A Double-Registration Based Algorithm for Secure Elections

Yaser M. Asem
Department of education technology, Faculty of Specific Education, South Valley University, Egypt

Abstract

Fair and democratic elections can change our life to the better. However, paper based elections suffer from many security breaches and need to be fixed. This paper proposes a secure electronic voting scheme that uses biometric measures for voters' authentications. In the proposed scheme, voters have to register twice for voters' anonymity and in order to prevent ballot box stuffing by the voters' authenticator. The proposed method uses three voting entities in each stage for registration, authentication, and vote tallying. The security analysis for the proposed electronic voting method shows that the characteristics of the ideal e-voting scheme are satisfied in the proposed method except for verifiability.

Keywords - *e-voting, electronic elections, privacy, secure elections, democracy.*

I. INTRODUCTION

All nations eager to freedom and liberty. To achieve these two needs, people need to select who govern them and who represent them in a freeway in order to solve their problems and fulfill their needs or to convey their desires, problems, and thoughts to the higher levels in the country. However, not all people think the same way and it is rarely and very hard for people to select the same representatives. The best way for people with different desires, points of view, and thoughts to select their representatives is through free and democratic elections. Paper-based elections are used for long periods. If we use it correctly, paper-based election guarantees the winning for whomever the majority of people select. However, paper-based elections have many security holes and can be breached easily besides some other drawbacks such as cost inefficiency, time consumption, and low tally speed ([5], [6], [15]). Therefore, researchers exert great efforts to build electronic election (electronic voting, or e-voting) systems to overcome the drawbacks of the paper-based election system ([7], [8], [16]). E-voting systems have the potential of being cheaper, faster, and easier to be controlled than the paper-based election systems. In addition, e-voting systems have a great impact to increase the participation of voters in the elections. However, e-voting systems need to meet certain security requirements in order to be secure and trusted by voters. This paper introduces a secure e-voting mechanism that satisfies the security requirements for safe and secure elections.

II. RELATED WORK

Electronic voting machines can be classified into two main categories. In the first category, voters use especial equipments in specific locations to cast their votes. This kind of voting is called electronic voting or e-voting.

The second category of electronic voting is called Internet voting or I-voting. In this kind of voting, voters cast their votes online from anywhere using computers or smart phones that are connected to the Internet.

In e-voting schemes, voting machines are kept in specific locations (polling stations) to maintain the physical security of the machines. Voters have to attend in person to the polling stations to cast their votes, so that e-voting mechanisms guarantees the authentications of voters.

As an example of e-voting schemes, the work presented in [3] proposed the direct-recording electronic voting machine (DRE) through which voters mark their votes using a keyboard or a touch screen which is connected to a polling station. The DRE machine immediately adds the votes to the tally and stores it to its memory. At the end of the voting period, the DRE tally is moved to a central location where the tally of other DRE machines are added.

On the other hand, in I-voting schemes, voters' participation increase because they can vote from anywhere in the world. However, voter authentication is very hard. As it rely on the Internet to deliver votes, I-voting schemes suffer from the Internet security concerns. In addition, I-voting schemes need high reliable infrastructure to guarantee the system availability. Examples of I-voting systems can be found in the work presented in ([10], [11], [17]).

This paper proposes a secure e-voting mechanism that is suitable to be used in developing countries as the Internet infrastructure in most of these countries is not matured yet.

III.CHARACTERISTICS OF AN IDEAL E-VOTING SCHEME

All paragraphs must be indented. All paragraphs must be justified, i.e. both left-justified and right-justified.

An ideal voting scheme is expected to satisfy certain requirements. Many studies have addressed

these requirements ([11] – [13]). In the following, a brief description of these requirements is given.

Accuracy: A voting scheme is said to be accurate if it is not possible for a vote to be altered or eliminated from the final tally and it is not possible for an invalid vote to be counted.

Democracy: In a democratic voting scheme, only eligible voters can vote and they can vote only once.

