2021 15th International Conference on Telecommunication Systems, Services, and Applications (TSSA) | 978-1-6654-2892-7/21/$31.00 ©2021 IEEE | DOI: 10.1109/TSSA52866.2021.9768253

e-Voting Protocol Modelling To Improve Verifiability Requirements

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

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

Rini Nuraini Sukmana
Department of Informatics,
Faculty of Engineering
Universitas Sangga Buana
Bandung, Indonesia
rnurainisukmana@gmail.com

***Abstract*— The ability of the voting system to protect voter votes until the end of the process can increase public confidence in the voting system. The verifiability aspect allows several parties to ensure that there is no change in the vote of the voters, thereby increasing trust in voting technology. To get to the concept of the proposed system of e-voting, an analysis e-voting needs has been carried out and the stage of the protocol model design analysis for verifiability needs. Some parties involved in meeting the needs of verifiability are Voters, Officers, Witnesses or KPU (Commission of General Election), where some parties can verify the votes of voters before, during, after, and after the vote count in election. In fulfilling the verifiability needs of this e-voting system, traditional simulation modeling and voting testing have been carried out as a comparison with modeling simulations and testing of e-voting protocols. Before modeling simulation and protocol testing, formal notation writing was carried out in the form of Communicating Sequential Processes (CSP) notation. Protocol testing will be carried out with formal verification, which proves that protocol specifications are in accordance with the integrity properties that have been defined previously. The verification tool used is based on reference modeling, which can analyze the specifications logical consistency, and verified properties reports, namely SPIN (Simple Promela Interpreter). The verified system used PROMELA language (MEta LAnguage process) which is translated from CSP formal notation.**

Keywords—:e-voting protocol; verifiability requirements; formal notation; formal method.

I. Introduction

The electoral system uses paper ballots which began to be used in 1856 (Victoria, Australia) and 1889 America (New York). The technology to help elections to grow. The "Myers Automatic Booth" voting machine that used levers in Lockport, New York in 1892, punchcard began to be used in Georgia in 1964. The electronic-based machines began to be made and used, including: Marksense (using optical scan techniques) began to be used in 1996 for the American presidential election, and a variety of DRE (Direct Recording Electronic) devices [1].

In addition to the type of e-voting that still requires the presence of voters physically to the voting booth (for example: the use of optical scan systems and DRE), there are also types of e-voting that do not require voters to be physically present (eg Polling Station Remote Voting where voting via telephone, sms, internet, digital TV etc.) [2]. E-voting is an election system where data is recorded, stored, and processed in the form of digital information [3]. Centinkaya and Centinkaya added that e-voting is the use of computer equipment or a computerized voting process for voting cards on voting [4]. e-voting is essentially the implementation of voting conducted electronically (digitally) starting from the voter registration process, carrying out the election, vote counting and sending the results of the vote.

The e-voting is expected to overcome the conventionally elections problems, namely [5] [6].

1. Faster in vote counting.
2. More accurate vote count results.
3. Ballot paper is more economical.
4. Save on ballot distribution cost.
5. Various language versions can be used on the ballot paper.
6. More voting information can be accessed.
7. Controlling those who are not entitled to choose.

Four main activities of voting to ensure certainty of choice [7] :

1. Registration: voting participant registering in accordance with applicable regulations.
2. Validation: to get voters who meet the criteria as voters and avoid data duplication, a voter data validation process is carried out.
3. Collection: vote collection.
4. Tallying, counting votes.

According to [7] states that e-voting must have parameters that can be used as guidelines. A statement known as the Golden Rules e-voting, which includes:

- accuracy: the choice does not change, the ballot cannot be eliminated and the defective ballot is not counted.
- invulnerability: choose only once and they are entitled.
- privacy: Vote choices from voters cannot be proven and cannot be known by anyone.
- verifiability: Can re-verify voter votes and vote count results.

The voting technology implemention cannot be well received by the wider community. This is greatly influenced by the level of public trust in the quality of voting technology used [7].

It can be that the verifiability is the most dominant thing in improving the quality of voting technology. The

978-1-6654-2892-7/21/$31.00 ©2021 IEEE

verifiability gives confidence to the voters that the voting system used will provide safety. [8]. In the e-voting system data security can be divided into security related to the ballot (starting from the voting stage to the calculation phase), and verification by voters to ensure that the contents of the ballot do not change and has been calculated correctlyr [9].

In this study, e-voting protocol modeling was proposed to accommodate verifiability needs. In this protocol, the Verifiability aspect must be able to accommodate the requirements of voters, officers, witnesses, and the KPU (General Election Commission), thus increasing the reliability of the e-voting system. Before modeling simulation and protocol testing, formal notation was written in the form of Communicating Sequential Processes (CSP) notation. Protocol testing will be done with formal verification. An important step in validating a communication program or protocol is to use formal verification. Consists of proving that the protocol specifications are in accordance with several previously defined properties. The verification tool used is based on reference modeling, which can analyze the specifications logical consistency, and verified properties reports, namely SPIN (Simple Promela Interpreter). The verified system used PROMELA language (MEta LAnguage process) which is translated from CSP formal notation [10].

