# Individual Verifiability Metric in e-Voting System

Teguh Nurhadi Suharsono, Kuspriyanto, and Budi Rahardjo

[1]School of Electrical Engineering and Informatics
Institut Teknologi Bandung, Indonesia

*Abstract:* The voting process is an essential part of the democratic system. As the size and breadth of voter distribution grow, the social aspects become more complex and the need to manage the voting process more efficiently and more quickly increases. This makes electronic voting (e-voting) a more interesting alternative voting technology. The voting confidence level highly depends on the ability of the system to protect the votes until the end of the process. Parameters in e-voting consist of accuracy, invulnerability, privacy, and verifiability, where verifiability is currently the most important factor in attempts to further improve the quality of e-voting technology. The availability of verifiability properties gives the voters confidence that the voting system used provides protection, both to the votes cast and to the identity of the voters themselves. Individual verifiability refers to the verifiability properties of the voting system that should be able to accommodate the needs of the voters. In this paper, an e-voting system that accommodates the individual verifiability requirements and a method for measuring the degree of individual verifiability are proposed.

Keywords: e-voting, e-voting paramater, verifiability, individual verifiability metrics

## 1. Introduction

Voting is an important part of the democratic system, enabling people to make choices regarding policies, to elect representatives who will sit in representative assemblies and to elect leaders. Paper voting cards were first introduced in Victoria, Australia in 1856 and began to be used in America (New York) in 1889. Since then, technology to support election processes has continued to developed. Mechanical machines were developed, for example the Myers Automatic Booth voting machine, which used levers and was first introduced in Lockport, New York in 1892. Punch cards were first introduced in Fulton and De Kalb in Georgia in 1964. In the following years, electronic-based machines were developed, including Marksense (using an optical scan technique), which was first introduced in the American presidential elections in 1996, and a variety of direct recording electronic (DRE) devices [*1*].

The growing number of voters and the extent of their distribution, the increasing complexity of social life, and the need to manage the voting process more efficiently and determine the results more quickly make e-voting a promising alternative technology. In addition to the type of e-voting that still requires the physical presence of voters at 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 (e.g. Polling Station Remote Voting, where voting can be done via telephone, SMS, internet, digital TV, etc.) [*2*]. E-voting is an election system where data are recorded, stored and processed in the form of digital information [*3*]. Centinkaya and Centinkaya define e-voting as a computerized voting process that uses digital ballots [*4*]. E-voting is essentially the implementation of voting that is conducted electronically (digitally), from registering the voters, carrying out the election and counting the votes to distributing the result.

The application of e-voting is expected to overcome problems that arise from conventionally held elections [*5*] [*6*] by:

1. Speeding up vote counting.
2. Achieving more accurate vote counting results.
3. Saving costs related to paper ballots.
4. Saving costs related to transporting paper ballots.

Received: October 15th, 2018. Accepted: March 24th, 2019
DOI: 10.15676/ijeei.2019.11.1.6

5. Being able to make ballots in various language versions.
6. Providing more access to information regarding voting choices.
7. Rejecting those who are not entitled to vote, for example, because they are underage or exceed the maximum age of voters that has been set.

To ensure vote security, implementation of the voting process is divided into four main activities [*7*]:

1. Registration, i.e. the process of registering each voter in accordance with applicable regulations.
2. Validation, i.e. the process of validating voter data to reject voters who do not meet the criteria and to avoid duplication of data.
3. Collection, i.e. the process of collecting the votes.
4. Tallying, i.e. the process related to counting ballots.

According to [*7*], e-voting must fulfill the following requirements:

1. Accuracy: votes cannot be changed or eliminated, and only valid votes are counted.
2. Invulnerability: only those who have the right to vote can vote and can vote only once.
3. Privacy: each vote is confidential.
4. Verifiability: the votes and the vote count results can be re-verified.

Based on [*7*], the application of a new voting technology may not be well received by the wider community. This greatly depends on the level of public trust in the quality of the voting technology.