Voter privacy: A voting scheme maintains voter privacy if no one (even the election authorities) can link the ballot to the voter who cast it. In addition, no voter can prove that he voted in a particular way.

Verifiability: A voting system is verifiable if all voters can verify that their votes have been counted correctly without sacrificing privacy.

Scalability: A voting system is scalable if we can deploy it on a variety of scales.

Mobility: A system is mobile if voters can cast their votes from a variety of destinations.

Robustness: A system has to be robust against faults, active and passive attacks.

Eligibility: The system is said to be eligible if only valid voters with certain pre-determined requirements (e.g. age – citizenship) can vote.

Fairness: Before the end of the voting period, no partial tally is revealed to ensure that all candidates are given a fair decision.

Uncoercibility: Any coercer should not be able to extract the value of the vote and should not be able to coerce a voter to cast his vote in a particular way. This requirement is very important to prevent vote buying and extortion that many countries suffer from.

IV. ANATOMY OFTHE E-VOTING PROCESS

The voting process includes some main steps, if correctly followed, it guarantees the security of the overall process and the correctness of the final results. These steps start with the voters' registration step an end with publishing the election results. In the following, we give a brief explanation of the voting steps:

a. ***Registration***: before the voting period and in a certain time, every eligible voter physically shows identification in the registration stage. The registrar checks the eligibility of the voter. If eligible, the registrar gives the voter some voting credentials, and the voter randomly chooses an ID. Then, the registrar blindly signs the ID to the voter. Later and during the voting stage, the validator (or the authenticator) checks for registrar's signature. In the same time, the validator does not know the ID of whoever voted.
b. ***Validation***: Once the voting period starts, voting authorities checks the credentials of who attempting to vote.
c. ***Voting and vote collection***: during this phase, validated voter takes a ballot paper from the authority, chooses his/her preferred candidate, and inserts the ballot paper in the ballot box. The voting authorities collect the voted ballots in the ballot boxes before the final stage of the tally.
d. ***Tallying and result publishing***: At this stage, the voting authorities count and publish the collected ballots to the public.

V. SOME VOTING FALSIFICATION PRACTICES

In this section, we explain the voting process and the vote falsification practices that some countries suffer from.

Most developing countries use paper-based election systems. In such case, voters cannot vote from any polling station. Instead, each voter is assigned to a specific polling center and this is based to the voter's address.

On the election day(s), each voter goes to his assigned polling center with his ID, signs in front of an election authority that verifies his identity to be sure that the voter is eligible to vote and he did not vote before. Then, the voter takes a voting ballot, chooses the candidate that he prefers and places the ballot paper in the ballot box. At the end of the election, ballots are manually counted and the result is announced.

The system seems to be fair and accurate. However, in this manual system, voting falsification may be conducted by candidates and by voting administrators too.

Vote falsification has been the bane of general elections in many countries, especially developing countries. Vote falsification points to the irregularities in any voting phase such as irregularities is voter registration, polling, counting, or tallying and announcing of election results.

For example, in Egypt, candidate vote fraud can be conducted through a technique called the circulating ballot paper. In this technique, a candidate's collaborator prints a single fake ballot paper that need to be good enough not to be detected when being placed in the ballot box. The candidate's collaborator goes to the polling station, takes a ballot paper, keeps it empty, and replaces it with the fake ballot that he places in the ballot box.

After getting out of the polling center, the collaborator marks the real empty ballot paper with the candidate he is representing. Then, he gives the marked ballot to the voter who is willing to sell his vote. The voter goes to the polling center, takes an empty ballot, keeps it empty, and replaces it with the pre-marked ballot. Then, the voter submits the empty ballot to the candidate's collaborator and takes whatever fees he agreed upon [6].

Besides, vote falsification may happen with the conspiracy of the voting authority who is supervising the polling stations by replacing the ballot boxes with other boxes that filled with ballots marked for the government's nominees. Unfortunately, this operation is hard to be detected as long as the fake boxes are

filled with the same number of ballots as the original boxes.