II. Literature Review

According to [11] verifiability is an electronic voting system that must provide a method to verify that the system works as expected. Voters must be able to verify the results of their votes according to their choices and be taken into account in the process of counting the votes. The auditor must be able to verify that all votes by the eligible voters who can enter the vote count. Verifiability aims to ensure the correctness of the votes given by voters. This technique is known as voter verification method, voter verifiable voting system and voter verified paper audit trails (VVPAT) [12]. This method gives trust to voters that the voting system used will provide security, both to the votes given and to the voters themselves [13].

Vote verification is one way to ensure the ballot paper is in accordance with the choice of voters. For voters, the goal is that the system in which each voter without special training must easily convince himself of the results of calculating the vote does reflect actual elections. With the aim of achieving different levels and scopes of verification requirements, it can be used in different e-voting phases [14].

In the system of e-voting system, verifiability aspect is one of the most dominant parameters, so that it becomes one of the parties determining the quality level of the e-voting system. Several related studies have conducted verifiability for several parties involved such as Voters, Officers and Witnesses, but not thoroughly for the e-voting system phase during elections, after elections and after vote count. This causes a decrease in the level of public confidence in the quality of the e-voting system. The KPU as the highest electoral institution involved as one of the parties to voting, in other studies did not conduct verification. So Verifiability is where ballot verification is carried out by several parties, namely by Voters called Individual Verifiability and by Officers, Witnesses and KPU called Universal Verifiability that the votes chosen by the Voters do not change and are included in the vote count and vote verification from before, dutring, after the election, and after the vote count is referred to as Verifiability of End-to-End.

The study there is a Protocol (P) which can improve verifiability (V) on e-voting, with the concept of Protocol (P):

1. By involving the Voter Party (V), Officer (O), Witness (W) and KPU (C)
2. Verifiability involving the Voter Party (V) is called Individual Verifiability (IV)
3. Verifiability involving the Officer (O), Witness (W) and KPU (C) is called Universal verifiability (UV)
4. Verifiability is done in Phase before selection (bv), during selection (ov), after selection (av), and after vote counting (ac) which is called End-to-End Verifiability ($e2e$)
5. Individual Verifiability Integration (IV), Universal verifiability (UV) and End-to-End Verifiability ($e2e$) output "rejects") and runs Verify (τ,α). If Verify (τ,α) evaluates "wrong" or "true", respectively, sending "reject" or "accept" to Judge J. The definition [1] does not explicitly explain about the voter always verifying whether it was triggered or not. So the protocol model looks decided to verify according to several possible distributions.

III. Proposed E-Voting Protocol Modeling

A protocol is a set of rules that govern the interaction of processes simultaneously on a distributed system [15]. . According to [16], the protocol is a rule that contains a series of steps, involving two or more people, which are made to complete an activity. Protocols in information technology are a set of specific rules in the use of telecommunications connections when communicating. The protocol determines the interaction between communicating entities [17].

According to [18] e-voting protocols, voters, may use a number of voter support devices (VSD / Voter Supporting Devices) (for example, desktop computers or smartphones), count the number of ballots, usually contain a choice of voters in encrypted or encoded form, and include his voice. Voting is placed on the bulletin board. Voice mail is collected (for example, from a bulletin board) and is counted by the teller / voting authority.

The design and development of protocol modeling for verifiability aspects of e-voting was designed according to the results of the protocol model design analysis for verifiability aspects.

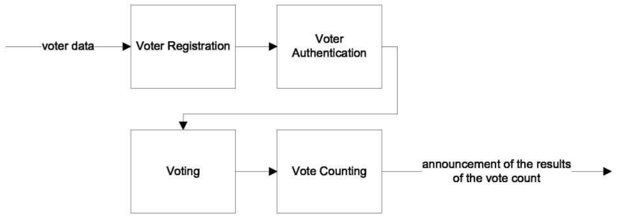

Fig. 1. E-voting system protocol modeling

In Figure 5 shows the protocol modeling for the e-voting system, with detailed protocols as follows:

1. Voter Registration Protocol

The Voters Registration Protocol in the e-voting system is as follows:

1. Voters register to the E-Voting website by inputting data in accordance with the identity printed on their respective Identity Card (KTP) and filling in the public key.
2. The data entered will be matched (Verification) with the KTP data registered with the KPU.
3. If the data entered by the voter does not have a match with the KTP data on the KPU, the registration process is stopped and if the data entered by the voter has a match, then the voter id and Public key will be stored in the E-Voting database
4. The public key is used to encrypt the ballot selection that will be distributed at each polling station that can be decrypted by the voter using the private key selector during the election.
5. Voters will get a voter ID QR Code via email along with the TPS name and TPS address.

