International Journal of Basic and Applied Sciences, 14 (6) (2025) 525-531

International Journal of Basic and Applied Sciences

Website: www.sciencepubco.com/index.php/IJBAS
https://doi.org/10.14419/v717s146
Research paper

Analyzing The Trade-Off between Anonymity and Verifiability in Electronic Voting Protocols

Teguh Nurhadi Suharsono [1] *, Deshinta Arrova Dewi [2, 6], Heri Purwanto [1], Tri Basuki Kurniawan [3], Azizul Azhar Ramli [4], Lee Pak Ting Harvey [5]

[1] Faculty od Engineering, Universitas Sangga Buana, Bandung, Indonesia
[2] Faculty of Data Science and Information Technology, INTI International University, Nilai, Malaysia
[3] Magister Program, Universitas Bina Darma, Palembang, Indonesia
[4] Fakulti Sains Komputer Dan Teknologi Maklumat, Universiti Tun Hussein Onn Malaysia, Parit Raja, Batu Pahat 86400, Malaysia
[5] Faculty of Business and Communication, INTI International University, Malaysia
[6] Faculty of Engineering and Technology, Shinawatra University, Thailand
**Corresponding author E-mail: i24026069@student.newinti.edu.my*

Received: July 4, 2025, Accepted: August 5, 2025, Published: October 25, 2025

Abstract

E-voting, also known as electronic voting, is the practice of casting a ballot or voting using digital technology. Verifiability and anonymity are two important considerations in this situation. The study aims to find the optimal balance between these two crucial concepts, specifically the method of value range area (trade-off) between anonymity and verifiability in e-voting protocols. High levels of e-voting verifiability and anonymity are combined in this value range. The result should be an electronic voting system that protects voters' rights to privacy while promoting confidence in and transparency surrounding election outcomes. This study evaluated several current e-voting protocols to see which ones came closest to the ideal harmony between anonymity and verifiability, utilizing verifiability calculation metrics and anonymity calculation metrics. The balancing area was divided into 4 areas in this investigation. The study's area of balance between verifiability and anonymity can demonstrate that the e-voting protocol is in the ideal category region for such a protocol. After examining numerous e-voting procedures, some issues have finally been identified. The e-voting protocol is ideal because Area 2 is the area where anonymity and verifiability have ideal degree values. E-voting enhancement verifiability protocols are examples of protocols that achieve the perfect balance between anonymity and verifiability.

Keywords: *Anonymity; E-Voting Protocol; Process Innovation; Transparent Governance; Verifiability.*

1. Introduction

E-voting, often known as electronic voting, is the practice of casting a ballot or casting a vote using digital technology. Verifiability and anonymity are two important considerations in this situation. Both are essential components of a reliable and secure e-voting system. An essential element of elections is anonymity, which guarantees that each voter can cast a ballot in confidence. An essential element of elections is anonymity, which guarantees that each voter can cast a ballot in confidence. The voter must have faith that his or her choice cannot be linked to them personally. This rule safeguards individual suffrage and forbids force, manipulation, or intimidation during the voting process. Using cryptographic technology and protocols, it is possible to provide voter anonymity in an electronic voting system. This enables voters to cast ballots without immediately disclosing their identities. To ensure that voters stay anonymous during the data transmission process, wireless cryptographic devices can be employed to encrypt voter data before it is transferred to an e-voting server.
The importance of anonymity is preventing coercion and intimidation: If voters' ballots can be tracked, they run the risk of being threatened or subjected to compulsion by parties, protecting the privacy of choice: Protecting the privacy of voters' choices, which is a fundamental human right in elections, includes protecting their anonymity.
Verifiability is the capacity of an electronic voting system to confirm the legitimacy and impartiality of votes cast by voters. Voters need to be confident that their ballots are accurately counted and not changed or influenced throughout the voting process. Transparency is crucial in the context of verifiability because it allows each voter to confirm that their vote is counted according to their intentions. In electronic voting, several strategies can be applied to provide verifiability. One such technique is "proof of correctness," in which an electronic voting system must offer a mathematical justification that the outcome accurately reflects the voters' ballots.
How crucial is verifiability?

