop a secure online voting system in Armenia, since the electronic voting can improve the country's image.

Because of its fundamental importance for democratic societies, Internet voting is subject to high legal standards, in particular security requirements for the voting method. However, these legal standards and resulting safety requirements partially contradict each other. As a result, many challenges arise to address mandatory security requirements.

A huge number of publications are devoted to the problems related to e-voting systems. Here we referee to the most recent surveys which in turn referee to a wide range of literature. Several remote e-voting solutions based on blockchain technology have been proposed. The survey [1] provides a comprehensive overview of the blockchain - based e-voting systems currently being implemented by various countries and companies and proposed for academic research. At the same time the challenges faced by blockchain e-voting systems are analysed here. [2] claims to apprehend the security and data management challenges in blockchain and provides an improved manifestation of the electronic voting process. In [3] the most revealing e-voting solutions based on blockchain technology are reviewed.

Indeed, in the scientifc literature, more and more research works propose e-voting applications based on blockchain. Nevertheless, only some of the proposed solutions have been implemented in real life and none of them have been tested on a large scale. Therefore, it is very difficult to conclude that blockchain is a completely secure alternative for national election at present. Although the principles on which blockchain is based are secure, e-voting applications are still vulnerable to several attacks. This makes it very challenging to guarantee the integrity of an election, which is problematic given the stakes of such an application. The National Academies of Sciences report [4] states that "blockchain technology does little to solve the fundamental security issues of elections, and indeed, blockchains introduce additional security vulnerabilities". Blockchain technology is designed to keep information secure once it is received. It cannot defend against the multitude of threats to that information before it is entered in the blockchain, and voters cannot verify their votes are entered into the blockchain correctly without compromising ballot secrecy. Recording ballots on a blockchain also risks ballot secrecy if encryption keys are not properly protected or software errors allow decryption of individual ballots.

State-of-the-art research includes, in particular [5], where a blockchain-based voting mechanism is presented underlying 5G Network, [6] that initiated the concept of E-voting attacks in the IoT-oriented smart cities, [7] where Re-Encryption Mix-Net is suggested to provide an efficient cryptographic anonymous channel for useful applications such as e-voting and web browsing.

Information theoretic notions and tools are also considered in various problems of e-voting. In particular, for information theoretic study we referee to [8]. In [9] an information-theoretic model of a vote counting system with well-defined criteria for evaluating such a system with respect to integrity, privacy and verifiability is presented. The information-theoretic approach proved the impossibility of achieving perfect integrity, perfect verifiability and perfect privacy and the existence of the tradeoffs among these criteria.

In this paper we suggest to use steganography to create an e-voting model with added security. Steganography is the science of hiding information within other information. It is a technique that has been used for centuries to convey secret

messages, and in recent years, it has found many applications in the field of computer security. In the proposed architecture, steganography is used to hide the voter's identity and voting preferences within the data packets transmitted between the storage, that keeps all the votes, and the counting server.

The previous information-theoretic research on the model of stegosystem with active adversary [10], where two-stage statistical hypothesis testing approach was studied, motivated to apply it in e-voting systems.

Our goal is to create a system that is suitable for a variety of choices and easily adaptable to different cases.

II. REQUIREMENTS

The online voting process consists of several stages. All these stages are present in traditional elections and must be carried out in exactly the same order. Online voting should allow voters to *securely* and *secretly* record their votes. Also the connection between the voter's computer and the election server must be secure, since the third party may try to change the votes while they are being transmitted to the server. Therefore, it is necessary to use *secure communication* over the Internet. It is also necessary to use different cryptographic methods, but at the same time the solution must be *user-friendly* to ensure maximum efficiency. There are quite a few cryptographic schemes which fulfill wide requirements for electronic elections. Their only disadvantage is inconvenience: they use sophisticated cryptographic tools that make them hard to implement and require expertise in various fields.

The e-voting system must be *reliable* to prevent election fraud (insider attacks) or attacks on the system from outside. When implementing a technical solution, it is necessary to take into account all types of attacks. *Interoperability* of all technical components and services used must be ensured, compatibility and correct functionality of the system must be assured, therefore suitable open electronic data interchange standards should be used.

