End-to-End Verifiability Degree Metric in e-Voting System

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

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

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

2021 15th International Conference on Telecommunication Systems, Services, and Applications (TSSA) | 978-1-6654-2892-7/21/$31.00 ©2021 IEEE | DOI: 10.1109/TSSA52866.2021.9768251

Abstract— **The verifiability provide protection for the votes cast and for the voters themselves in e-voting. The notion of verifiability includes Verifiability of Individual, Universal and End-to-End. End-to-End Verifiability (EV) is a type that allows voters to be able to verify after the voting process, even though the voting process has not yet been closed. Some research on End-to-End Verifiability is more for the selectors only and does not see for some e-voting phases and has not proposed any metrics. In this research, it has been proposed an End-to-End Verifiability Metric to measure the degree of End-to-End verifiability consisting of End-to-End Verifiability Metrics Before Election, End-to-End Verifiability Metrics When Election, End-to-End Verifiability Metrics After Election, End-to-End Verifiability Metrics After Vote Counting and to determine the position of degree of verifiability, followed by the degree range of verifiability.**

Keywords—: e-voting system, end-to-end verifiability, End-to-End Verifiability Degree Metric.

I. Introduction

The verifiability provide protection for the votes cast and for the voters themselves in e-voting. The notion of verifiability includes Individual Verifiability, Universal Verifiability and End-to-End Verifiability. Individual Verifiability (IV) is a type that allows each voter to be able to ensure that the ballots that are included, are actually counted in the final tabulation. Universal Verifiability (UV) is a verification model that allows election officials to be able to match the results of a calculated vote with existing ballots. End-to-End Verifiability (EV) is a type that allows voters to be able to verify after the voting process, even though the voting process has not yet been closed.

Some research on End-to-End verifiability is more for the voters only and not for some e-voting phases. [1] [2]. In this study, the idea of End-to-End Verifiability accommodates for the Voters, Witness Officers and KPU in the phase before the election, during the election, after the election and after the vote count. Then, several studies relating to End-to-End verifiability have not proposed metrics. In this research, the End-to-End Verifiability Metric has been proposed to measure the degree of End-to-End Verifiability which consists of the End-to-End Verifiability Metrics Before Election, End-to-End Verifiability Metrics on Election, End-to-End Metrics Verifiability After Selection, End-to-End Verifiability Metrics After Vote Counting and to determine the position of the degree of verifiability, followed by the range of degree of verifiability.

II. Literature Review

Based on research [1], the P_{KZZ} protocol with Set agent Σ consists of voters, *bulletin board B*, *EA* voting authority, Judge J, *teller* $T_1, \ldots, T_m$ and the remaining participants. When the V run program honest π_V program in the casting phase, he expects Option c, a credential and general election parameters. Then, he run Cast in interaction with B, and expects a receipt α (if he does not receive a receipt, he stops). When the voter is triggered by Judge in the verification phase, the voter reads the election transcript τ from bulletin board B (if he does not receive τ, the 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.

In [2] defines Verifiability of End-to-End with the aim of γ_{E2E} to be a set of all runs of the P_{CEKMW} protocol as a result of r from fulfilling the selection $r = \rho(rlist)$ for some rlist containing (as multiset) all c_i choices for some honest voters (honest) V_i which achieved $Happy(i, c_i, crediB)$. End-to-end verifiability is characterized by the fact that the P_{CEKMW} protocol is (γ_{2E2}, 0) verifiable by judge J.

Research [2] and [1] have defined the idea of End-to-End Verifiability, yet the metric has not produced a metric. To measure the degree of End-to-End Verifiability requires the End-to-End Verifiability Metric.

III. Proposed End-to-End Verifiability Metric

We propose end-to-end verifiability metrics with this degree of Verifiabiity in this section,.

A. Proposed End-to-End Verifiability Metric

According to [3] the value that facilitates decision making and is derived from measurement is the definition of metrics.. Metrics are results, and measurement is activity [4].