Copyright © Teguh Nurhadi Suharsono et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

- Voters will be more inclined to believe that the election results are correct and that there was no fraud or manipulation if the e-voting technology can be independently confirmed.
- Identify errors and fraud: Verifiability enables impartial examinations of the electoral process's integrity, enabling the identification and correction of faults and fraud.

It is crucial to keep in mind that there must be a careful balance between verifiability and anonymity. Any of the variables could be jeopardized by improper e-voting technology installation, endangering the credibility and trust of election outcomes. Overall, the design and implementation of a safe and reliable e-voting system must consider two crucial factors: anonymity and verifiability. In electronic voting systems, combining anonymity and verifiability is a difficult technological and security challenge. Voters' rights can be upheld by maintaining complete anonymity, and public confidence in the voting process can be preserved by meticulous verification. E-voting systems must strike a balance between anonymity and verifiability to maintain the honesty, security, and confidence of voters in the electronic voting process.

Based on the concept of the range of verifiability degree values [1], the maximum verifiability degree is 1. If an e-voting protocol reaches the value of verifiability degree = 1, then the e-voting protocol is verified. If based on the concept of the range of anonymity degree values, then the maximum anonymity degree is 1, so the e-voting protocol with the anonymity degree value = 1 is the e-voting protocol is anonymity [2]. The description of the degree of verifiability and the degree of maximum/best anonymity is shown in Fig. 1, where the x-axis shows the degree of anonymity, and the y-axis shows the degree of verifiability. The ideal point is indicated by the X mark with an anonymity value = 1 and a verifiability value = 1.

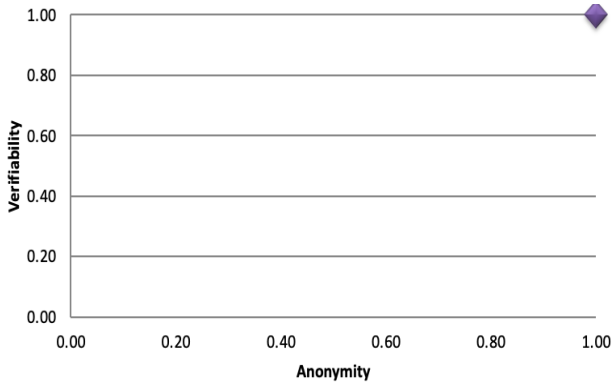

Fig. 1: The Ideal Degree of Verifiability and Anonymity.

