Implementation of Simple Verifiability Metric to Measure the Degree of Verifiability of E-Voting Protocol

Teguh Nurhadi Suharsono
Faculty of Engineering
Universitas Sangga Buana YPKP
Bandung, Indonesia
teguh.nurhadi@usbypkp.ac.id

Dini Anggraini
Informatics Engineering
STMIK LPKIA
Bandung, Indonesia
dinianggraini026@gmail.com

Kuspriyanto
School of Electrical Engineering and Informatics
Institut Teknologi Bandung
Bandung, Indonesia
kuspriyanto@yahoo.com

Budi Rahardjo
School of Electrical Engineering and Informatics
Institut Teknologi Bandung
Bandung, Indonesia
br@paume.itb.ac.id

Gunawan
Faculty of Engineering
Universitas Sangga Buana YPKP
Bandung, Indonesia
gunawan@usbypkp.ac.id

***Abstract*— Verifiability is one of the parameters in e-voting that can increase confidence in voting technology with several parties ensuring that voters do not change their votes. Voting has become an important part of the democratization system, both to make choices regarding policies, to elect representatives to sit in the representative assembly, and to elect leaders. the more voters and the wider the distribution, the more complex the social life, and the need to manage the voting process efficiently and determine the results more quickly, electronic-based voting (e-Voting) is becoming a more promising option. The level of confidence in voting depends on the capabilities of the system. E-voting must have parameters that can be used as guidelines, which include the following: Accuracy, Invulnerability, Privacy and Verifiability. The implementation of the simple verifiability metric to measure the degree of verifiability in the e-voting protocol, the researchers can calculate the degree of verifiability in the e-voting protocol and the researchers have been able to assess the proposed e-voting protocol with the standard of the best degree of verifiability is 1, where the value of 1 is is absolutely verified protocol.**

Keywords*— *e-voting, verifiability, simple verifiability metric

I. INTRODUCTION

General elections are part of a democratic process. Indonesia is a democracy that holds general elections every five years. In Indonesia, the implementation of general elections is carried out starting from the village level (village head election), city / district level (election for mayors / regents and members of DPRD level 2), provinces (election for governors and members of DPRD 1), to the level of central government (president and members DPR). General elections in Indonesia are still carried out manually. Citizens who have the right to vote come to the polling station on election day. They then vote or check (✓) the ballot paper and then put it in the ballot box.

The problem of technological development that cannot be stopped, makes some assistance for certain problems can be solved with technology, especially in terms of voting problems. In the election, the issue of technology is quite considered by various groups, especially those who will fight in the election. The more complex aspects of social life, and the need to manage the voting process efficiently and determine the results more quickly, one of which is how elections use technology assistance or what is often called e-Voting. E-Voting is a method of voting using electronic media or electronic (digital) devices starting from the voter registration process, implementing elections, counting votes, and sending the results of votes.

E-Voting must have parameters that can be used as guidelines, namely a statement known as the Golden Rules of e-Voting, which includes the following[1]:

1. accuracy: the choice cannot be changed, the sound cannot be eliminated and the disabled sound cannot be counted;
2. invulnerability: only those who have the right can vote and vote only once;
3. privacy: the choice is unknown and the voice choice cannot be proven;
4. Verifiability: voters' votes and vote count results can be re-verified.

Of the four parameters of e-Voting above, the Verifiability parameter is the most dominant in improving e-voting quality. With the Verifiability parameter, it gives confidence and trust to voters that the voting system used will provide protection, both for the votes given and for the voters themselves. To fulfill the Verifiability requirements, 12 Verifiability requirments have been described, namely[2]:

1. Voters can verify that voters have not made their choice before the election
2. Officers can verify that voters have not made their choice before the election
3. Witnesses can verify that voters have not made their choice before the election

978-1-7281-7598-0/20/$31.00 ©2020 IEEE

4. Voters can verify that the voter choice of voters has not changed and is included in the vote count after voting
5. Voters can verify that the voters' choice of votes has not changed and is included in the vote count after performing the vote count
6. Officers can verify that the voters' choice of votes has not changed and is included in the vote count after voters have made a vote
7. Witnesses can verify that the voters' choice of votes has not changed and is included in the vote count after voters have made a vote
8. The KPU (General Election Commissions) can verify that the voters' choice of votes has not changed and is included in the vote count after voters have made a vote
9. Officers can verify that the voter choice of voters has not changed and is included in the vote count after the vote count
10. Witnesses can verify that the vote choices of voters have not changed and are included in the vote count after the vote count
11. KPU may verify that the voting choices of voters have not changed and are included in the vote count after the vote count
12. Voters can ensure their choices do not change during election

To measure the degree of verifiability, a metric is needed so that it can be assessed how the degree of verifiability of the e-Voting protocol. The implementation of the simple verifiability metric to measure the degree of verifiability in the e-voting protocol, the researchers can calculate the degree of verifiability in the e-voting protocol and the researchers have been able to assess the proposed e-voting protocol with the standard of the best degree of verifiability is 1, where the value of 1 is is absolutely verified protocol[2].