Verifiability is is currently the most important factor in attempts to further improve the quality of e-voting technology. The availability of verifiability properties gives the voters the confidence that the voting system used provides protection, both to the votes cast and to the identity of the voters themselves [*8*]. In e-voting systems, data security can be divided into two parts, namely: security related to the ballots (from the voting stage to the counting stage), and verification by voters to ensure that the content of their vote has not been changed and has been counted correctly [*9*].

In this paper, an e-voting system that accommodates the individual verifiability requirements and a method for measuring the degree of individual verifiability are proposed. The verifiability properties of this system should be able to accommodate the needs of voters. To measure the degree of verifiability a metric is needed. Several studies have produced metrics that can be used in e-voting systems. Reiter and Rubin have published measurement models using a spectrum of anonymity that ranges from 0 to 1 with several levels [*10*]. Berthold et al. have proposed notations for the level of anonymity using the size of the anonymity set [*11*]. Serjantov and Danezis state that the size of the anonymity set is influenced by the number of subjects connected to IOIs and the distribution of opportunities among the subjects (anonymity set) [*12*]. Mapping several ideas and previous studies [*13*] [*14*] [*15*] [*16*] [*17*] [*18*] [*19*] related to verifiability parameters does not explain how to measurer the degree of verifiability.

In the next section of this paper a literature review about metrics in e-voting systems is presented. In the third part, the verifiability metric is proposed. The following section contains the results and analysis of this study.

## 2. Literature Review

The definition of a metric according to [*20*] is a value that facilitates decision-making that is derived from measurement. According to [*21*] metrics are results while measurement is an activity. Measurement is the activity of carrying out observation and data collection in an effort to obtain a practical view of what is attempted to be understood. In [*22*] [*23*] the metric is mentioned as a consistent standard for measurement. Good metrics should be measured consistently, affordable, expressed in cardinal numbers or percentages, expressed in at least one

unit of measurement, and contextually specific (relevant to decision makers to base a decision on).

Some researchers have proposed metrics that can be used in e-voting systems, but verifiability metrics do not yet exist. Reference [*10*] proposes measurement models using a spectrum of anonymities ranging from 0 to 1 with several levels.

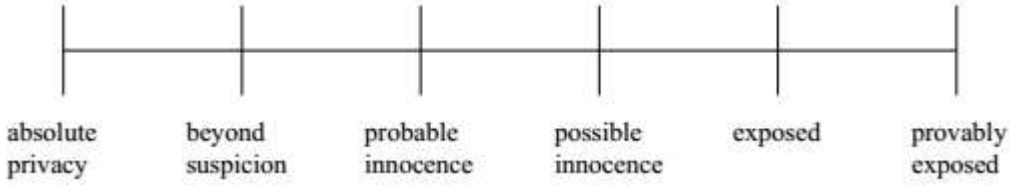


Figure 1. Degrees of anonymity [*10*]

The level of anonymity is defined as $1 - p$, where p is the probability of a particular user being targeted by an attacker. The notation applied for the degree of anonymity ($d$) is $d = 1 - p$. In this model the value of the level of anonymity is strongly influenced by the number of voters or messages. When in a system there are 2 (two) voters, then the anonymity level of the voters is ½ or 50%. If the number of voters reaches 1,000, the attack probability value of each user is 0.001 and the level of anonymity is 1 - 0.001 or 0.999.

Berthold et al. [*11*] use as notation for the level of anonymity, $A = log_2(N)$. The most basic way to measure anonymity is to use the anonymity set size. If message $(M_1)$ sent by subject $(S_1)$ in subject set $(S)$ with size N can be intercepted by an attacker at the recipient, then the size of the anonymity set $= 1/N$, where set size $N$ = 10 and $M$ messages are sent to $S_1$. Hence, the anonymity set size $= 1/10$.

The size of the anonymity set is influenced by two factors [*12*], namely the number of subjects connected with IOIs and the distribution of attack opportunities among the subjects (anonymity set).