The requirements for anonymity and verifiability in e-voting protocols have been the subject of numerous studies, but most of these studies have not calculated the degree of verifiability or degree of anonymity, nor have they identified or evaluated the e-voting protocol's requirements for the ideal degree of verifiability and needs. The initial study focused on developing a blockchain-based framework for fully verified online electronic voting. The cryptographic primitives used in our electronic voting protocol, known as VYV for Verify-Your-Vote, include pairings, identity-based encryption, and elliptic-curve cryptography (ECC). It guarantees the following security and privacy features: only eligible voters may cast ballots; voter authentication; vote privacy; receipt-free voting; fairness; and individual and global verifiability. Additionally, we use the ProVerif tool to explicitly demonstrate the security of our protocol [3]. The research that follows suggests AvecVoting, a blockchain-based electronic voting system that is anonymous and verifiable, offers high performance and excellent security and employs threshold encryption and one-time ring markings to safeguard voter privacy and ballot confidentiality. In addition, we added the idea of a "counter" for counting votes to enhance performance. The reputation-based PayOff algorithm, based on smart contracts and a carefully crafted RandomSortition, allows AvecVoting to achieve accurate counting even when some counters cannot be trusted. Our research on the security and performance of AvecVoting reveals that it offers robust security features like anonymity, non-repeatability, secrecy, and verifiability while also addressing the performance challenges brought on by blockchain and offering good efficiency during the voting and counting stages [4]. The following study introduces the TrustedEVoting (TeV) framework, a blockchain-based strategy that includes not only the essential components needed for secure and verifiable e-Voting but also extra features like support for re-voting, post-election vote checking, and channel preference voting. The latter is crucial because TeV's framework offers a multi-channel approach to voting, and the switch from traditional physical voting to electronic voting is not immediate [5]. Future research suggests an Internet e-voting system that uses double signatures to satisfy fundamental requirements, including anonymity, verification, eligibility, privacy, free receipts, and fairness. Using formal methods, we demonstrate the efficiency and validity of our system. Thorough performance tests reveal that our method performs better than the currently used advanced signature blind e-voting internet protocols [6]. The PVPBC voting system was suggested in a different study. It is an electronic voting system that ensures privacy and verification without impairing voter use. The PVPBC voting system makes use of a distributed authorization technique that is efficient and based on irrevocable anonymity. It also makes use of smart contracts and legally distributed ledgers. Additionally, employing the Selene voting scheme, the PVPBC voting system passes election verification requirements. A verifiable e-voting protocol is the Selene Protocol. It posts audio files in plain text along with a tracking number. This enables voters to verify that the system has accurately recorded their votes. The PVPBC scale is also a function of voter and candidate turnout, according to numerical experiments. Specifically, the PVPBC authorization time grows linearly with population size. With the number of the voting population, there is a linear increase in the average access latency as well. When a valid authentication transaction is made and sent through a DLT network, there is a 6.275 ms latency [7]. The following study suggests a novel e-voting system based on secret sharing and k-anonymity that not only achieves fundamental security goals like non-cheating, universal verification, confidentiality, and anonymity but also additional properties like coercive resilience and unconditional security because the proposed system's security is independent of any computationally challenging problems [8]. The research that follows focuses on a verifiable E2E internet voting system that gives voters mobility and enables them to covertly cast their votes on public computers while enjoying the advantages of early voting. The suggested method uses the individual identity and biometric characteristics of voters to support the electoral process globally. We suggest a brand-new anonymous voting-based blind signature system. We used the Boneh-Lynn-Shacham short signature approach, which provides the greatest degree of ballot size secrecy.

The technology gives each voter a digital witness so they can verify their vote was recorded as intended, and the public may verify that all recorded ballots have been appropriately counted. Under the discrete logarithm of the well-known elliptic curve and the Diffie-Hellman

gap assumption, the suggested system's privacy is attained [9]. Next, examine potential threats to voting privacy under each model and conduct a study on the framework of the opposing model concerning electronic voting systems. Based on our analysis, we contend that voting procedures based on secret sharing provide a more organic and elegant privacy-preserving solution than those based on encryption. As a result, we created and put into place the Koinonia voting system, which offers long-term privacy against strong adversaries and enables anyone to check that every ballot has been properly formed, and the counting is carried out. Our tests demonstrate that Koinonia protects voting privacy effectively [10]. Following an investigation, the Ordinos end-to-end counting concealment e-voting system was offered as the first to be verified secure and verifiable. We designed our system using the MPC protocol and the proper cryptographic primitives for increased testing, deployment, and performance evaluation, proving the system's viability. Additionally, our research contributes to a greater knowledge of tally concealment in general, specifically how much it impacts the degree of privacy and verification of electronic voting systems [11]. The analysis of e-voting needs and protocol model design stages for verifiability requirements has been done as follows. Voters, Officers, Witnesses, or General Election Commissions are a few of the parties involved in meeting verification needs. These commissions allow multiple parties to verify voters' ballots before, during, and after the counting of votes in elections. Traditional simulation modeling and voting testing have been done in comparison with simulation modeling and testing of e-voting protocols to meet the verifiability requirements of this e-voting system. Before performing simulated protocol modeling and testing, formal notation authoring using Communicating Sequential Processes (CSP) notation was carried out. With formal verification demonstrating that the protocol specification complies with predefined integrity properties, protocol testing will be carried out. The verification tool, SPIN (Simple Promela Interpreter), is based on reference modeling and can assess the logical coherence of specifications and report proven attributes. The verified system speaks PROMELA, a translation of CSP's formal notation, which stands for MEta LANguage Process [12]. Fig. 2 provides a summary of numerous e-voting protocol settings with varying degrees of verifiability and anonymity.