Moreover, voting authorities may add fictitious voters to the voting database. Therefore, more polling boxes corresponding to those fictitious voters are sent to the tallying centers without being detected. Another falsification technique is to fill ballot boxes with ballots on behalf of some voters that did not show up on the election day(s).

Furthermore, voting authorities may provide multiple credentials to a single voter to allow him to vote more than once or they may provide certain credentials to some voters that allow the authorities to track the voters to know how they voted.

By using the electronic voting and security techniques, we can overcome and eliminate these falsification practices.

VI. PROPOSED METHOD

In this proposed voting method, the overall number of entities participate during the voting stages are four, they are:

- ***Registrar (R)***: *R* performs the registration task for citizens who are willing to vote.
- ***Voter (V)***: *V* is a person who wants to cast his/her ballot in a secure way.
- ***Authenticator (A)***:*A* is the authenticator who checks the validity of the voter and ensures that the voter did not vote before.
- ***Tallier (T)***: *T* is a server that accumulates the valid ballots and announce the voting results.

Throughout the paper, the following notations are used:

Notation	***Description***
ek, dk	Encryption/decryption key pair
pk_i/pk_i^{-1}	Public/private keys of party i
$\{m\}_{ek}$	Message encrypted using encryption keyek
$\{m\}_{pk_i}$	Message encrypted using public key ofparty i
$\{m\}_{pk_i^{-1}}$	Message signed using the private key of party i
$(m)_{blind}$	Blinding of message m
$h(m)$	Hash (digest) of message m

The proposed method assumes that every entity in the voting process owns some information. Table 1 shows each entity and the information that entity holds.

VII. TABLE I

INFORMATION HELD by VOTING ENTITIES

Entity	Held Information
R:	- pk_R, pk_R^{-1} - Biometric measures for eligible voters. - $ID1_v$Identity numbers foreligible voters
V	- $pk1_v, pk1_v^{-1}, pk2_v, pk2_v^{-1}$ - pk_A, pk_T, pk_R - $ID1_v, ID2_v$ - B (the ballot) - ek, dk
A	- pk_A, pk_A^{-1} - pk_R - $ID1_v$ (Identifiers for the eligible and registered voters) - $pk1_v$ (public keys for the eligible and registered voters) - $token_v$ (list of tokens for registered voters)
T	- pk_T, pk_T^{-1} - pk_A - $ID1_v, pk1_v$ - VBL *(List of Valid Ballots)* - L1 (An Empty list to store $ID2_v, pk2_v$)

Before voters' registration, the proposed method assumes that the government has a database of the biometric measures (such as fingerprints or Iris) for each citizen who is eligible to vote.

Voter registration phase: election laws differ from one country to another. In some countries, all adults are eligible to vote (except for some citizens such as judges) and are added automatically to the eligible voters' database. While in other countries, citizens that are willing to vote have to register for voting. In case that registration is needed prior to the voting day, the registration can be done using the biometric measures and the ID card of the voter, Fig. 1.shows this process. Several researches have been done regarding voter registration using biometric measures ([1], [4], [9], [14]), by this way of registration, voters can vote from any polling station.

Fig. 1: Voters Registration Process

Before the election day(s), the eligible and registered voters' database is moved to thepollingstations that are connected to a central server, Fig. 2.

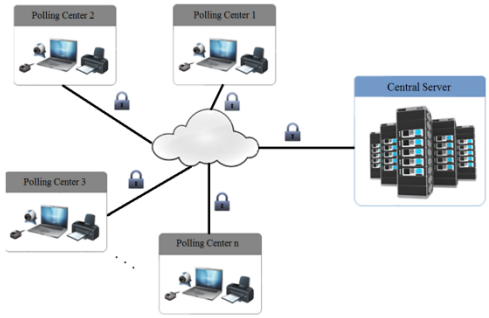

Fig. 2: Structure of Polling Centers

Upon successful registration, the registrar *R* generates a token, signs it, and submits it securely to the voter, this is shown in steps 1 and 2.