Formal notation for voter registration protocols on e-voting systems that describe communication between entities using CSP as follows:

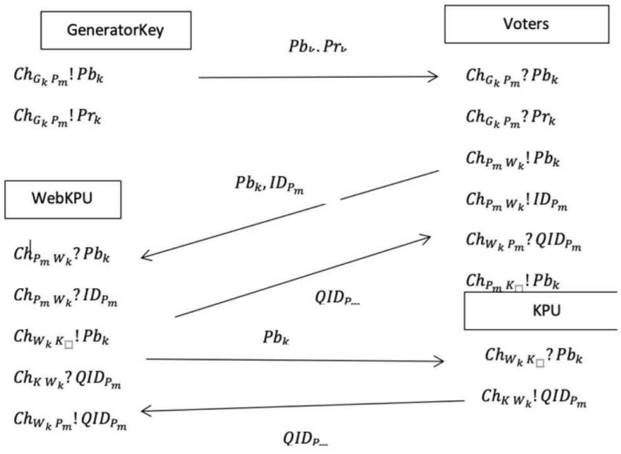

Fig. 2. CSP Formal Notation for Protocol Voter Registration on the e-Voting system

2. Voter's Authentication Protocol

The Selector authentication protocol is as follows:

1. The voter brings the voter ID and QR Code ID to the polling station
2. The officer checks the voter's ID card followed by scanning the voter QR Code id to ensure the voter has been registered in the E-Voting system and has not made an election. If the Voter's status is valid, the Officer submits the KTP voter and QR Code id to the Witness, if it's not valid, the Voters are not allowed to vote.
3. The witness checks the ID card voter followed by scanning the QR Code of the ID voter to ensure the voter has been registered in the system of E-Voting and has not made an election. If the Voter's status is valid, the Witness submits the voter's KTP and QR Code id to the Officer, if it's not valid, the Voters are not allowed to vote.

If the entire authentication process is complete and the valid voter is allowed to make the selection process and the Officer returns the KTP, the Voter ID Code and the No queue to the Voters.

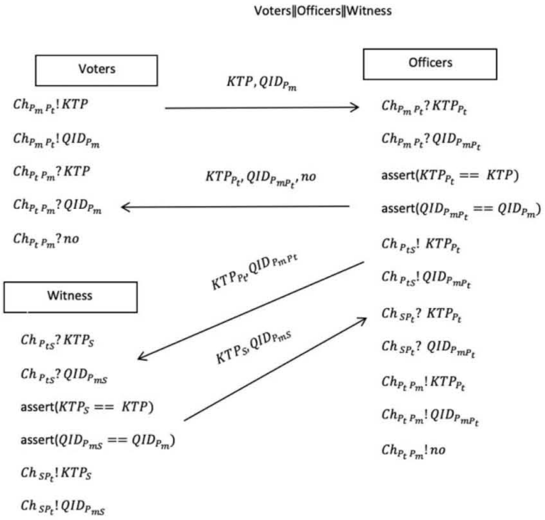

Fig. 3. CSP Formal Notation for the Voter Authentication Protocol on the e-Voting system

3. Voting Protocol

The voting protocol is as follows:

1. The voter selects by entering the E-Voting application and scanning the QR Code id selector to find the ballot Selector that has been encrypted.
2. After ballot is found in the system, the selector is required to decrypt the ballot by using the private key selector.
3. Voters vote for candidates.
4. The filled ballot will be encrypted again with the public key selector and hashing to the choice, saved to the TPS Database.
5. Voters get proof of election in the form of a QR Code that can be verified to ensure the choice does not change.

Formal notation for the voting protocol that describes communication between entities using CSP as follows:

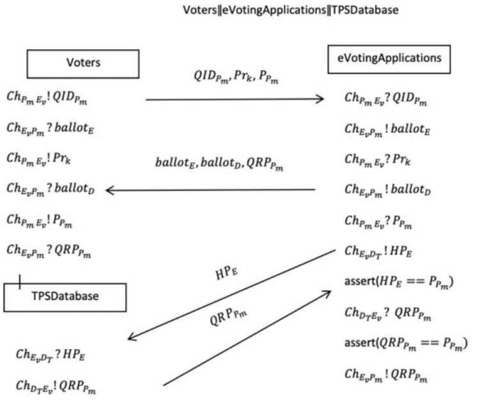

Fig. 4. CSP Formal notation for the voting protocol on the e-Voting system

4. Vote Counting Protocol

The vote counting protocol is as follows:

1. Selection data collected from each polling station will be calculated by the E-voting system and stored in the TPS Database.
2. Voters can do verifiability by bringing proof of election in the form of a QR Code that contains the results of an encrypted hashing option and private key to the KPU or after the election at the polling station.
3. Officers, the Witness can verify the results of vote counting through ballot blocks.
4. The officer will upload block ballot results of the vote count to the Central database on the KPU.
5. KPU can verify the results of the vote count for each polling station from the upload ballot by the Officer.