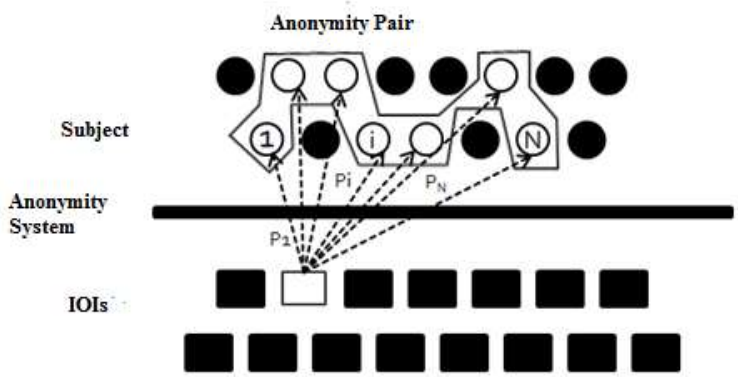


Figure 2. Anonymity set [*12*]

Serjantov and Danezis proposed the use of Shannon's information theory, especially entropy, to measure the level of anonymity. This theory provides a measure of the uncertainty of a random variable. Let $X$ be a random variable with a probability of mass function $pi = Pr(X_i)$, where $i$ represents each possible value with probability $pi > 0$. In this model each $i$ refers to a subject in the anonymity set, for example $pi$ is the probability of subject $i$ related to IOIs. $H(X)$ is the entropy of the random variable and $N$ (users) is the number of subjects in the anonymity set. $H(X)$ can be calculated by [*12*]:

$$H(X) = -\sum_{i=1}^{n} p_i \log_2(p_i) \quad (1)$$

The maximum entropy of the measured system is:

$$H_M = \log_2(N) \quad (2)$$

Thus, the value of the level of anonymity in this method can be expressed as the difference in entropy before and after an attack with $H_M - H(X)$, with normalization:
A scale from 0 (zero) to 1 (one) indicates the level of anonymity, where the level of anonymity
$(d) = 0$ when all users appear as senders of messages with probability one.
$(d) = 1$ when all users appear as senders of messages with the same probability of $1/N$.

According to [*12*] a standard measure of good anonymity (reference value) is when the level of anonymity is higher or equal to zero point eight ($d \geq 0.8$), which means it is difficult to find the partner's subject anonymity.

Mapping several ideas and previous studies [*13*] [*14*] [*15*] [*16*] [*17*] [*18*] [*19*] related to verifiability parameters does not explain how to measure the degree of verifiability. Castello [*14*], Kusters et al. [*15*], Cortier et al. [*17*] [*19*], Smith [*18*] developed the idea of individual verifiability, where the voters can make sure that their vote does not change. Smith [*18*], Cortier et al. [*17*] [*19*] developed the idea of universal verifiability, where some parties other than the voters make sure that the votes do not change. Kiayias et al. [*13*] [*16*] developed the idea of end-to-end verifiability, where voters can trace the results of their votes. In this paper, the Individual Veriafiabiliy Metric for measuring the degree of verifiability for voters is proposed.

## 3. Proposed Verifiability Metrics

According to [*14*], e-voting systems must provide a method for verifying that they work as expected. An auditor must be able to verify that all votes that enter the vote count are from eligible voters. Voters must be able to verify that the result of their vote is according to their choice and that it is counted correctly. Verifiability aims to ensure the correctness of each vote according to the choice made by the voter. Methods that can be used are: Voter Verification, the Voter Verifiable Voting System, or Voter Verified Paper Audit Trails (VVPAT) [*24*]. These methods aim to give confidence to the voters that the voting system used provides protection both to the votes and to the identity of the voters [*8*].

Vote verification is a way to ensure that the content of each ballot is in accordance with the choice of the voter. The ultimate goal of the system is that the voters must be able to easily convince themselves, without any special training, that the result of the election reflects the actual votes. Vote verification can be applied in different phases of the voting process with the aim of achieving different levels and scopes of verifiability [*25*]. If vote verification is carried out by voters, it is called individual verifiability.