1- V → biometric measures + $ID1_v$ → R
2- R →(if eligible) $\{token\}_{pk_R^{-1}}$ → V

Throughout this paper and for the security purpose, every message sent from one entity to another has to be encrypted using the public key of the receiving entity. However, this paper omitted this encryption from the notation of messages for readability.

The token has to be a random value and there is no link between the token and the voter.

The flowchart shown in Fig. 3.shows the voting validity check steps during the registration phase.

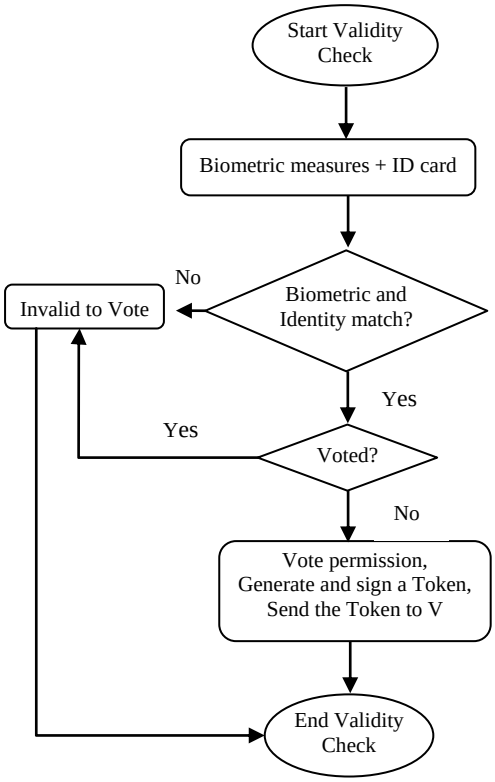

Fig.3: Voting Validity Check

After the validity check step completes and before voting, voters and the tallier follow the following steps to register the second identity and public number pair ($ID2_v$, $pk2_v$):

3- V →$\{((h(pk2_v, ID2_v))_{blind})_{pk1_v^{-1}}, ID1_v\}$→T

In this step. *V* blinds the hash value of $(pk2_v and ID2_v)$, signs the blinded digest with his private key $pk1_v^{-1}$, adds $ID1_v$ and sends the whole message to *T*.

4- T →$\{(h(pk2_v, ID2_v))_{blind}\}_{pk_T^{-1}}$→ V

When *T* receives message 3, it retrieves $pk1_v$ using $ID1_v$, verify the signature of *V*, signs the blinded digest and sends it to *V*.

5- V →$\{(h(pk2_v, ID2_v))_{pk_T^{-1}}, pk2_v, ID2_v\}$→ T

Upon receiving message 4, *V* removes the blind in order to obtain the signature of the tallier on the digest of the pair ($pk2_v$, $ID2_v$), sends the signed digest and the plaintext of the pair to *T*.

When *T* receives message 5, it verifies its own signature, calculates the digest of the received plaintext of the pair. If the calculated digest equals the received one, *T* registers $pk2_v, ID2_v$ in L1.

After this phase completes, *V* has registered twice. V has registered once with R using his biometric measures and $ID1_v$ and also has registered another once with *T* using $ID2_v$ and $pk2_v$.

Before the election day, *R* sends the list of tokens $\{token_v\}_{pk_R^{-1}}$ and the identifiers $ID1_v$ of the registered voters to *A*.

Voting Phase: In order to cast votes, the voter *V* and the authenticator *A* follow the following steps:

6- V→$\{\{(h(\{B\}_{ek}))_{blind}\}_{pk1_v^{-1}}, ID1_v, \{token\}_{pk_R^{-1}}\}$ →A
7- A→$\{(h(\{B\}_{ek}))_{blind}\}_{pk_A^{-1}}$→$V$

Through steps 6 and 7, *A* checks the signature of the registrar *R*, authenticates the identity of *V* using the token, $ID1_v$, and $pk1_v$. If the authentication succeeds, *A* puts a mark in front of $ID1_v$ to trace voters who submitted their tokens, signs the blindeddigest of the encrypted ballot and sends it to *V*.