Formal notation for the vote counting protocol that describes communication between entities using CSP as follows:

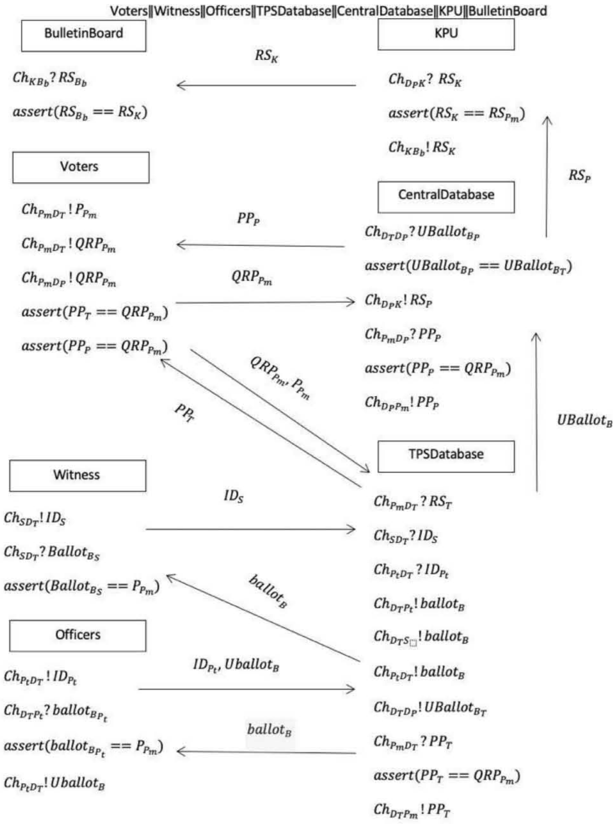

Fig. 5. CSP Formal notation for the vote counting protocol on the e-Voting system

The description for all formal CSP notations used in the e-voting protocol can be seen in table I.

Table I. Description of CSP Formal Notation for e-Voting Protocol

Notation	Description
‖	Paralel
?	Input
!	Output
==	comparison
$Ch_{G_k P_m}$	Channel Generator Key to Voters
$Ch_{P_m W_k}$	Channel Voters to Web KPU
$Ch_{W_k P_m}$	Channel Web KPU to Voters
$Ch_{P_m K}$	Channel Voters to KPU
$Ch_{W_k K}$	Channel Web KPU to KPU
$Ch_{K W_k}$	Channel KPU to Web KPU
$Ch_{P_m P_t}$	Channel Voters to Officers
$Ch_{P_t P_m}$	Channel Officers to Voters
$Ch\ _{P_tS}$	Channel Officers to Witness
$Ch\ _{SP_t}$	Channel Witness to Officers
$Ch_{P_m E_v}$	Channel Voters to e-Voting Application
$Ch_{E_vP_m}$	Channel e-Voting Application to Voters
$Ch_{E_vD_T}$	Channel e-Voting Application to Local TPS Database
$Ch_{D_TE_v}$	Channel to Local TPS Database to e-Voting Application
Ch_{KB_b}	Channel KPU to Bulletin Board
Ch_{D_PK}	Channel Central Database to KPU
$Ch_{P_mD_T}$	Channel Voters to Local TPS Database
$Ch_{P_mD_P}$	Channel Voters to Central Database
$Ch_{D_TD_P}$	Channel Central Database to Central Database
$Ch_{D_PP_m}$	Channel Central Database to Voters
Ch_{SD_T}	Channel Witness to Local TPS Database
$Ch_{P_tD_T}$	Channel Officers to Local TPS Database
$Ch_{D_TP_t}$	Channel Local TPS Database to Officers
Ch_{D_TS}	Channel Local TPS Database to Witness
$Ch_{D_TP_m}$	Channel Local TPS Database to Voters
$ballot_{B_{P_t}}$	Block Ballot at Officers
$Ballot_{B_S}$	Block Ballot at Witness
$ballot_B$	Block Ballot
$Uballot_B$	Upload Block Ballot
$UBallot_{B_T}$	Block Ballot upload results in the Local TPS Database
PP_T	Voters vote options in the Local TPS Database
ID_S	ID Witness
ID_{P_t}	ID Officers
RS_T	Results of vote counting verification in the Local TPS Database
PP_P	Voters votes in the Central Database
RS_P	Results of vote counting verification in the Central Database
Pb_k	Public Key Voters
Pr_k	Private Key Voters
ID_{P_m}	Voters Identity
QID_{P_m}	QR Code ID Voters
$UBallot_{B_P}$	Results of uploading Ballot Block in the Central Database
KTP	Voters Identity Card
no	Queue Number for Voters
KTP_{P_t}	Voters Identity Cards at Officers
$QID_{P_{mP_t}}$	QR Code ID Voters at Officers
KTP_S	Voters Identity Card located in Witness
$QID_{P_{mS}}$	QR Code ID Voters who are in Witness
$ballot_E$	*Encrypted ballot*
$ballot_D$	*Decypted ballot*
P_{P_m}	Voters vote selection results
QRP_{P_m}	QR Code Proof of Voters vote selection
HP_E	The Encrypted hashing result is the choice of the ballot hashing
RS_{B_b}	The vote count results on the Bulletin Board