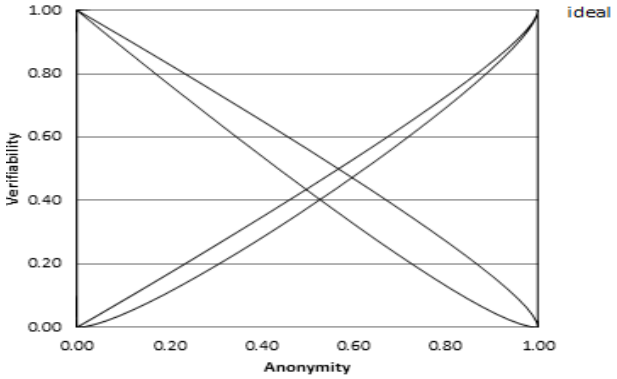

Fig. 2: Overview of the E-Voting Protocol's State, Degree of Verifiability, and Degree of Anonymity.

In Fig. 2, there are various verifiability and anonymity conditions in the e-voting protocol, which make it very difficult to see that the e-voting protocol is included in the category of the ideal area of balance between the degree of anonymity and verifiability, where the x-axis shows the degree of anonymity, and the y-axis shows the degree of verifiability. The ideal point is indicated by the X mark with an anonymity value = 1 and a verifiability value = 1. This study on the method of value range area (trade-off) between anonymity and verifiability in e-voting protocols aims to find the ideal balance point between these two important principles. This value range area includes a combination of high anonymity and high verifiability of e-voting. The goal is to produce an e-voting protocol that secures voters' privacy rights while ensuring trust and transparency in election results. This study assessed several existing e-voting protocols to see which e-voting protocols approached the ideal balance between anonymity and verifiability using anonymity calculation metrics from the study [2] (as follows:

$$d = 1 - p \tag{1}$$

Based on formula (1), the level of anonymity is further defined as, where p is the likelihood that a specific user will be identified by the attacker. In this approach, the value of the anonymity level is significantly determined by the number of voters or messages. The value of the voter anonymity level is 1/2, or 50% if there are 2 (two) voters in a system. The level of anonymity is 1 - 0.001 or 0.999 when there are 1,000 votes. In the meantime, each voter's probability value is 0.001. Calculation of the degree of verifiability using metrics from the study is as follows [1]:

$$V_T = \frac{\sum_{i=1}^{n} v_i}{n} \tag{2}$$

$$d = 1 - p \tag{3}$$

Based on formula (2), V_T is the degree of verifiability, v_i is the value of verifiability requirements, and n is the total of verifiability requirements.

2. Ease of use

The procedures are followed as described in Fig. 3. below to see if a protocol achieves the appropriate balance between anonymity and verifiability.

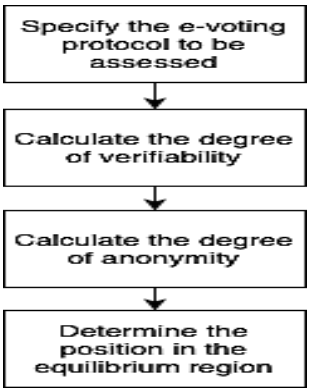

Fig. 3: How to Evaluate the E-Voting Protocol's Position in Terms of Balancing Verifiability and Anonymity.

The stages for setting the electronic voting system to strike a balance between anonymity and verifiability are shown in Figure 3:

- Determine the e-voting protocol to be assessed.

Based on several existing e-voting protocols, we assess to see which protocols enter which balance area.

- Calculate the degree of verifiability.