8- V→$\{\{(h(\{B\}_{ek})_{pk_A^{-1}}\}_{pk2_v^{-1}}, ID2_v, \{B\}_{ek}\}$→$T$
9- T→$\{RN\}_{pk_T^{-1}}$→V

In these two steps, *T* checks its database to be sure that the sending voter whose identity is $ID2_v$ did not vote before. Secondly, it retrieves $pk2_v$ from L1 using $ID2_v$, then it verifies the signatures of the voter *V* and the authenticator *A*. If the signatures' verification succeeds, T computes the digest of $\{B\}_{ek}$ and compare it with the received digest. In case of digest equality,

T inserts $\{B\}_{ek}$ in the VBL and gives it a reference number *RN*, marks $ID2_v$ as VOTED, signs the reference number and sends it to the voter *V*.

10- V →$\{RN\}_{pk_T^{-1}}, dk$→ T

Finally, when the voter *V* receives the signed reference number from the tallier *T*, he sends it and the decryption key of the ballot "*dk*" to *T*. Then, *T* decrypts the ballot and adds it to the final tally.

At the end of the voting stage, *T* publishes the final tally, and the VBL list to the public. Furthermore, the registrar *R* and the authenticator *A* publish the list of the submitted and received tokens $\{token\}_{pk_R^{-1}}$ respectively. Fig. 4 summarizes the overall process (Fig (a)is for the registration phase, andFig (b)is for the voting phase).

VIII. ANALYSIS

In the proposed voting method, V has to register twice; once using his biometric measures with R, and once using ID2, pk2 with *T*. To understand the reason for that consider the following scenario, suppose that the voter has to register only once with *R* using the biometric measures. In this case, the authenticator *A* can cast his own votes to *T* as a voter without being detected. In this case, steps 8, 9, and 10 will be as following:

8- A → $\{(h(\{B\}_{ek})_{pk_A^{-1}}, ID1_v, \{B\}_{ek}\}$→ T

9- T →$\{RN\}_{pk_T^{-1}}$→ A

10- A →$\{RN\}_{pk_T^{-1}}, dk$→ T

From the previous steps, it is clear that, double registration prevents the authenticator from stuffing the ballot box with votes instead of absent voters.

In addition, as both of the registrar *R* and the authenticator *A* publish the list of tokens, *R* cancheck the honesty of *A* by checking his own signature on the tokens.

Furthermore, after the end of voting, the tallier publishes only the valid ballots list VBL to the public (not the list of voters). The reason of that is to overcome the coercibility problem; this problem is serous and widespread in some countries especially in the developing countries. Only the observers of the voting process can get the list of voters in order to ascertain the completeness of the voting process.

However, the system suffers from one main drawback. The system is unverifiable. Only the voting observers can verify the encrypted ballots.

As each voter registers his second identity and public key pair (ID2, pk2) blindly, T cannot link the ballot to the voter who cast it. So that the proposed scheme maintains the privacy of voters. Moreover, the proposed system is eligible and democratic as only valid and eligible voters can get tokens from R. Besides, as T publishes the final tally only after the voting period, no one can get partial results before the end of the voting period. Therefore, the proposed voting scheme maintains the fairness for all candidates.

Likewise, as all polling stations are connected to a central server that stores the voters' measures, voters can cast their votes from any polling station; the validity check algorithm will discover voters who wish to vote more than once. Therefore, the proposed scheme maintains the mobility property.

IX. CONCLUSION AND FUTURE WORK

As conventional election systems suffer from many security concerns, electronic voting schemes become an acceptable alternative. This paper proposed a secure e-voting mechanism that uses the biometric measures to authenticate the eligibility of voters. The proposed method maintains most of the requirements needed for an e-voting system such as privacy, fairness, democracy, and Uncoercibility. The nice feature in the proposed scheme is the voter mobility. Voters can cast their votes from any voting center. However, the weak point in our scheme is that the property of verifiability is not satisfied; only the voting observers can verify the results of the voting process.