To produce end-to-end metrics, the steps are as follows.

1. Define verifiability requirements

End-to-end verifiability requirements are defined from the requirements of functional and non-functional of the evoting system described in the journal [5], with the following results.

TABLE I. End-to-end Verifiability Requirements based on Functional requirements of e-Voting systems

FS Code	Verifiability Requirements
FS2,FS3	KV1: Voters can verify that they have not already voted (before voting)
	KV2: Voting Officers can verify that they have not already voted (before voting)
	KV3: Witness can verify that they have not already voted (before voting)
FS6	KV4: Voters can verify that their vote has been not changed and has entered the vote count (after voting)
	KV5: Voters can verify that their vote has not been changed and entered the vote count (after vote counting)
FS14	KV6: Voting Officers can verify that their vote has been not changed and has entered the vote count (after voting)
	KV7: Witness can verify that their vote has been not changed and has entered the vote count (after voting)
	KV8: KPU can verify that their vote has been not changed and has entered the vote count (after voting)
	KV9: Voting Officers can verify that their vote has not been changed and entered the vote count (after vote counting)
	KV10: Witness can verify that their vote has not been changed and entered the vote count (after vote counting)
	KV11: KPU Officers can verify that their vote has not been changed and entered the vote count (after vote counting)

TABLE II. The requirements of the Non-Functional e-Voting system for End-to-end Verifiability Requirements

NF Code	Verifiability Requirements
NF2	KV12: Voters can make sure that their votes do not change during the voting process

2. Make the need for end-to-end verifiability for before, during, after the election and after the vote count phase.

3. Create End-to-End Verifiability Metrics Before Election, End-to-End Verifiability Metrics When Election, End-to-End Verifiability Metrics After Election, End-to-End Verifiability Metrics After Vote Counting.

For stages 2 and 3 are explained in the following sections:

End-to-End Verifiability requirements consist of:

1. End-to-End Verifiability Before Election

Based on the Verifiability requirements table, the End-to-End Verifiability requirements table is obtained before the selection as follows.

TABLE III. End-to-End Verifiability Requirements before selection

KV Code	End-to-End Verifiability Requirements
KV2	BV1: Voting Officers can verify that they have not already voted (before voting)
KV3	BV2: Witness can verify that they have not already voted (before voting)
KV1	BV3: Voters can verify that they have not already voted (before voting)

Based on the End-to-End Verifiability requirements table before the selection, the dependency between End-to-End Verifiability requirements to be drawn is shown in the following figure. Based on the End-to-End Verifiability requirements table before the selection, the dependency between End-to-End Verifiability requirements to be drawn is shown in the following figure.

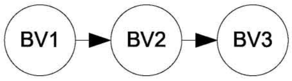

Fig. 1. Dependency between End-to-End Verifiability requirements before selection

Based on Figure 1 above, because there is a dependency between requirements, if the previous requirements are not met, then the next requirements cannot be fulfilled as well. For example, if BV1 is not fulfilled, BV2 and BV3 are also not met. For more details, it can be seen in the Flowchart and pseudocode of the algorithm for dependency on End-to-End Verifiability requirements before the selection.

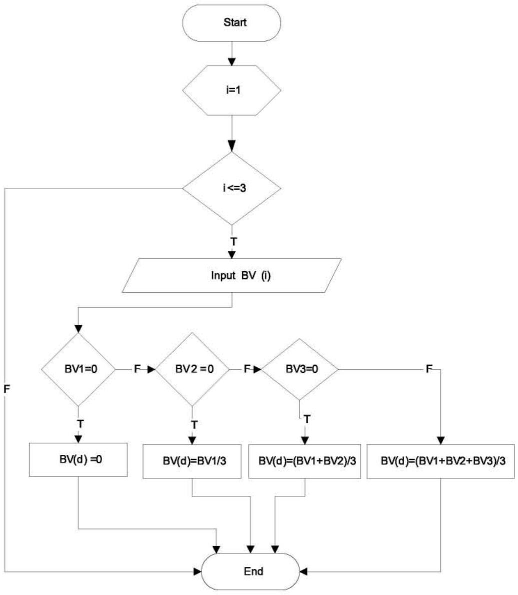

Fig. 2. Flowchart dependency algorithm between End-to-End Verifiability requirements before selection