To calculate the degree of verifiability using formula (2) with the need for verifiability that has been determined from the study [13] [12]. The verifiability requirements and the value of the verifiability needs of each e-voting protocol for the verification needs are filled with a value of 1, which means verified, and a value of 0, which means not verified, for the verification needs, as in Table 1.

Table 1: Examples of Requirements and Verifiability Values in E-Voting Protocols

Code	Requirement Verifiability	Value of Requirement Verifiability
KV1	Voters can confirm that they did not cast their ballots before the election	1
KV2	Officers can confirm that voters did not cast their ballots before the election	1
KV3	Witnesses can attest that voters did not decide who they would support before the election	1
KV4	After casting their ballots, voters can confirm that their decision has not been altered and that it has been counted	1
KV5	After the vote count has been completed, voters can confirm that their choice of votes has not been altered and has been counted	0
KV6	After voters have cast a ballot, officers can confirm that their selection of votes has not been altered and is included in the vote total	1
KV7	After voters have cast a ballot, witnesses can confirm that their selection of votes has not been altered and has been included in the vote total	1
KV8	After voters have cast a ballot, the General Election Commissions can confirm that their selection of votes has not been altered and that it has been counted	1
KV9	After the vote count, officers can confirm that the voter's choice of voters has not changed and is included in the vote count	0
KV10	After the vote is counted, witnesses can confirm that the voters' vote choices have not changed and that they were included in the vote count	1
KV11	General Election Commissions may check, following the vote count, if voters' ballot choices have not altered and are still counted	1
KV12	Voters may make sure their preferences don't change throughout the election	1

- Calculate the degree of anonymity

Based on formula (1), the degree of verifiability is calculated by looking at how likely a ballot can be seen.

- Determine the position of the e-voting protocol in anonymity balance with verifiability

The proposed anonymity balance area with verifiability for the e-voting protocol is shown in Fig. 4.

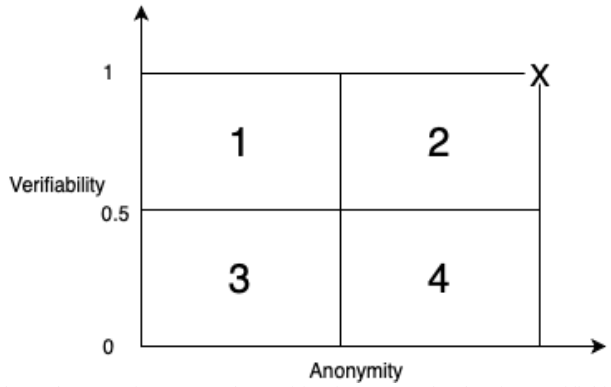

Fig. 4: How to Evaluate the E-Voting Protocol's Position in Terms of Balancing Verifiability and Anonymity.

Based on Fig. 4, the x-axis shows the degree of anonymity, and the y-axis shows the degree of verifiability. The ideal point is indicated by the X mark with an anonymity value = 1 and a verifiability value = 1.

Determination of the balance area into 4 areas with the following value range provisions:

- Area 1 is a non-ideal anonymity category with a range of anonymity degree values >= 0 to <= 0.5 and the ideal verifiability category with a verifiability degree value range of > 0.5 to <= 1.

- Area 2: ideal anonymity and verifiability degree value range > 0.5 s to <= 1 and the range of verifiability degree values > 0.5 to <= 1.
- Area 3: the anonymity category is not ideal with a range of anonymity degree values >= 0 to <= 0.5, and verifiability is not ideal with a range of verifiability degree values >= 0 to <= 0.5.
- Area 4: ideal anonymity category with anonymity degree value range > 0.5 to <= 1, verifiability is not ideal with a range of verifiability degree values >= 0 to <= 0.5.

Flowchart to determine the anonymity and verifiability balance category areas for e-voting protocols, as in Fig. 5.