As a future work, we plan to implement the proposed voting scheme in a prototype model and compare the results with the results of other voting methods. Moreover, we plan to implement the proposed voting scheme using the Java API for mobile smart phones.

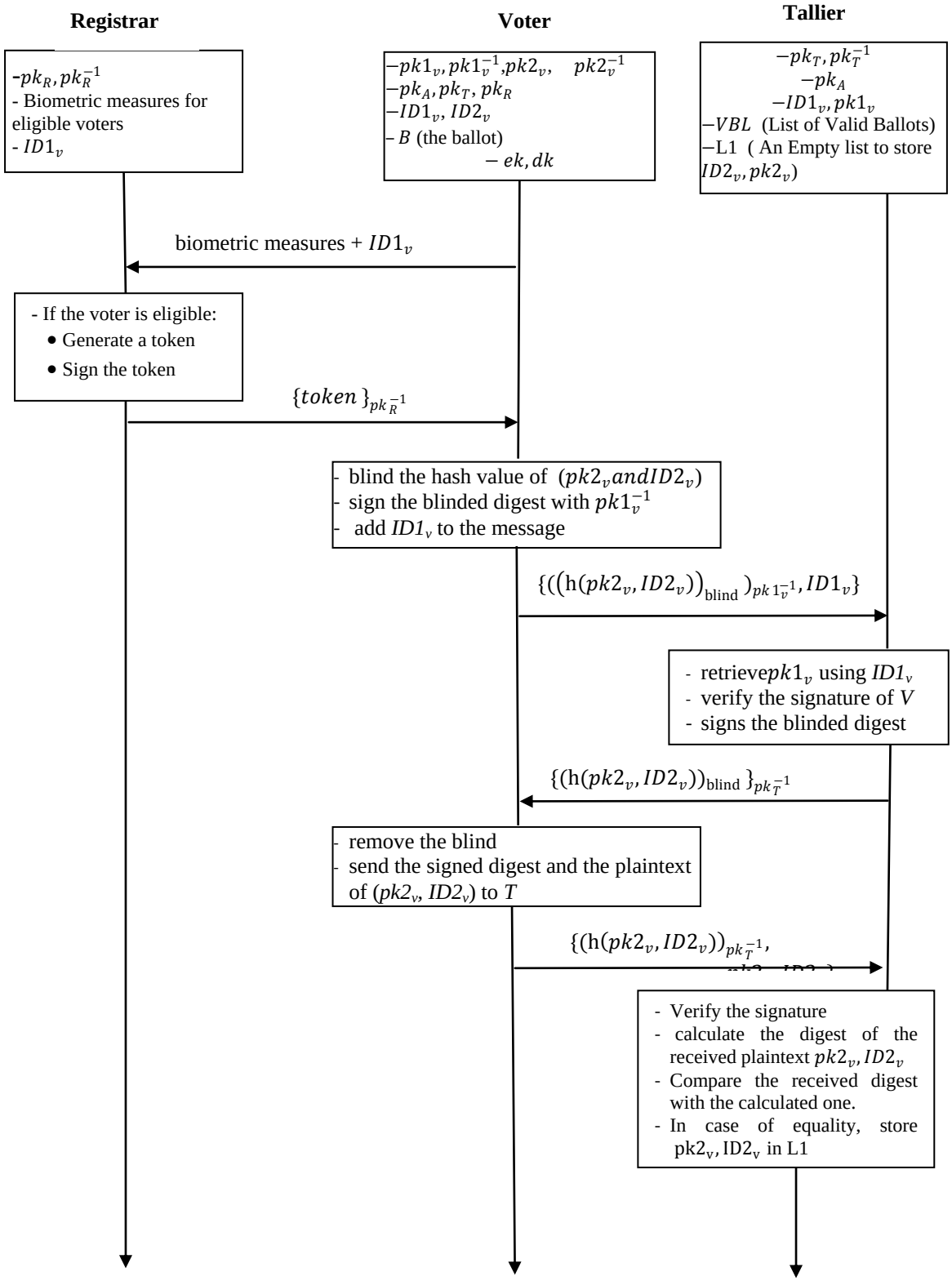

Fig. 4 (a): Registration phase