Based on figures 2 about the requirements for End-to-End Verifiability before the selection, there are 3 steps that must be passed to achieve the degree of End-to-End Verifiability before the selection of 1. Value 1 is the highest value of the degree End-to-End -End Verifiabilityi before the election. The provisions of calculating the degree of End-to-End Verifiability before selection based on the dependency between End-to-End Verifiability requirements are:

1. If BV1 is fulfilled, then the degree of End-to-End Verifiability before selection = 1/3.
2. If BV1 and BV2 are met, then the degree of End-to-End Verifiability before selection = 2/3.
3. If BV1, BV2 and BV3 are fulfilled, the degree of End-to-End Verifiability before selection = 1.
4. Because there is a dependency between stages, if the previous stage is not met, then the next stage cannot be counted. For example, if BV1 is not fulfilled, BV2 and

BV3 are not counted, then the degree of End-to-End Verifiability before selection = 0.

Based on the above conditions, the proposed metric to measure the degree of End-to-End Verifiability before the election in the e-voting system is as follows.

$$bv_i = f(p_i) = \begin{cases} 1, verifiable \\ 0, not\ verifiable \end{cases} \quad (1)$$

when,

$bv = Value\ end\ to\ end\ verifiability\ requirements\ before\ selection$

$i = end\ to\ end\ verifiability\ requirements\ before\ election\ to$

$p_i = the\ requirements\ for\ verifiability\ of\ the\ voting\ protocol$

The End-to-End Verifiability stage before selection (bv) is determined with a value of: 0 means that verification is not carried out (cannot be verified), while a value of 1 means verification (can be verified).

$$BV_d = \frac{\sum_{i=1}^{n} b_i}{n} \quad (2)$$

when,

$BV_d = The\ degree\ of\ end\ to\ end\ verifiability\ before\ selection$

$n = Number\ of\ end - to - end\ verifiability\ requirements\ before\ selection$

$$b_i = \begin{cases} bv_i, \text{if } \forall j \in \{1..i-1\},\ bv_j \neq 0\ OR\ i = 1 \\ 0, \text{if } \exists j \in \{1..i-1\},\ bv_j = 0 \end{cases}$$

The range of the degree of End-to-End Verifiability before the selection is 0 to 1. The higher the value of the degree of End-to-End Verifiability before the selection approaches 1, then the degree of End-to-End Verifiability before the selection is increasingly fulfilled.

2. End-to-End Verifiability During Election

Based on the Verifiability Requirement table, the End-to-End Verifiability Requirement table is obtained during the selection as follows.

Table IV. End-to-End Verifiability Requirements during selection

KV Code	End-to-End Verifiability Requirements
KV12	OV1: Voters can make sure that their votes do not change during the voting process

Based on the End-to-End Verifiability requirements table at the time of selection, OV1 requirements are not met (1) or fulfilled (0).

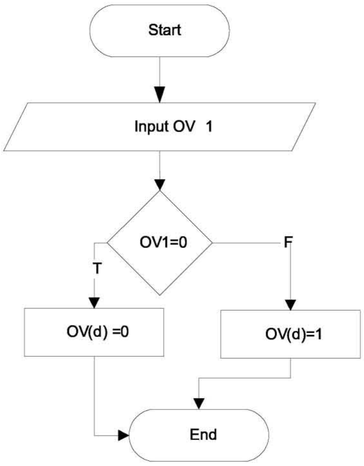

Fig. 3 Flowchart dependency algorithm between the need for End-to-End Verifiability at the time of selection