Notation	Description
RS_K	Results of vote count verification at the KPU
RS_{P_m}	Voters vote selection verification results
$assert$	Testing integrity properties

IV. Simulation of Protocol e-Voting Modelling

Based on the formal notation in section 3, simulations and formal verification of the e-voting protocol were carried out using Promela language and Spin tool. Simulation is carried out under ideal protocol conditions, where the protocol runs as expected The properties tested from the protocol are integrity properties using assert conditions.

The modeling simulation on the e-voting protocol is carried out as follows:

1. Voters Registration Protocol

In figure 6 shows a simulation of Voters authentication protocol on traditional voting in ideal conditions, which consists of several entities involved:

0. Generator Key
1. Voters
2. WebKPU
3. KPU

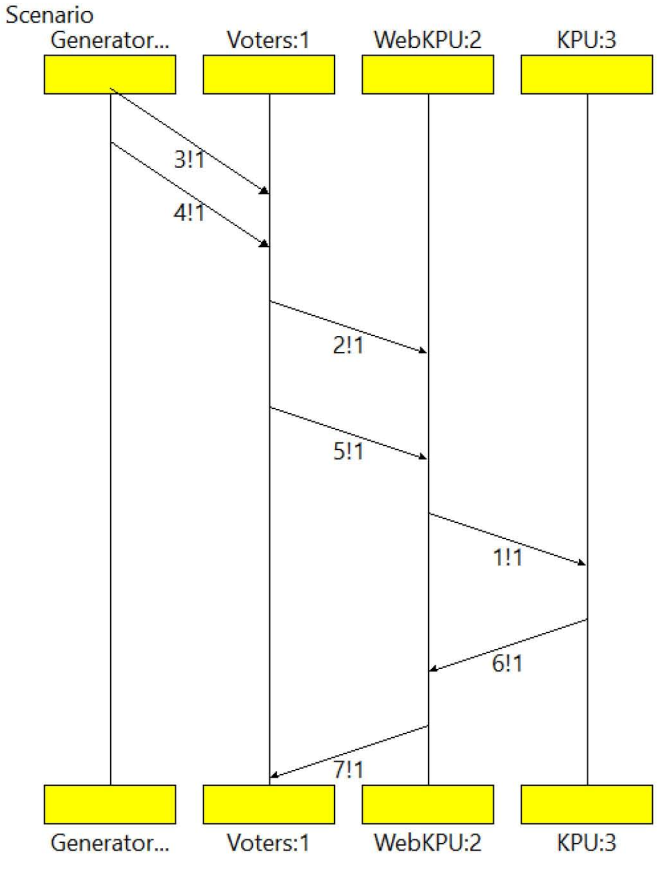

Fig. 6. Simulation of the Voters registration protocol on the e-voting system

The ideal condition expected from the e-voting protocol is to maintain the integrity of Voters Data from the KPU until it is given to Voters, but when Voters gives identity = 1 then when the KPU verifies Voters Data the value is still 1, Voters data does not change get to Voters, keep Voters data = 1. The test done is to test the property integrity with assert.

2. Voters Authentication Protocol

In Figure 7 shows a simulation of the Voters authentication protocol in the e-voting system in ideal conditions, which consists of several entities involved:

0. Voters
1. Officers
2. Witness

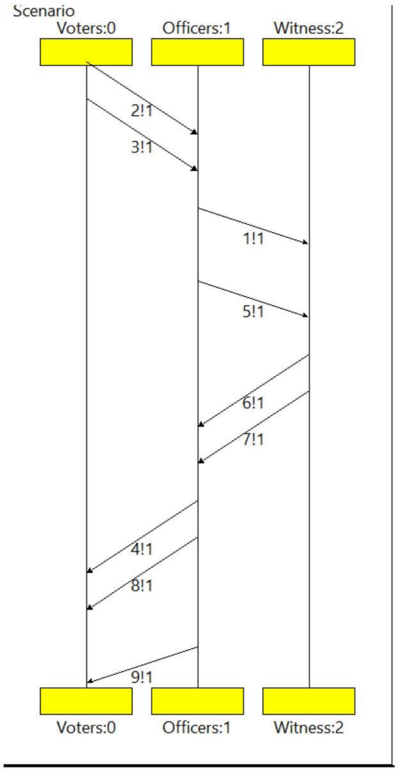

Fig. 7. Simulation of the Voters authentication protocol on the e-voting system

The ideal condition expected from the e-voting protocol is to maintain the integrity of data from Voters, ie when Voters identifies = 1, Voters identity does not change at Officers or Witness. The test done is to test the property integrity with assert.