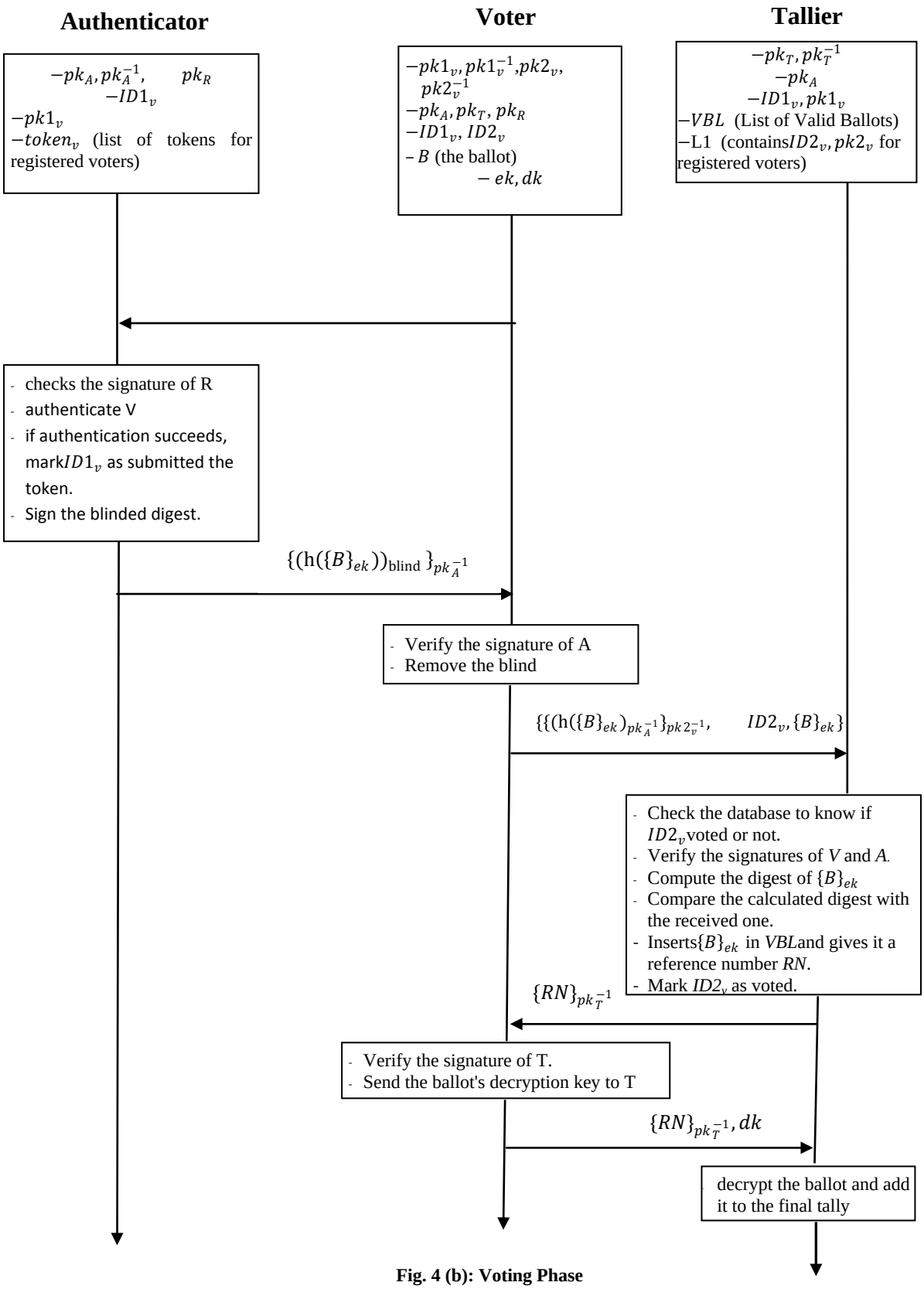

Fig. 4 (b): Voting Phase

REFERENCES

[1] Alaguvel R., Gnanavel G. and Jagadhambal K., "Biometrics using electronic voting system with embedded security," International journal of advanced research in computer engineering & technology (IJARCET), ISSN: 2278 – 1323, Vol. 2, No. 3, 1065-1072, 2013.