To determine the individual verifiability requirements of the e-voting system, the proposed analysis stages are carried out as shown in Figure 2.

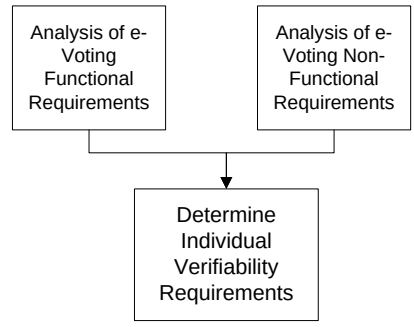


Figure 3. Stages of analysis related to the individual verifiability requirements of the proposed e-voting system

The stages of analysis related to the proposed individual verifiability requirements of the e-voting system in this study were:

1. Analysis of functional e-voting system requirements
   Analysis of the functional requirements of the e-voting system shown in Table 1 [*26*].

Table 1. Analysis of Functional Requirements of E-Voting System [*26*]

| FS Code | Functional (FS) Requirements of E-voting System |
|---|---|
| FS1 | Check voter's age and marital status |
| FS2 | Check voter's id to see if the voter has already voted in the province, regency/city, district, or village. If the voter has already voted, the voter cannot vote anymore |
| FS3 | The system is able to update the voters' status for each election |
| FS4 | The system is able to store the voters' voting data |
| FS5 | The system generates a public key and a private key, which the voters can use to verify their vote to ensure that it has not been changed after voting and is included in the vote count |
| FS6 | The system provides an encrypted ballot to the voter after voting as evidence that the voter has voted and as proof for verification |
| FS7 | Read the voter's QR id code to check the eligibility of the voter at the voter authentication stage |
| FS8 | Read the QR code ID at the voter authentication stage |
| FS9 | The system provides an admin page through a login process |
| FS10 | The system provides functions for adding, changing, reading, and deleting candidate data |
| FS11 | The system provides functions for adding, changing, reading, and deleting voter data |
| FS12 | The system provides a vote result page that is automatically filled in based on the voting data |
| FS13 | The system provides an election minutes page that is filled in automatically based on the vote count |
| FS14 | The system allows voting officers, witnesses and KPU to carry out each stage of voter/vote verification |

2. Analysis of non-functional e-voting system requirements
   Analysis of the non-functional requirements of the e-voting system shown in Table 2 [*26*].

Table 2. Analysis of Non-functional Requirements of E-Voting System [*26*]

| RD Code | Non-Functional Requirements (NF) of E-voting System for Elections in Indonesia |
|---|---|
| NF1 | Use encryption during data exchanges between terminals, local servers and central servers. |
| NF2 | The system provides a voter confirmation page to ask whether the voter is sure of his/her choice for a candidate. |
| NF3 | A system is available for exchanging data through intranet and internet networks. |
| NF4 | The system provides a voting terminal, a local server and a central server. |
| NF5 | There are restrictions on voter interaction with voting terminals. |
| NF6 | The system must be able to be used outside the selected voter area for all elections at the provincial, regency/city, district, and village levels. |
| NF7 | The system can only accept votes during the voting period. |

3. Determination of individual verifiability requirements
   Based on Table 1 (Analysis of Functional Requirements) and Table 2 (Analysis of Non-Functional Requirements) it was then determined which ones would be included in the individual verifiability requirements, the results of which are listed in Tables 3 and 4.

Table 3. Individual Verifiability Requirements based on Functional Requirements

| FS Code | Verifiability Requirements |
|---|---|
| FS2 | IV1: Voters can verify that they have not already voted (before voting) |
| FS5<br>FS6 | IV3: Voters can verify that their vote has been not changed and has entered the vote count (after voting) |
| | IV4: Voters can verify that their vote has not been changed and has entered the vote count (after vote counting) |

Table 4. Individual Verifiability Requirements based on Non-Functional Requirements

| NF Code | Verifiability Requirement |
|---|---|
| NF-02 | IV2: Voters can make sure that their votes do not change during the voting process |

Based on Tables 3 and 4, there are 4 steps that must be passed to achieve 1individual verifiability. Dependency between stages is shown in Figure 3.