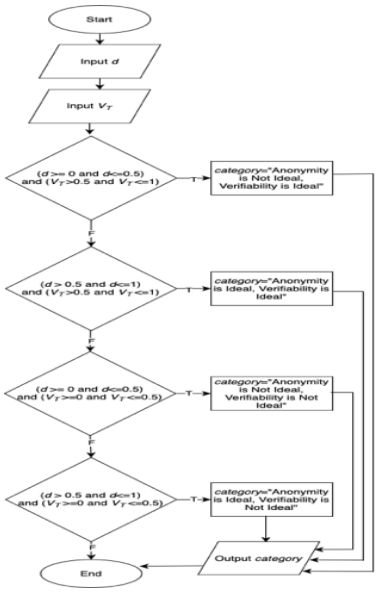

Fig. 5: Flowchart to Determine the Anonymity and Verifiability Balance Category Areas for E-Voting Protocols.

Pseudocode to determine the balance category area of anonymity and verifiability for e-voting protocols exists as in Fig. 6.

```
Input     : d, V_T
Output    : category

if  (>d= 0 and <=d0.5)  and ( > 0V_T.5 and  <=V_T1)
    category =  "Anonymity is Not Ideal, Verifiability is Ideal"
else
    if  (> 0.5 and <=1)  and ( >0ddV_T.5 and , V_T <=1)
        category =        "Anonymity is Ideal, Verifiability is Ideal"
    else
        if  (>d= 0 and <=d0.5)  and ( >=0 and V_T, V_T <=0.5)
            category =            "Anonymity is Not Ideal, Verifiability is Not Ideal"
        else
            if  (> 0.5 and <=1)  and ( >=0 and ddV_T, V_T <=0.5)
                category =              "Anonymity is Ideal, Verifiability is Not Ideal"
            endif
        endif
    endif
endif
```

Fig. 6: Pseudocode to Define Anonymity and Verifiability Balance Category Areas for E-Voting Protocols.

Based on The flowchart in Figure 5 and the Pseudocode in Figure 6 can be explained as follows.

- Input the value of degree Amomity (d).
- Input the value of degree Verifiability (VT).
- Selection of Anomity degree value (d) and Verifiability degree value (VT):
- If the range of anonymity degree values is >=0 to <= 0.5 and the range of verifiability degree values >0.5 to <=1, then the categories are anonymity is not ideal and verifiability is ideal.
- If the range of anonymity degree values >0.5 to <=1 and the range of verifiability degree values >0.5 s to <=1, then the category is ideal for anonymity and verifiability.
- If the range of anonymity degree values >=0 to <= 0.5 and the range of verifiability degree values >=0 to <= 0.5, then the category is anonymity is not ideal and verifiability is not ideal.
- If the range of anonymity degree values >0.5 to <=1 and the range of verifiability degree values >=0 to <= 0.5, then the category is ideal anonymity and verifiability is not ideal.
- The output is the category area for the e-voting protocol

3. Result and Analysis

Several e-voting protocols are chosen to determine the area of balance between anonymity and verifiability of the e-voting protocol. The next step is to analyze and calculate the degree of anonymity based on formula (1) for these e-voting protocols, as in Table 2. For Example, Verify-Your-Vote [3] has several Anonymity Possibilities (p) = 0, then value d =1 (d =1-0).

Table 2: Anonymity Degree Calculation Result

No	E-voting Protocol	Number of Anonymity Possibilities	Value of d
1	Verify-Your-Vote [3]	0	1
2	Ordinos [11]	1	0
3	Koinonia [10]	0	1
4	Identity-Based Blind Signature [9]	1	0
5	Secret Sharing and K-anonymity [8]	0	1
6	PVPBC [7]	0	1
7	Anonymous and formally verified dual signature (AAFVDS) [6]	0	1
8	For you [5]	0	1
9	AvecVoting [4]	0	1
10	Improvement Verifiability Requirements (IVR) [12]	0	1

Then also analyzed and calculated the degree of verifiability of the e-voting protocols based on formula (2) in Table 3. For Example, Verify-Your-Vote [3] has a value of $v_i = 7$, n = 12, then the value of $V_T = 7/12$ is 0.58.