3. Voting Protocol

In figure 8 shows the simulation of the voting protocol on traditional voting in ideal conditions, which consists of several entities involved:

0. Voters
1. e-Voting Application
2. TPS Database

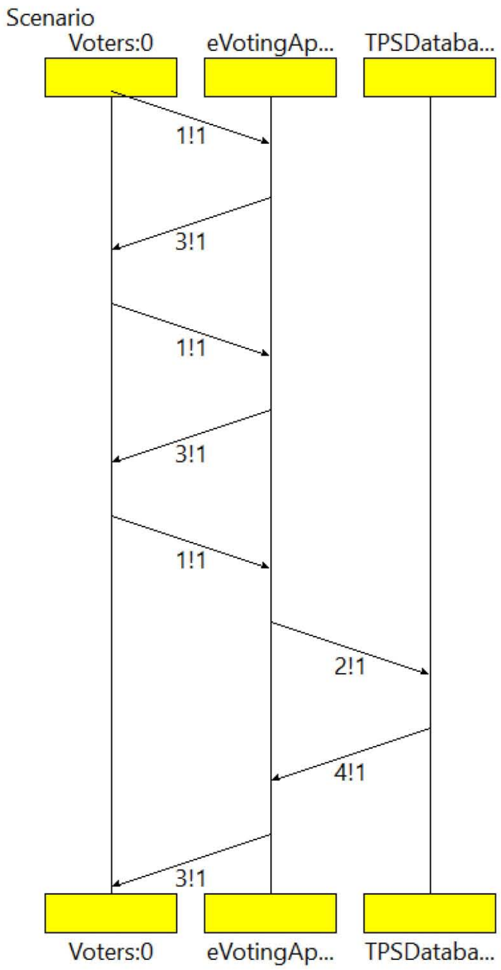

Fig. 8. Simulation of the voting protocol on the e-voting system

The ideal condition expected from the e-voting protocol is maintaining integrity of voice data from Voters, ie when Voters votes = 1, the voice of Voters does not change until the TPS Database = 1. The test done is to test the property integrity with assert.

4. Vote Counting Protocol

In figure 9 shows the simulation of the voting protocol on traditional voting in ideal conditions, which consists of several entities involved**:**

0. Voters
1. Witness
2. Officers
3. TPSDatabase
4. CentralDatabase
5. KPU
6. BulletinBoard

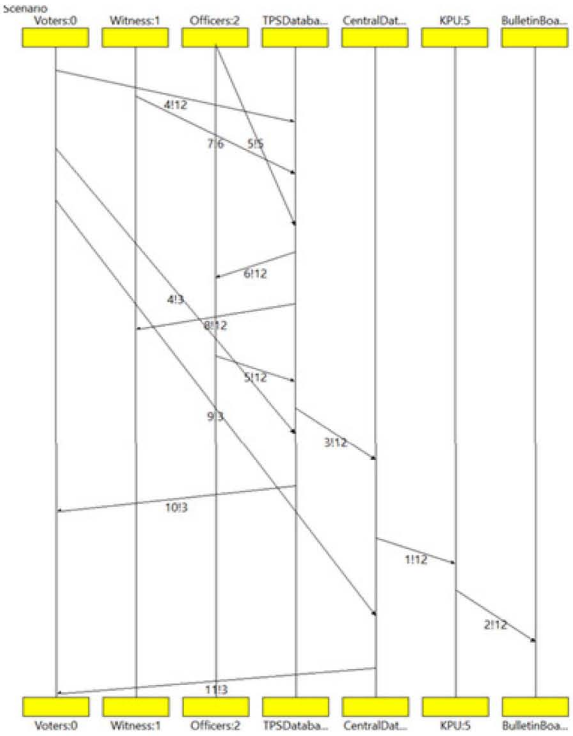

Fig.9. Simulation of the vote counting protocol in the e-voting system

The ideal condition expected from the e-voting protocol is to maintain the integrity of ballot data from Voters, which is when the results of counting are performed in the TPS Database, then upload the ballot results in the form of ballot blocks which the Officers vote = 12 until announced on BulletinBoard. Voters can verify their choice = 3 to the TPS database or to the Central Database, not having a fixed change = 3. Officers and TPS Database = 12, no change = 12. KPU can verify the vote = 12, still not change = 12. The test done is to test the property integrity with assert.

5. E-Voting Protocol with Attack Scenarios

One example of an e-voting protocol simulation that is carried out for a scenario is to change the voice in the database by changing the value in the voice column.