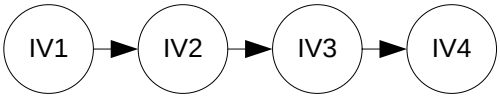


Figure 4. Dependency between stages in the proposed individual verifiability

Based on Figure 3, the following provisions for the Individual Verifiability Metric were made:
1. If IV1 is fulfilled, then the individual verifiability degree = 1/4.
2. If IV1 and IV2 are fulfilled, then the individual verifiability degree = 2/4.
3. If IV1, IV2 and IV 3 are fulfilled, then the individual verifiability degree = 3/4.
4. If IV1, IV2, IV3 and IV4 are fulfilled, then the individual verifiability degree = 1.
5. There is dependency between the stages: if the previous stage is not fulfilled, then the next stage cannot be calculated. For example if IV1 is not fulfilled, then IV2, IV3 and IV 4 are not taken into account and the individual verifiability degree = 0.

Based on the above conditions, the proposed Individual Verifiability Metric is:

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

where,

$v = Value\ of\ Verifiability\ stage$
$i = stage\ to$
$p_i = verifiablity\ stage\ of\ the\ protocol\ voting$

Verifiability stage ($v$) is determined, where a value of 0 means that verification will not be done (not verifiable), while a value of 1 means that verification will be done (verifiable).

$$IV_d = \frac{\sum_{i=1}^{n} w_i}{n} \quad (4)$$

where,

$IV_d = Individual\ Verifiability\ Degree$
$n = Number\ of\ Individual\ Verifiability\ stages$
$w_i = \begin{cases} v_i, \text{if } \forall j \in \{1..i-1\},\ v_j \neq 0\ OR\ i = 1 \\ 0, \text{if } \exists j \in \{1..i-1\},\ v_j = 0 \end{cases}$

The range of the individual verifiability degree is 0 to 1. The closer the value of the verifiability degree to 1, the more individual verifiability is fulfilled.

## 4. Results and Analysis

To show an example of the calculation of the Individual Verifiability Metric, we apply it to several existing voting protocols, namely:

### *A. Traditional Voting Protocol in Indonesia [27]*

The discussion of the traditional voting protocol deals with the voting protocol currently in force in Indonesia, which uses traditional methods, consisting of:

a. Voter registration:
   - The General Election Commission (KPU) verifies the voter data to establish the Permanent Voters List (DPT) based on the Population Database.
   - KPU prints a Notice of Model C-6 to be submitted to the Voting Organizing Group (KPPS) Officer.
   - The KPPS Officer then submits a Notice of Model C-6 to the voters.

b. Voter authentication:
   - The KPPS Officer submits copies of DPT, DPTb, Form C, Model C1, Annex KPPS to the supervisor and witnesses who participate in monitoring the implementation of the vote counting.
   - Voters enter the polling station carrying form C6, which is a notification letter. If they do not have a C6 form, they can bring an Identification Card/Passport (KTP) or another form of identification.
   - Voters have been registered in the Permanent Voters List (DPT) or Special Voters List (DPK).
   - The KPPS officer checks the names of the voters on the final voter list (DPT).
   - Voters get a queue number from the KPPS officer.

c. Voting:
   - Voters receive a ballot from the KPPS officer.
   - Voters go to the voting booth and cast their vote.
   - Selector enters a voice mail to the voice box.
   - Each voter dips his or her finger into an ink bottle to prevent them from voting twice. Voters leave the polling station.

d. Vote calculation:
   - The ballots in the ballot box are counted by the KPPS officer, supervisor and witnesses.
   - The results of the vote calculation are verified to produce the Vote Report.
   - The Vote Report is submitted to the KPU.
   - The KPU verifies all Vote Reports and stores the results of the votes in the KPU database.
   - The KPU announces the results of the vote counting in media announcements.