Based on the End-to-End Verifiability requirements table during the selection, the proposed metric to measure the degree of End-to-End Verifiability when voting in the e-voting system is as follows.

$$ov = f(p_i) = \begin{cases} 1, verifiable \\ 0, not\ verifiable \end{cases} \quad (3)$$

when,

$ov = Value\ of\ end\ to\ end\ verifiability\ requirements\ at\ the\ time\ of\ selection$

$p_i = the\ requirements\ for\ verifiability\ of\ the\ voting\ protocol$

The End-to-End Verifiability stage when selecting (OV_d) is determined with a value: 0 means that verification is not carried out (cannot be verified), while a value of 1 means verification (can be verified).

$$OV_d = ov \quad (4)$$

when,

$OV_d = The\ degree\ of\ end\ to\ end\ verifiability\ at\ the\ time\ of\ selection$

3. End-to-End Verifiability After Selection

Based on the Verifiability requirements table, the End-to-End Verifiability requirements table is obtained after the selection as follows.

Table V. End-to-End Verifiability Requirements after selection

KV Code	End-to-End Verifiability Requirements
KV4	AV1: Voters can verify that their vote has been not changed and has entered the vote count (after voting)
KV6	AV2: Voting Officers can verify that their vote has been not changed and has entered the vote count (after voting)
KV7	AV3: Witness can verify that their vote has been not changed and has entered the vote count (after voting)
KV8	AV4: KPU can verify that their vote has been not changed and has entered the vote count (after voting)

Based on the End-to-End Verifiability requirements table after the selection, the dependency between End-to-End Verifiability requirements to be drawn is shown in the following figure.

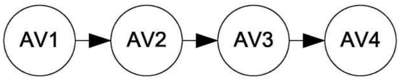

Fig. 6. Dependency between End-to-End Verifiability requirements after selection

Based on Figure 6 above, because there is a dependency between requirements, if the previous requirements are not met, then the next requirements cannot be fulfilled as well. For example if AV1 is not met, then AV2, AV3 and AV4 are not met as well. For more details, it can be seen in the Flowchart and pseudocode of the algorithm for dependency on End-to-End Verifiability requirements after the selection.

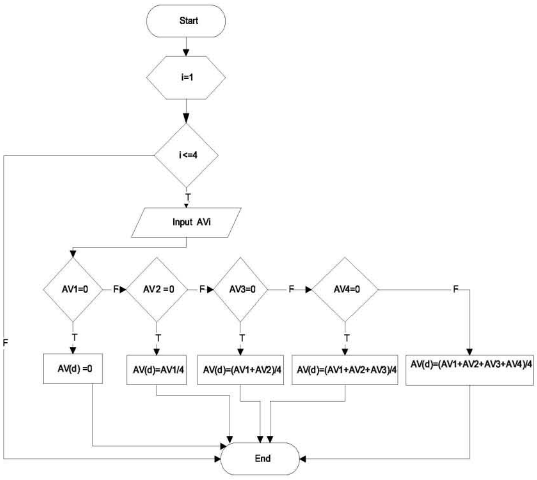

Fig. 4. Flowchart dependency algorithm between End-to-End Verifiability requirements after selection

Based on figure 4 about the need for End-to-End Verifiability after the selection, there are 3 steps that must be passed to reach the degree of End-to-End Verifiability after the selection of 1. Value 1 is the highest value of the degree End-to-End -End Verifiabilityi after the election. The provisions of calculating End-to-End Verifiability degrees after selection based on dependencies between End-to-End Verifiability requirements are:

1. If AV1 is met, the degree of End-to-End Verifiability after selection = 1/4.
2. If AV1 and AV2 are met, then the degree of End-to-End Verifiability after selection = 2/4.
3. If AV1, AV2 and AV3 are met, then the degree of End-to-End Verifiability after selection = 3/4.
4. If AV1, AV2, AV3, and AV4 are met, the End-to-End Verifiability degree after selection = 1.
5. Because there is a dependency between stages, if the previous stage is not met, then the next stage cannot be counted. For example, if AV1 is not met, then AV2, and AV3 are not taken into account, then the degree of End-to-End Verifiability after selection = 0.