The system must be operational under any circumstances, even if some problems arise (for example, with the network), equipment failures, hacker attacks, etc.). The reliability of the system must be tested, evaluated and improved constantly. The Internet voting system must be *uninterruptedly accessible* to voters. Its interface should be easy to use and all voters should be able to access it equally, regardless of age, education or physical condition. Ballots should be written as clearly as possible so that voters can minimize the possibility of votes being miscounted due to any misleading aspect of the ballot design.

The main security characteristics of e-voting system can be formulated in the following list:

- *Authenticity:* only eligible voters can participate in the election;
- *Eligibility*: all ballots that are to be counted are sent by eligible voters,
- *Completeness*: all ballots are counted, no ballot is ignored or erased;
- *Stability*: no ballot is subject to change after being sent to ballot storage;
- *Anonymity*: make ballots indistinguishable from one another, not to find who is the voter;
- *Privacy*: ensures that there is no link between a voter and his vote, in other words, protects any information about the voter;
- *Unreusability or uniqeness*: voter can vote only once, does not permit any voter to cast more than once;
- *Verifiability*: voter can check if his vote was counted correctly and was not changed;
- *Confidentiality or non-coercibility*: a voter should not have a record of voting choice, not to be able to prove how he has voted;
- *Accuracy*: ensure that the declared results correspond precisely to the election results, that votes are recorded correctly;
- *Integrity*: Votes cannot be altered or deleted, all valid votes encountered in the ballot box, and only those, will be included in the count;
- *Accountability*: The system has the ability to verify that votes are correctly counted.

It is hard to create a system or a protocol fulfilling all requirements, especially unconditionally. Designing effective voting systems is challenging because these aspects often conflict with each other. For example, one of such challenges is trying to keep votes anonymous while still being able to verify them. Another challenge is to ensure identification and maintain voter privacy. Hence, constant investigations and improvements are needed.

III. THE STRUCTURE OF ELECTION PROCESS

The online election process (Fig. 1) starts with so called *setting phase*, where the staff creates ballot, election parameters are formed and published. These parameters include encryption keys, the number of candidates, list of voters, etc. The election is announced with sending login credentials to users.

The next is the *ballot filling phase,* during which the voter login to user interface and prepare his/her vote. The result should be an e-ballot with voter's personal info embedded in it.

In the *ballot registration phase* the ballot with embedded info and voter's personal number are sent to public ballot storage.

The voter's info must be removed from the ballot and as a result a ballot without voter info is collected, this is called *ballot anonymity phase*. The authenticity of the ballot can be checked via private keys that are only given to election committee.

At last in the *counting phase* the committee uses a personal key to decode all the ballots and count the voices.

Designing an electronic voting system involves several key components to ensure the main security characteristics. Let us discuss the correspondence of each step of e-voting to the main security requirements. Process 1 on the Fig. 1 are the *Login* steps of the staff and voters. The secure management access must solve the *authenticity challenge*. Authentication methods may include biometric verification (e.g., fingerprint

or facial recognition), government-issued ID verification, or unique login credentials.

Process 2 is the *creation of the Ballot.* The system should provide a mechanism for creating and managing electronic ballots. Ballots may contain candidates' names, party affiliations, and other relevant information. Ballot creation should be customizable to accommodate various election

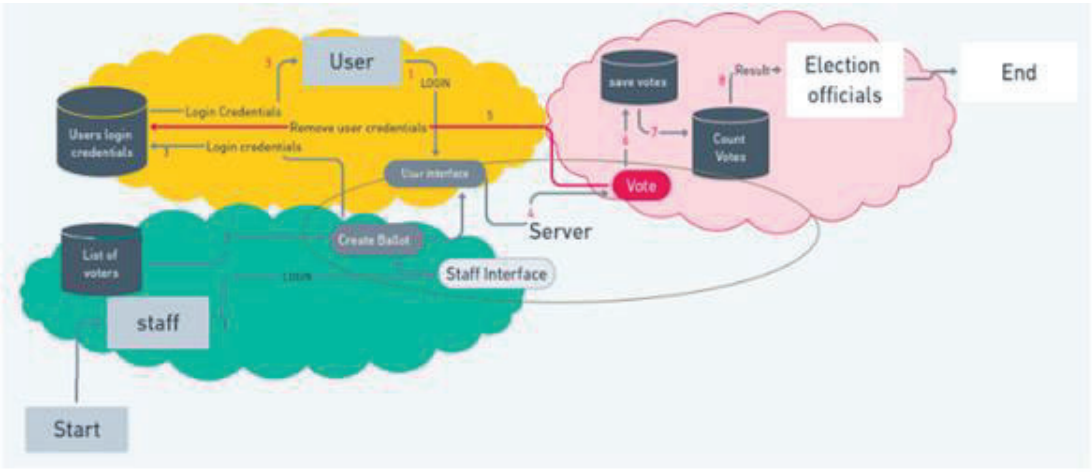

Figure 1. The structure of online election process.

types (e.g., local, national, or organizational elections). At this stage the *security* of information must be ensured.