### *B. Modified Three Ballot Protocol [28]*

After going through the process of checking eligibility, the voters enter their vote through an electronic voting console. Based on the selected data received, the system then produces one electronic ballot, one paper ballot, and one paper ballot receipt. The three ballot items are then given a unique identity (ballot ID), which is generated randomly and the choice part (voting

region) is filled with patterns according to the rules for filling ThreeBallot that are random but represent the choices that have been entered.

During the voting period, representatives (witnesses from other candidates or observers) can carry out checks (sampling checks) of the operational correctness using a ballot & receipt generator module and a checker module. Checking is done through the checking console provided. With the vote input and random ID entered by the representatives, the ballot & receipt generator module will generate 3 tuples and a verification code. The module output is matched with the output expected by the representatives (previously calculated according to the algorithm claimed to be used in the module). Checking the checker module is done in a similar way. Authorities can also check another ballot & receipt generator module and another checker module.

Before being stored in the e-ballot box database, the three tuples representing the three parts of the electronic ballot will pass through a mixer to randomize their placement in the e-ballot box. This is done to obscure the connection between the three parts of the ballot. If all three are stored sequentially in the database, the relationship between the three will be too easy to guess. All data stored in the e-ballot box are also sent to a backup database (mirror). A bulletin board is used to announce the total number of ballots that have been entered into the system. This bulletin board can be consulted directly by the public.

*C. Cortier et al.'s Protocol [17]*

Cortier et. al.'s protocol defines verifiability for the case when the bulletin board could potentially act improperly and create vote entries (i.e. it creates votes on behalf of voters who did not vote) or removes ballots submitted by voters. Where to model the e-voting scheme $\Pi$ as a tuple $(Setup, Credential, Vote, VerifyVote, Valid, Board, Tally, Verify)$ of the polynomial-time probabilistic algorithm (ppt) where $VerifyVote$ and $Verify$ are non-interactive. The entities are registrar *Reg*, bulletin board $B$, teller $T$ and voter $V_i$. The setup $(\ell)$ algorithm is run by teller $T$ and outputs the public parameters from the election $(prm_{pub})$ and the key to the secret calculation $(sk)$. The credential procedure is executed by *Reg* with identity $id_i$ of voter $V_i$, and the public/secret credential $(upk_i, usk_i)$. The Vote algorithm is run interactively between $B$ and $V_i$, on $prm_{pub}$, the input, $c_i$, and the credential options $(upk_i, usk_i)$. After successful termination, ballot $b_i$ is added to the public transcript ($\tau$) of the election. The procedure output $Valid$ $(b)$ (1 or 0) depends on whether $b$ is well formed. The board shows the algorithm that $B$ must run to update $\tau$. The Tally algorithm is run at the end of the selection by $T$, giving the content of $B$ and secret key $sk$ as input, and the output of the calculation of proof $P$ and the end result. VerifyVote$(\tau, upk_i, usk_i, \text{b})$ is an algorithm that is run by voter $V_i$ and checks whether vote $b$ appears in $\tau$. The algorithm $Verify(\tau, Result, P)$ shows verification of the election result, temporarily. VerifyVote$(\tau, upk_i, b_i)$ shows verification of vote $b_i$ from voter $V_i$ included in the final transcript of the election announced by $B$.

For some of the voting protocols above, the degrees of individual verifiability are calculated based on Formulas (3) and (4), as shown in Table 5.

Table 5. Results of Calculation of Individual Verifiability Degrees for Voting Protocols

| Name of Protocol | Individual Verifiability Stages | | | | Individual Verifiability Degreee |
|---|---|---|---|---|---|
| | IV1 | IV2 | IV3 | IV4 | |
| Traditional Voting Protocol in Indonesia [27] | 0 | 0 | 0 | 0 | 0 |
| Modified Three Ballot Protocol [28] | 1 | 1 | 1 | 1 | 1 |

| Name of Protocol | Individual Verifiability Stages | | | | Individual Verifiability Degreee |
|---|---|---|---|---|---|
| | IV1 | IV2 | IV3 | IV4 | |
| Cortier et al.'s Protocol [*17*] | 1 | 1 | 1 | 0 | 0.75 |