[2] D. Demirel, R. Frankland and M. Volkamer, "Readiness of various e-voting systems for complex elections,"TechnischeUniverstität Darmstadt, Tech. Rep. TUD-CS-2011-0193, 1–14, 2011.

[3] Dill, D., R., Mercuri, P., Neumann, and D., Wallach (2003) Frequently asked questions about DRE voting system. [online]. Available:https://www.verifiedvoting.org/resources/voting-equipment

[4] Dixit, P.V., Phalke, S., Ubale, R., Gavali, A.B., Prajkta, S. and Aparna, S., "A Biometric-Secure E-Voting System for Election Process," International Journal of Advanced Engineering and Global Technology, ISSN No: 2309-4893, Vol. 3, Issue 3, 2015.

[5] Kelsey J., Regenscheid A., Moran T., Chaum D."Attacking Paper-Based E2E Voting Systems," In: Chaum D. et al. Towards Trustworthy Elections. Lecture Notes in Computer Science, vol 6000, pp. 370–387. Springer, Berlin, Heidelberg, 2010

[6] MagdiAmer and Hazem El-Gendy, "Towards a Fraud Prevention E-Voting System". International Journal of Advanced Computer Science and Applications (IJACSA), vol.4 No.4, 147-149, 2013.

[7] M.J. Moayed, A. Abdul Ghani & R. Mahmod, "A survey on Cryptography Algorithms in Security of Voting System Approaches," Proceedings of the International Conference on Computational Sciences and Its Applications(ICCSA), 190 – 200, 2008.

[8] Mona F M Mursi, Ghazy M R Assassa, Ahmed Abdelhafez and Kareem Abo M Samra, "On the Development of Electronic Voting: A Survey," International Journal of Computer Applications, Vol. 61 No. 16, 2013.

[9] Noha E. El-Sayad, Rabab Farouk Abdel-Kader and Mahmoud Ibraheem Marie, "Face Recognition as an Authentication Technique in Electronic Voting," International Journal of Advanced Computer Science and Applications (IJACSA), Vol. 4 No. 6, 2013.

[10] Purushothama B R & Alwyn R Pais, "Design and Implementation of Secure Internet Based Voting System with User Anonymity using Identity Based Encryption System," IEEE International Conference on Services Computing, 474 – 481, 2009.

[11] Qadah, G. Z. and Taha, R., "Electronic voting systems: Requirements, design, and Implementation," Computer Standards & Interfaces, Vol. 29 No. 3, 376–386, 2007.

[12] Rossler, T. G. (2012). "e-Voting A Survey and Introduction," Austria Secure Information Technology Center.-2004.Available:https://www.a-sit.at/pdfs/evoting_survey.pdf

[13] Sampigethaya K. and Poovendran R., "A framework and taxonomy for comparison of electronic voting schemes," Computers & Security, Vol. 25, No. 2, 137-153, 2006.

[14] S. Kumar and M. Singh, "Design a secure electronic voting system using fingerprint technique," International journal of computer science issues, Vol 10, issue 4, No 1, 2013.

[15] Thomas Bronack. "The problems with a paper based voting system," [online white paper]. Available: http://www.dcag.com/images/White_Paper_-_The_problems_with_a_paper_based_voting_system.pdf

[16] L. Rura et al., "Online Voting System Based on Image Steganography and Visual Cryptography," Journal of Computing and Information Technology, Vol. 25, No. 1, pp. 47–61, March 2017.

[17] Sid diquee et al., "A Scalable and Secure MANET for an i-Voting System," Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 8:3, pp. 1-17, , September, 2017.