Process 3 implements the *transmission of Login credentials* to voters. The challenge here is that e-voting systems must enhance the *security* of transmitting login credentials and mitigate the risks associated with unauthorized access and tampering.

Once authenticated, voters can cast their votes electronically (Fig. 1, step 4). The system should check the *eligibility* of the voter. After that the credentials must be removed from the ballot (step 5) ensuring the *unreusability* and voter *anonymity.*

In the process 6 the system records each vote maintaining *stability* and *privacy*. After the voting period ends, the system should tabulate the votes and generate results guaranteeing *completeness* and *integrity* (step 7). This process may involve aggregating individual votes, detecting any anomalies or discrepancies, and resolving any issues encountered during tabulation. The final stage 8 must record results *accurately.*

At last, to enhance trust in the e-voting system, *accountability* or independent verification mechanisms should be in place. This may involve allowing third-party organizations or experts to audit the system for vulnerabilities and verify the integrity of the voting process.

IV. OUR CONTRIBUTION

Our approach is that the use of various steganographic models can help to reduce the risks of data corruption and tampering. More specifically, the steganography models with active adversary [10] are very close to imitating attacks that can happen during elections.

Steganography, the technique of hiding secret information within non-secret information, has potential applications in e-voting systems, although its usage comes with significant considerations and challenges.

Ballot Concealment: Steganography can be used to embed encrypted ballot data within seemingly innocuous digital files, such as images or audio recordings. This could help protect the privacy of voters by concealing their choices within the noise of other data.

Steganography could be employed to embed audit trail information within e-voting records. This would enable the verification of the integrity and authenticity of the voting process without compromising voter anonymity.

Steganographic techniques could be used to embed digital signatures or cryptographic hashes within voting records. This would allow election officials and voters to verify the authenticity and integrity of the recorded votes.

Despite these potential applications, there are several challenges and considerations to using steganography in e-voting systems:

- Ensuring the security and integrity of steganographic techniques is challenging. Any vulnerabilities in the steganographic algorithms or implementation could be exploited by adversaries to manipulate or compromise the voting process.
- Detecting the presence of steganographically hidden information is difficult without access to the appropriate decoding keys or algorithms. This could hinder efforts to audit and verify the integrity of e-voting systems.
- Implementing steganography in e-voting systems without compromising usability is a significant challenge. The process of embedding and extracting hidden information must be seamless and intuitive for both election officials and voters.

Nowadays ensuring the accuracy of step 8, one of the most important issues, still remains unsolved. Secure data transfer from the storage, that keeps all the votes, to the counting server in modern systems rely on physical copies of data and are

transferred manually, which is a major security issue. Thus, the usage of steganography methods is explored for that step. The main concern is that the channel between servers may be vulnerable to attacks and if an adversary can send unreliable data to the counting server, the entire electoral process will be in doubt.

In [11] most popular steganography methods were studied in terms of their viability when used for a secure electronic voting model. The statistical method was found to be most useful and practical. Unlike traditional steganography methods that rely on imperceptible changes in the cover data (like slight alterations in pixel values in images or LSB manipulation), statistical steganography operates by subtly modifying statistical properties of the cover data to embed the secret information. The goal of statistical steganography is to ensure that the statistical properties of the cover data remain similar to the original while embedding the secret message in a way that's difficult to detect statistically. This can involve techniques such as modifying the frequency distributions, correlations, or other statistical characteristics of the cover data to embed the secret message. Overall, statistical steganography aims to maintain the cover data's statistical fidelity while embedding secret information, making it a challenging task to detect without knowledge of the embedding process or access to the original, unaltered cover data.