Based on Table 5, we find the result of individual verifiability measurement, as shown in the following graphic:

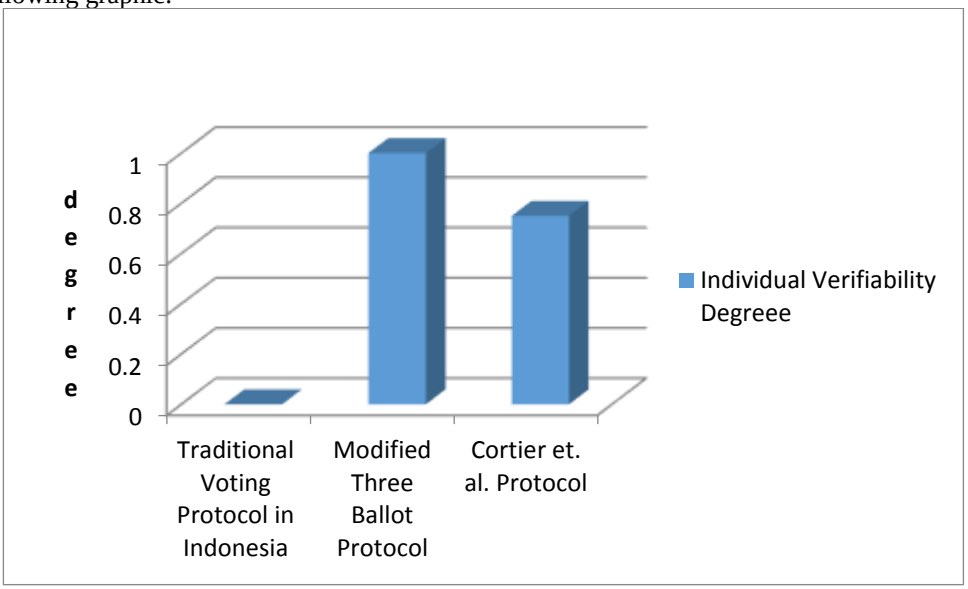


Figure 5. Individual verifiability calculation result

Based on the degree of verifiability formulas (3) and (4), the degree of verifiability was successfully measured for 3 protocol examples of the e-voting system. Based on the result of the calculation of the degree of verifiability, an agreement can be reached about which e-voting protocol will be selected for implementation, considering the degree of verifiability.

## 5. Conclusions

In this paper, an Individual Verifiability Metric for e-voting systems was proposed. For 3 examples of voting protocols, the degree of individual verifiability was measured. Based on the results of calculating the degree of individual verifiability in these 3 examples, agreement can be reached about which protocol will be selected for implementation, considering the degree of individual verifiability.

## 6. Future Work

In addition to individual verifiability there is also universal verifiability, related to verifiability for officers and witnesses or other parties. In that case, verifiability relates to each voting stage, i.e. before the election, during the election, after the election and after the vote count, which is called end-to-end verifiability. In view of this, future research can be conducted to create Universal Verifiability and End-To-End Verifiability Metrics.

## 7. References

[1] M. Bellis. (2015, December ) 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 Europe – Technology, Law, Politics and Society. Lake of Constance*, Bregenz, 2004.

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

[4] D Cetinkaya and O. Cetinkaya, "Verification and Validation Issues in Electronic Voting," *The Electronic Journal of e-Government*, vol. 5, no. 2, pp. 117 - 126, 2007.

[5] A. Riera and P. Brown, "Bringing Confidence to Electronic Voting," *Electronic Journal of e-Government*, vol. 1, no. 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-Governmen*, vol. 2, no. 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, pp. 190–200.

[10] M. K. Reiter and A. D. Rubin, "Crowds: Anonymity for Web Transactions," *ACM Transactions on Information and System Security*, vol. 1, 1998.