Table 3: Anonymity Degree Calculation Result

No.	E-voting protocol	Verifiability Requirements												Value of V_T
		KV 1	KV 2	KV 3	KV 4	KV 5	KV 6	KV 7	KV 8	KV 9	KV 10	KV 11	KV 12	
1	Verify-Your-Vote [3]	0	1	0	1	1	1	1	0	1	0	0	1	0.58
2	Ordinos [11]	1	1	1	1	1	1	1	1	1	1	1	0	0.92
3	Koinonia [10]	0	1	0	1	1	1	1	1	1	1	1	0	0.75
4	Identity-Based Blind Signature [9]	0	0	0	1	1	1	0	0	1	0	0	1	0.42
5	Secret Sharing and K-anonymity [8]	0	0	0	1	1	1	0	1	0	0	0	1	0.42
6	PVPBC [7]	1	1	1	1	1	1	1	1	1	1	1	0	0.92
7	Anonymous and formally verified dual signature (AAFVDS) [6]	1	1	1	1	1	1	1	1	1	1	1	0	0.92
8	For you [5]	1	1	1	1	1	1	1	1	1	1	1	0	0.92
9	AvecVoting [4]	1	1	1	1	1	1	1	1	1	1	1	0	0.92
10	Improvement Verifiability Requirements (IVR) [12]	1	1	1	1	1	1	1	1	1	1	1	0	0.92

Based on Table 4, Fig. 4 illustrates the balance between anonymity and verifiability for several e-voting systems.

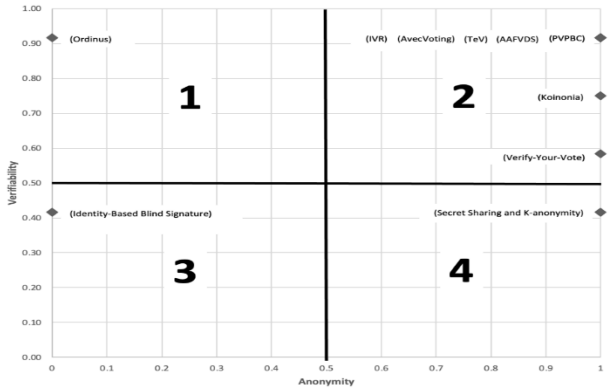

Fig. 7: Electronic Voting Protocol Balance Graph.

Table 4 and Figure 4's graph led to the following conclusion about the protocols' calculations of the degree of anonymity and verifiability based on the flowchart in Fig. 5 and pseudocode in Fig. 6:

- Area 1 has the Ordinos e-voting protocol [11].
- Area 2 has a protocol e-voting Improvement Verifiability Requirements (IVR) [12], AvecVoting [4], TeV [5], Anonymous and formally verified dual signature (AAFVDS) [6], PVPBC [7], Koinonia [10], Verify-Your-Vote [3].
- Area 3 has an Identity-Based Blind Signature e-voting protocol [9].
- Area 4 has Secret Sharing and K-anonymity e-voting protocols [8].

For protocols that are not included in area 2, it is recommended that, for anonymity (p) and verifiability (KV) requirements that are still at 0, it is recommended to improve the protocol so that it can meet the anonymity and verifiability requirements to a value of 1. These requirements can be adjusted to those listed in Table 1 so that they will be ideal (Area 2).

4. Conclusion

Two essential criteria for e-voting systems are anonymity and verifiability, which are opposed. It is possible to classify an electronic voting protocol as perfect if it satisfies both needs. An area of balance between verifiability and anonymity has been created in the study to demonstrate where the e-voting protocol stands in the optimum category area for an e-voting protocol. Several electronic voting protocols have been examined, and finally, some of them can be classified. The e-voting protocol is ideal because Area 2 is the area where anonymity and verifiability have ideal degree values. E-voting enhancement verifiability protocols are examples of protocols that achieve the perfect balance between anonymity and verifiability.