Based on the above conditions, the proposed metric to measure the degree of End-to-End Verifiability after the election in the e-voting system is as follows.

$$av_i = f(p_i) = \begin{cases} 1, verifiable \\ 0, not\ verifiable \end{cases} \quad (5)$$

when,

$av = Value\ requirements\ end\ to\ end\ verifiability\ after\ selection$

$i = end\ to\ end\ verifiability\ requirements\ after\ election\ to$

$p_i = the\ requirementsfor\ verifiability\ of\ the\ voting\ protocol$

The End-to-End Verifiability stage after selection (av) is determined with a value of: 0 means that verification is not performed (cannot be verified), while a value of 1 means verification (can be verified).

$$AV_d = \frac{\sum_{i=1}^{n} a_i}{n} \quad (6)$$

when,

$AV_d = The\ degree\ of\ end\ to\ end\ verifiability\ after\ selection$

n
$= Number\ of\ end - to$
$- end\ verifiability\ requirements\ after\ selection$

$$a_i = \begin{cases} av_i, \text{if } \forall j \in \{1..i-1\},\ av_j \neq 0 \ \ OR\ \ i = 1 \\ \quad 0, \text{if } \exists j \in \{1..i-1\},\ av_j = 0 \end{cases}$$

The range of the degree of End-to-End Verifiability after the selection is 0 to 1. The higher the value of the degree of End-to-End Verifiability after the selection approaches 1, then the degree of End-to-End Verifiability after the selection is increasingly fulfilled.

4. End-to-End Verifiability Degree After Vote Counting

Based on the Verifiability requirements table, the End-to-End Verifiability requirements table is obtained after the selection as follows.

Table VI. End-to-End Verifiability Requirements after flare calculation

KV Code	End-to-End Verifiability Requirements
KV11	AC1: KPU Officers can verify that their vote has not been changed and entered the vote count (after vote counting)
KV5	AC2: Voters can verify that their vote has not been changed and entered the vote count (after vote counting)
KV10	AC3: Witness can verify that their vote has not been changed and entered the vote count (after vote counting)
KV9	AC4: Voting Officers can verify that their vote has not been changed and entered the vote count (after vote counting)

Based on the End-to-End Verifiability requirements table after vote counting, the dependency between End-to-End Verifiability requirements to be drawn is shown in the following figure.

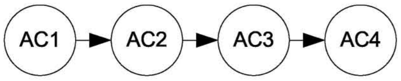

Fig. 5. Dependency between End-to-End Verifiability requirements after vote counting

Based on Figure 6 above, because there is a dependency between requirements, if the previous requirements are not met, then the next requirements cannot be fulfilled as well. For example if AC1 is not met, then AC2, AC3 and AC4 are not met as well. For more details, it can be seen in the Flowchart and pseudocode of the algorithm for the dependency of End-to-End Verifiability requirements after vote counting.

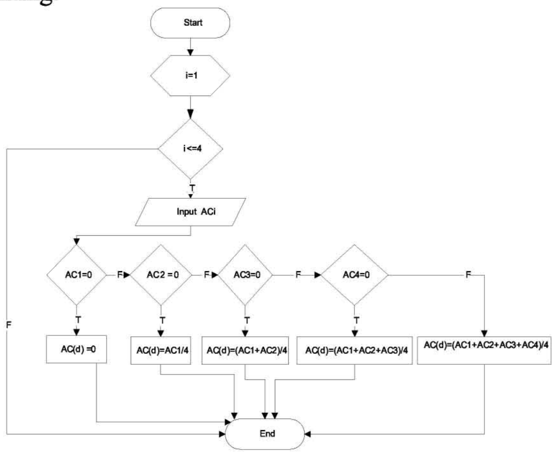

Fig. 6. Flowchart dependency algorithm between the need for End-to-End Verifiability after vote counting