[11] O. Berthold, A. Pitzmann, and R. Standtke, "The Disadvantages of Free MIX Routes and How to Overcome Them," in *Proceedings of the International workshop, on Designing Privacy Enhancing Technologies: Design Issues in Anonymity and Unobservability*, 201, pp. 30-45.

[12] A. Serjantov and G. Danezis, "Towards an information theoretic metric for anonymity," in *Privacy Enhancing Technologies workshop (PET 2002), volume 2482 of LNCS*, R. Dingledine and P. Syverson, Eds. San Francisco, CA, USA: Springer-Verlag, 2002.

[13] Aggelos Kiayias , Thomas Zacharias, and Bingsheng Zhang, "Formal Analysis of Chaumian Mix Nets with Randomized Partial Checking," *IEEE Security & Privacy*, vol. 15, no. 3, June 2017.

[14] C. S. Guasch, "Individual verifiability in electronic voting," Universitat Polit`ecnica de Catalunya, Barcelona, Dissertation 2016.

[15] Ralf Kuster, Tomasz Truderung, and Andreas Vogt, in *2014 IEEE Symposium on Security and Privacy*, 2014.

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

[17] Veronique Cortier, David Galindo, Stephane Glondu, and Malika Izabachene, "Election Verifiability for Helios under Weaker Trust Assumptions," in *Computer Security - ESORICS 2014*, 2014, pp. 327-344.

[18] Ben Smyth, Steven Frink, and Michael R. Clarkson, "Computational Election Verifiability: Definitions and an Analysis of Helios and JCJ," Technical Report 2015.

[19] Veronique Cortier, David Galindo, and Ralf Kusters, "SoK: Verifiability Notions for EVoting Protocols," in *IEEE Symposium on Security and Privacy*, 2016.

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

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

[22] A. Jaquith, *Security metrics : replacing fear, uncertainty, and doubt*., 2007.

[23] T.W. Purboyo, B. Rahardjo, and Kuspriyanto, "Security Metrics: A Brief Survey," in *Communication Information Technology and Biomedical Engineer*, Bandung, 2011.

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

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

[26] Fitrah Satrya Fajar Kusumah, *Pengembangan Sistem E-Voting Pilkada Di Indonesia Berbasis Direct Record Electronic Dengan Pendekatan Kiosk*. Bogor: Institut Pertanian Bogor, 2016.

[27] *Undang-Undang Republik Indonesia No. 7*., 2017.

[28] T. N. Suharsono, Kuspriyanto, B. Rahardjo, and F. A. Yulianto, "Verifiability notion in e-Voting based on modified ThreeBallot system," in *2017 International Conference on Information Technology Systems and Innovation (ICITSI)*, Bandung, 2017, pp. 67 - 72.

**Teguh Nurhadi Suharsono** graduated from STT Indonesia in Bachelor of Informatics Engineering in 2001 and Master Degree of Informatics in 2008 from Bandung Technology Institute. He is now a Senior Lecturer at Sangga Buana YPKP University. His research interest lies in the area of Information System, Security System, and Data Mining.
email: teguhns21@gmail.com

**Kuspriyanto** is a professor at the School of Electrical Engineering and Informatics, Institut Teknologi Bandung. He received his bachelor degree in Electrical Engineering from Institut Teknologi Bandung in 1974, D.E.A (1979) and Ph.D. (1981) in Automatic System from USTL, France. His field of interest includes Computer System, Computer Architecture, and Real Time Systems.
email: kuspriyanto@yahoo.com

**Budi Rahardjo** is a lecturer at the School of Electrical Engineering and Informatics, Institut Teknologi Bandung. He received his bachelor degree in Electrical Engineering from Institut Teknologi Bandung, Magister and Ph.D. from University of Manitoba Winnipeg, Canada. His field of interest includes IT Security, Cryptography, High Performance Computing, Impact of Information Technology (IT) in various areas, Digital Entertainment, Electronic Payment, Social network analysis, big data Artificial Intelligence (AI) and Machine Learning.
email: br@paume.itb.ac.id