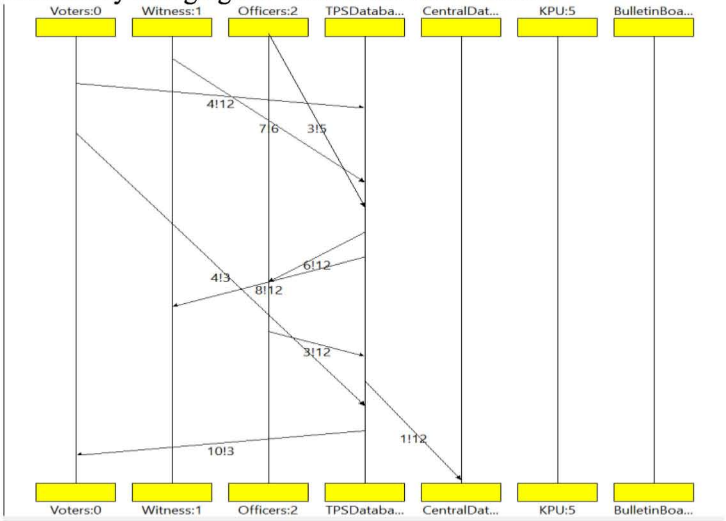

Fig. 10. Simulation of the e-Voting Protocol carried out in the scenario of changing the ballot in the database by changing the value in the voice column

In the simulation carried out an attack on the Database Center, where previously the result of the vote was = 12, then someone attacked the Central Database by changing several ballots so that the ballot results in the Database were worth 20. Because there was a verification protocol by the KPU to the Central Database, then the next phase could not continue, KPU must show verified status first to block ballot in the Central database, so that later the next can be continued.

V. RESULTS AND ANALYSIS OF THE e-VOTING PROTOCOL VERIFICATION

Based on the simulation results verification of the e-Voting Protocol model with the results and analysis is as follows:

1. Voter Registration Protocol

The verification results from the Voters registration protocol simulation on the e-voting system for ideal conditions are as follows, where there is no error for **assertion violations:**

```
Verification result:

 (Spin Version 6.4.8 -- 2 March 2018)
        + Partial Order Reduction

Full statespace search for:
        never claim            - (not selected)
        assertion violations   +
        cycle checks           -   (disabled   by   -
DSAFETY)
        invalid end states     -   (disabled   by   -E
flag)

State-vector 112 byte, depth reached 34, errors: 0
       43 states, stored
        8 states, matched
       51 transitions (= stored+matched)
        0 atomic steps
hash conflicts:         0 (resolved)
```

2. Voter's Authentication Protocol

The verification results from the Voters registration protocol simulation on the e-voting system for ideal conditions are as follows, where there is no error for **assertion violations:**

```
Verification result:

 (Spin Version 6.4.8 -- 2 March 2018)
        + Partial Order Reduction

Full statespace search for:
        never claim            - (not selected)
        assertion violations   +
        cycle checks           -   (disabled   by   -
DSAFETY)
        invalid end states     -   (disabled   by   -E
flag)

State-vector 132 byte, depth reached 34, errors: 0
       95 states, stored
       48 states, matched
      143 transitions (= stored+matched)
        0 atomic steps
hash conflicts:         0 (resolved)
```

3. Voting Protocol

The verification results from the voting protocol simulation on the e-voting system for ideal conditions are as follows, where there is no error for **assertion violations:**

```
Verification result:

 (Spin Version 6.4.8 -- 2 March 2018)
        + Partial Order Reduction

Full statespace search for:
        never claim            - (not selected)
        assertion violations   +
        cycle checks           -   (disabled   by   -
DSAFETY)
        invalid end states     -   (disabled   by   -E
flag)

State-vector 84 byte, depth reached 45, errors: 0
       58 states, stored
       10 states, matched
       68 transitions (= stored+matched)
        0 atomic steps
hash conflicts:         0 (resolved)
```

4. Vote Counting Protocol

The verification results from the voting protocol simulation on the e-voting system for ideal conditions are as follows, where there is no error for **assertion violations:**

```
Verification result:

 (Spin Version 6.4.8 -- 2 March 2018)
        + Partial Order Reduction

Full statespace search for:
        never claim            - (not selected)
        assertion violations   +
        cycle checks           -   (disabled   by   -
DSAFETY)
        invalid end states     -   (disabled   by   -E
flag)

State-vector 200 byte, depth reached 57, errors: 0
     1967 states, stored
     3309 states, matched
     5276 transitions (= stored+matched)
        0 atomic steps
hash conflicts:        23 (resolved)
```

5. E-Voting Protocol with Attack Scenarios

The verification results from the e-voting protocol simulation for the scenario scenario change the voice in the database by changing the value in the voice column, where there is an error if there is a ballot change due to verification of the ballot block by KPU:

```
Verification result:
pan:1:             assertion             violated
(UploadBlockBallotCentral==UploadBlockBallotTPS)
(at depth 24)
pan: wrote attacking.pml.trail

 (Spin Version 6.4.8 -- 2 March 2018)
Warning: Search not completed
        + Partial Order Reduction

Full statespace search for:
        never claim            - (not selected)
        assertion violations   +
        cycle checks           -   (disabled   by   -
DSAFETY)
        invalid end states     -   (disabled   by   -E
flag)

State-vector 200 byte, depth reached 24, errors: 1
       25 states, stored
        0 states, matched
       25 transitions (= stored+matched)
        0 atomic steps
hash conflicts:         0 (resolved)
```