Based on figure 6 about the need for End-to-End Verifiability after vote counting, there are 8 steps that must be passed to achieve the degree of End-to-End Verifiability after vote counting of 1. Nlai 1 is the highest value of the End degree - to-End Verifiability after vote counting. Provisions for the calculation of the degree of End-to-End Verifiability of vote counting based on the dependency between the requirements of End-to-End Verifiability are:

1. If AC1 is met, the degree of End-to-End Verifiability after vote counting = 1/4.
2. If AC1 and AC2 are met, then the degree of End-to-End Verifiability after vote counting = 2/4.
3. If AC1, AC2 and AC3 are met, then the degree of End-to-End Verifiability after vote counting = 3/4.
4. If AC1, AC2, AC3 and AC4 are met, then the degree of End-to-End Verifiability after vote counting = 1.
5. Because there is a dependency between stages, if the previous stage is not met, then the next stage cannot be counted. For example if AC1 is not met, then AC2 up to AC8 are not counted, then the degree of End-to-End Verifiability after vote count = 0.

Based on the above conditions, the proposed metric to measure the degree of End-to-End Verifiability after vote counting in the e-voting system is as follows.

$$ac_i = f(p_i) = \begin{cases} 1, verifiable \\ 0, not\ verifiable \end{cases} \qquad (7)$$

when,

ac

$= Value\ of\ end\ to\ end\ verifiability\ requirements\ after\ vote\ counting$

$i = end\ to\ end\ verifiabilityrequirementsafter\ vote\ counting\ to$

$p_i = the\ requirements\ for\ verifiability\ of\ the\ voting\ protocol$

The End-to-End Verifiability stage after vote counting (ac) is determined with a value of: 0 means that verification is not done (cannot be verified), while a value of 1 means verification (can be verified).

$$AC_d = \frac{\sum_{i=1}^{n} c_i}{n} \qquad (8)$$

when,

$AC_d = The\ degree\ of\ end\ to\ end\ verifiability\ after\ vote\ counting$

n

$= Number\ of\ end - to$

$- end\ verifiability\ requirements\ after\ vote\ counting$

$$c_i = \begin{cases} ac_i, \text{if } \forall j \in \{1..i-1\}, ac_j \neq 0\ \ OR\ \ i = 1 \\ 0, \text{if } \exists j \in \{1..i-1\},\ ac_j = 0 \end{cases}$$

The range of the degree of End-to-End Verifiability after vote counting is 0 to 1. The higher the value of the degree of End-to-End Verifiability after vote counting approaches 1, then the degree of End-to-End Verifiability after vote counting is more fulfilled.

5. Create End-to-End Verifiability Degree Metrics

After knowing the results of the calculation of the metric degree of end-to-end verifiability before the selection (BV_d), during the selection (OV_d), after the selection (AV_d) and after the calculation voice (AC_d), the following end-to-end verifiability metrics are obtained.

$$EV_d = \frac{BV_d + OV_d + AV_d + AC_d}{4} \qquad (9)$$

when,

EV_d = *degree of end to end verifiability*

BV_d = *degree of end to end verifiability before election*

OV_d = *degree of end to end verifiability at the time of election*

AV_d = *degree of end to end verifiability after election*

AC_d = *degree of end to end verifiability after vote counting*

B. *Proposed Range of Values of Verifiability*

The range of the degree of verifiability is 0 to 1. The more the value of the degree of verifiability is close to 1, then the verifiability is increasingly absolute verified. The following figure shows the range of degrees of verifiability.