By applying statistical steganography to the encryption of votes, the system ensures that the encrypted votes remain hidden within the data, making them undetectable to potential attackers. This helps in maintaining the confidentiality of the voting process. The verifier uses hypothesis testing to ensure the integrity of the voting process. It checks whether the votes are distributed randomly and not manipulated without using the extraction algorithm.

In [10] two-stage statistical hypothesis testing approach from the receivers point of view for the information-theoretic model of stegosystem with an active adversary is suggested. The functional dependence of reliabilities of the first and second kind of errors in both stages is constructed. The advantages of the two-stage approach are discussed.

We suggest to apply this research to the system of e-voting at the process 8. As a result of two-stage hypothesis testing the verifier will gain in time without loss in error probability. Moreover, using the functional dependence of reliabilities of the first and second kind of errors, the election officials can fix the level of important parameter and find the best possible values for others.

V. CONCLUSION

The proposed internet voting system architecture using statistical steganography and hypothesis testing provides a secure and private electronic voting system. The use of statistical steganography ensures that the encrypted vote is undetectable, while hypothesis testing ensures the integrity of the voting process. The system also ensures the privacy of the voters by using statistical steganography to encrypt and decrypt the votes. This system can be used for various types of elections, from small-scale local elections to national elections.

Future work: One of the challenges is to ensure biometric identification and maintain voter privacy. The next step of our research is implementation of privacy preserving face recognition to this system.

ACKNOWLEDGMENT

The work was supported by the Science Committee of RA, in the frames of the research 21T-1B151

REFERENCES

1. M. V. Vladucu, Z. Dong, J. Medina and R. Rojas-Cessa, "E-voting meets blockchain: A survey," in *IEEE Access*, vol. 11, pp. 23293-23308, 2023. doi: 10.1109/ACCESS.2023.3253682
2. B. Shahzad and J. Crowcroft, "Trustworthy electronic voting using adjusted blockchain technology," in *IEEE Access*, vol. 7, pp. 24477-24488, 2019. doi: 10.1109/ACCESS.2019.2895670
3. A. Benabdallah, A. Audras, L. Coudert, N. El Madhoun and M. Badra, "Analysis of blockchain solutions for E-voting: A systematic literature review," in *IEEE Access*, vol. 10, pp. 70746-70759, 2022. doi: 10.1109/ACCESS.2022.3187688
4. A Consensus Study Report of National Academies of Sciences, Engineering, and Medicine, "Securing the vote: protecting American democracy", Washington, DC: The National Academies Press, 2018. https://doi.org/10.17226/25120
5. S. Chaudhary *et al*., "Blockchain-based secure voting mechanism underlying 5G network: A smart contract approach," in *IEEE Access*, vol. 11, pp. 76537-76550, 2023. doi: 10.1109/ACCESS.2023.3297492
6. G. Rathee, R. Iqbal, O. Waqar and A. K. Bashir, "On the design and implementation of a blockchain enabled E-voting application within IoT-oriented smart cities," in *IEEE Access*, vol. 9, pp. 34165-34176, 2021. doi: 10.1109/ACCESS.2021.3061411
7. M. Kim, "Toward round-efficient verifiable re-encryption Mix-Net," in *IEEE Access*, vol. 10, pp. 91397-91413, 2022. doi: 10.1109/ACCESS.2022.3202966
8. E. Yaakobi, M. Langberg and J. Bruck, "Information-theoretic study of voting systems," *2013 IEEE International Symposium on Information Theory*, Istanbul, Turkey, pp. 1087-1091, 2013. doi: 10.1109/ISIT.2013.6620394
9. B. Hosp and P. L. Vora, "An information-theoretic model of voting systems", Mathematical and Computer Modelling, vol. 48, pp. 1628–1645, 2008. https://doi.org/10.1016/j.mcm.2008.05.040
10. M. Haroutunian, P. Hakobyan and A. Avetisyan, "Two-stage optimal hypotheses testing for a model of stegosystem with an active adversary", JUCS - Journal of Universal Computer Science, vol. 29, no. 11, pp. 1254-1273, 2023. https://doi.org/10.3897/jucs.112913
11. A. Avetisyan, M. Haroutunian and P. Hakobyan, "Discussion on steganographic methods from the perspective of E-voting implementation", Proceedings of **14th** International Conference Computer science and information technologies CSIT 23, pp. 214-217, 2023. https://doi.org/10.51408/csit2023_51