VI. Conclusion

The most dominant parameters in the system of e-voting is verifiability, so that it becomes one of the parties determining the quality level of the e-voting system. Several related studies have conducted verifiability for several parties involved such as Voters, Officers and Witnesses, but not thoroughly for the e-voting system phase during elections, after elections and after vote count. This causes a decrease in the level of public confidence in the system of e-voting quality. The KPU as the highest electoral institution involved as one of the parties to voting, in other studies did not conduct verification. So Verifiability is where ballot verification is carried out by several parties, namely by Voters called Individual Verifiability and by Officers, Witnesses and KPU called Universal Verifiability that the votes chosen by the Voters do not change and the ballots has in the vote count and verification, from before, during, after the election, and after the vote count is referred to as Verifiability of End-to-End.

This research has been produced a Protocol (P) that can improve verifiability (V_f) on e-voting, with the concept of Protocol (P):

1. By involving the Voter Party (V), Officer (O), Witness (W) and KPU (C)
2. Verifiability involving the Voter Party (V) is called Individual Verifiability (IV)
3. Verifiability involving the Officer (O), Witness (W) and KPU (C) is called Universal verifiability (UV)
4. Verifiability is done in Phase before selection (bv), during selection (ov), after selection (av), and after vote counting (ac) which is called End-to-End Verifiability ($e2e$)
5. Individual Verifiability Integration (IV), Universal verifiability (UV) and End-to-End Verifiability ($e2e$)

References

[1] M. Bellis. (2015, Desember) The History of Voting Machines - History of the Voting. [Online]. http://inventors.about.com/library/weekly/aa111300b.htm

[2] T. M. Buchsbaum, *E-voting: International developments and lessons learnt," in Electronic Voting in Europe - Technology, Law, Politics and Society*. Lake of Constance: Schloß Hofen / Bregenz, 2004.

[3] VoteHere Inc, *Network Voting Systems Standards*.: Public Draft 2, April 2002.

[4] D Cetinkaya and O Cetinkaya, "Verification and Validation Issues in Electronic Voting," *The Electronic Journal of e-Government*, vol. 5 (2), pp. 117 - 126, 2007.

[5] A Riera and P Brown , "Bringing Confidence to Electronic Voting," *Electronic Journal of e-Government*, vol. 1 (1), pp. 14-21, 2003.

[6] B de Vuyst and A Fairchild, "Experimenting with Electronic Voting Registration: the Case of Belgium," *The Electronic Journal of e-Government*, vol. 2 (2), pp. 87-90, 2005.

[7] L. Cranor and R. Cytron, "Sensus: A securityconscious electronic polling system for the Internet," in *Hawaii International Conference on System Sciences*, 1997.

[8] D. Chaum, Peter Y. A. Ryan, and Steve A. Schneider, "A Practical, Voter verifiable Election Scheme," School of Computing Science, University of Newcastle, Technical Report Series CS-TR-880 2004.

[9] M. J. Moayed, A. A. A. Ghani, and R. Mahmod, "A Survey on Cryptography Algorithms in Security of Voting System Approaches," in *International Conference on Computational Sciences and Its Applications, 2008. ICCSA '08*, 2008, pp. 190–200.

[10] Mohamed Aymen Chalouf, Francine Krief, Nader Nader Mbarek, and Tayeb Lemlouma, "Improvement of a Service Level Negotiation Protocol using Formal Verification," in *IEEE Symposium on Computers and Communications (ISCC)*, 2013.

[11] Sandra Guasch Castell´o, , "Individual Verifiability in Electronic Voting," Universitat Polit`ecnica de Catalunya, 2016.

[12] Rebecca Mercuri, "Electronic Vote Tabulation Checks & Balances," University of Pennsylvania, 2001.

[13] D. Chaum, Peter Y. A. Ryan, and Steve A. Schneider, "A Practical, Voter verifiable Election Scheme," School of Computing Science, University of Newcastle, Technical Report Series CS-TR-880, 2004.

[14] Ali Fawzi Najm Al-Shammari, Adolfo Villafiorita, and Komminist Weldemariam, "Understanding the Development Trends of Electronic Voting Systems," University of Bolzano, Bolzano, Italy, 2012.

[15] Gerard J. Holzmann, *DESIGN AND VALIDATION OF COMPUTER PROTOCOLS*. Englewood Cliffs, New Jersey: PRENTICE-HALL, 1991.

[16] Rinaldi Munir, *Kriptografi*. Bandung: Informatika, 2006.

[17] M. Rouse. (2007) searchnetworking. [Online]. http://searchnetworking.techtarget.com/definition/protocol

[18] Veronique Cortier, David Galindo, Ralf Kusters, Johannes Muller, and Tomasz Truderung, "Verifiability Notions for E-Voting Protocols," LORIA/CNRS, 2016.