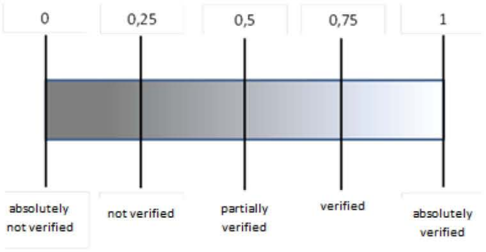

Fig. 12. Range of Values of Verifiability Degree

For example if the result of calculating the degree of verifiability is 0.81, then the Protocol is near absolute verified.

IV. Results and Analysis

To see examples of calculations from the End-to-End Verifiability Metrics applied to the Traditional Voting Protocol in Indonesia that has been described in the journals [5], Kiayias et al [1] and Cortier et al [2]. End-to-end verifiability requirements that are met are given a value of 1, whereas if not met are given a value of 0.

Table VII. Protocol Requirement Data

Protocol	bv			ov	av				ac			
	V	O	W	V	V	O	W	C	V	O	W	C
Traditional Voting Protocol in Indonesia [5]	0	1	1	0	0	0	0	0	0	0	0	0
Cortier et. al. Protocol [2]	1	0	0	1	1	1	0	0	0	0	0	0
Kiayias et. al. Protocol [1]	1	0	0	1	1	0	0	0	0	0	0	0

bv= before election ov= at the time of election
av= after election ac= after vote counting
V = Voters W= Witness
O = Voting Officer C= KPU
1= Verification 0= not verification

Then calculate the degree of End-to-End Verifiability and determine the range of degrees of verifiability with the following results.

Table VIII. End-to-end Verifiability Calculation Results

Protocol	bv_d	ov_d	av_d	ac_d	*EVd*	Range of Values of Verifiability Degree
Traditional Voting Protocol in Indonesia [5]	0.67	0.00	0.00	0.00	0,17	not verified
Cortier et. al. Protocol [2]	0.00	1.00	0.50	0.00	0,38	Approaching partially verified
Kiayias et. al. Protocol [1]	0.00	1.00	0.25	0.00	0,31	Approaching partially verified

Based on the table above, the results of the degree of Verifiability measurement are obtained as in the following chart.

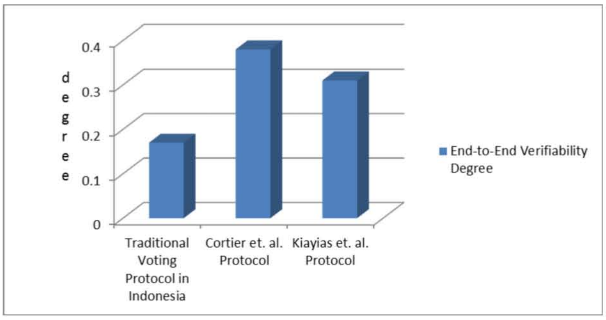

Fig. 13. Graph of the result of calculating the degree of end-to-end verifiability

V. Conclusion

An end-to-end Verifiability Degree Metric for e-voting systems was proposed in this research. The degree of end-to-end was measured for Traditional Voting Protocol, Cortier et. al. Protocol and Kiayias et. al. Protocol. After calculating the level of verifiability of each of these protocols, taking into account the level of end-to-end verifiability, one can choose which protocol to implement.

References

[1] A. Kiayias, T. Zacharias, and B. Zhang, "End-to-End Verifiable Elections in the Standard Model," in Advances in Cryptology - EUROCRYPT 2015, 2015, pp. 468–498.

[2] V. Cortier, D. Galindo, R. Kusters, J. Muller, and T. Truderung, "Verifiability Notions for E-Voting Protocols," LORIA/CNRS, 2016.

[3] Nwokedi C. Idika, Characterizing and Aggregating Attack Graph-Based Security Metrics.. PhD Dissertation. Purdue University. West Lafayette. Indiana, 2010.

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

[5] T.N. Suharsono, Kuspriyanto, and B. Rahardjo, "Individual Verifiability Metric in e-Voting System," International Journal on Electrical Engineering and Informatics, vol. 11, no. 1, pp. 101-111, 2019.