References

[1] T. N. Suharsono, D. Anggraini, Kuspriyanto, B. Rahardjo, and Gunawan, "Implementation of Simple Verifiability Metric to Measure the Degree of Verifiability of E-Voting Protocol," *2020 14th International Conference on Telecommunication Systems, Services, and Applications (TSSA*, pp. 1–3, 2020, https://doi.org/10.1109/TSSA51342.2020.9310915.

[2] M. K. Reiter and A. D. Rubin, "Crowds," *ACM Transactions on Information and System Security*, vol. 1, no. 1, pp. 66–92, 1998, doi: https://doi.org/10.1145/290163.290168.

[3] M. Chaieb, S. Yousfi, P. Lafourcade, and R. Robbana, "Verify-Your-Vote: A Verifiable Blockchain-Based Online Voting Protocol," *Information Systems*, pp. 16–30, 2019, https://doi.org/10.1007/978-3-030-11395-7_2.

[4] M. Li, X. Luo, W. Sun, J. Li, and K. Xue, "AvecVoting: Anonymous and Verifiable E-voting with Untrustworthy Counters on Blockchain," *ICC 2022 - IEEE International Conference on Communications*, May 2022, https://doi.org/10.1109/ICC45855.2022.9838840.

[5] M. B. Verwer, I. Dionysiou, and H. Gjermundrød, "TrustedEVoting (TeV) a Secure, Anonymous and Verifiable Blockchain-Based e-Voting Framework," *Communications in Computer and Information Science*, pp. 129–143, 2019, https://doi.org/10.1007/978-3-030-37545-4_9.

[6] M. N. Saqib *et al.*, "Anonymous and formally verified dual signature based online e-voting protocol," *Cluster Computing*, vol. 22, no. S1, pp. 1703–1716, 2018, https://doi.org/10.1007/s10586-018-2162-7.

[7] M. Sallal, Ruairi de Frein, and A. Malik, "PVPBC: Privacy- and Verifiability-Preserving E-Voting Based on Permissioned Blockchain," vol. 15, no. 4, pp. 121–121, Mar. 2023, https://doi.org/10.3390/fi15040121.

[8] Y. Liu and Q. Zhao, "E-voting scheme using secret sharing and K-anonymity," *World Wide Web*, vol. 22, no. 4, pp. 1657–1667, Apr. 2018, https://doi.org/10.1007/s11280-018-0575-0.

[9] M. Kumar, S. Chand, and C. P. Katti, "A Secure End-to-End Verifiable Internet-Voting System Using Identity-Based Blind Signature," *IEEE Systems Journal*, vol. 14, no. 2, pp. 2032–2041, 2020, https://doi.org/10.1109/JSYST.2019.2940474.

[10] H. Ge *et al.*, "Koinonia," *Proceedings of the 35th Annual Computer Security Applications Conference*, pp. 270–285, 2019, https://doi.org/10.1145/3359789.3359804.

[11] R. Küsters, J. Liedtke, J. Müller, D. Rausch, and A. Vogt, "Ordinos: A Verifiable Tally-Hiding E-Voting System," *IEEE Xplore*, 2020. https://doi.org/10.1109/EuroSP48549.2020.00022.

[12] T. N. Suharsono, N. Gunawan, and Rini Nuraini Sukmana, "e-Voting Protocol Modelling To Improve Verifiability Requirements," pp. 1–8, 2021, https://doi.org/10.1109/TSSA52866.2021.9768253.

[13] H. Almutairi, A. Alqahtani, Z. S. Jabbar, J. F. Tawfeq, A. D. Radhi, and Poh Soon JosephNg, "Design of an optimized energy-efficient routing protocol for reliable wireless body area networks," *International Journal of Power Electronics and Drive Systems/International Journal of Electrical and Computer Engineering*, vol. 14, no. 4, pp. 4386–4386, 2024, https://doi.org/10.11591/ijece.v14i4.pp4386-4393.