II. Literature Review

In study [2] individual verification requirements were determined. Based on this, the Individual Metric was created, which only measures the verifiability of the voters. In research [3], the measurement of verifiabity is also considered the need for anonymity, where anomyty is the opposite of verifiability, that is, how other parties cannot see or predict the voters' choice of votes. In this research, a simpler metric is produced to measure verifiability and can meet all the verifiability needs of voters, officers, witnesses and the KPU.

III. Simple Verifiability Metric Proposed

The definition of a metric according to[4] (Idika, 2010) is a value that facilitates decision making and is derived from measurement. According to [5] (Hayden, 2010) metrics are results while measurement is activity. Measurement is the activity of carrying out observation and data collection in an effort to gain a practical view of what is being tried to understand.

The metric for measuring Verifiability in the e-Voting system is the formula:

$$V_T = \frac{\sum_{i=1}^{n} v_i}{n} \quad \text{(III.1)}$$

where:

V_T = Degree of Verifiability

v_i= Value of Verifiability Requirements (0 or 1)

n= Total of Verifiability Requirements

Pseudocode of simple verifiability metric is:

Input : v_i , n
Output : V_T

Input $v_i \leqq n$
Do while X = Yes
    if choice = X
        $X = 1$
    else
        X = X+1
        total= total + X
    endif
endwhile
    V_T =Jtotal/n

IV. Implementation Of Simple Metric Verifiability

From table 1 below, it is assumed that an assessment of the need for verification has been carried out.

Table 1. Example for requirement of e-voting protocol

Code	Requirement Verifiability	Value of Requirement *Verifiability*
KV1	Voters can verify that voters have not made their choice before the election	1
KV2	Officers can verify that voters have not made their choice before the election	1
KV3	Witnesses can verify that voters have not made their choice before the election	1
KV4	Voters can verify that the voter choice of voters has not changed and is included in the vote count after voting	1
KV5	Voters can verify that the voters' choice of votes has not changed and is included in the vote count after performing the vote count	0
KV6	Officers can verify that the voters' choice of votes has not changed and is included in	1

Code	Requirement Verifiability	Value of Requirement *Verifiability*
	the vote count after voters have made a vote	
KV7	Witnesses can verify that the voters' choice of votes has not changed and is included in the vote count after voters have made a vote	1
KV8	The KPU can verify that the voters' choice of votes has not changed and is included in the vote count after voters have made a vote	1
KV9	Officers can verify that the voter choice of voters has not changed and is included in the vote count after the vote count	0
KV10	Witnesses can verify that the vote choices of voters have not changed and are included in the vote count after the vote count	1
KV11	KPU may verify that the voting choices of voters have not changed and are included in the vote count after the vote count	1
KV12	Voters can ensure their choices do not change during election	1

Based on table 1 above, it can be seen that there are some parties who do not verify, namely with the value of the need for Verifiability = 0.From formula (1) the level of verification is calculated, namely: the sum of all the values for the verifiability requirement which in this example is 10. obtained the value of the Verifiability Level is 10/12 = 0.83.

$$V_T = \frac{10}{12} = 0.83$$

Based on the interpretation of the degree of verification, the value of 0.83 means that the protocol is almost absolutely verified.

V. CONCLUSION

The implementation of the simple verifiability metric to measure the degree of verifiability in the e-voting protocol, the researchers can calculate the degree of verifiability in the e-voting protocol and the researchers have been able to assess the proposed e-voting protocol with the standard of the best degree of verifiability is 1, where the value of 1 is is absolutely verified protocol.

REFERENCES

[1] Cranor, Lorrie Faith, and Ron K. Cytron. 1997. "Sensus: A Security-Conscious Electronic Polling System for the Internet." Proceedings of the Hawaii International Conference on System Sciences 3(c): 561–70.

[2] Suharsono, Teguh Nurhadi, Kuspriyanto, and Budi Rahardjo. 2019. "Individual Verifiability Metric in E-Voting System." International Journal on Electrical Engineering and Informatics 11(1): 101–11.

[3] Suharsono, Teguh Nurhadi, Kuspriyanto, and Budi Rahardjo, Verifiability Metric Notion in e-Voting System, 2019 IEEE 13th International Conference on Telecommunication Systems, Services, and Applications (TSSA).

[4] Idika, N. C. (2010): Characterizing and aggregating attack graph-based security metrics., Disertasi Program Doktor, Purdue University, West Lafayette, Indiana.

[5] Hayden, L. (2010): IT Security Metrics. New York, The McGraw-Hill Companies.