ESP Journal of Engineering & Technology Advancements (ESP-JETA)
ISSN : 2583-2646
Special Issue

VISION VOTE: DETECTION OF FRAUDS IN ELECTION USING THE IMPLEMENTATION OF OPEN CV

Dr.S. Muthukumar
HOD/CSE
Sree Sowdambika College Of Engineering
hodcse@sowdambikaengg.edu.in

V.Pon Tharani
UG scholar
SreeSowdambika College Of Engineering
tharaniponu@gmail.com

S.ShanmugaPriya
UG Scholar
SreeSowdambika College Of Engineering
Shanmugapriya648@gmail.com

Abstract—In this paper, an online voting method for elections in India is initially suggested. The suggested model has higher security as the voter's raised secure password must be validated prior to the recording of the vote in the major database owned by our nation's Election Commission. The model's additional feature allows the voter to verify that the right candidate or party received their vote. In this arrangement, a voter has the option to cast a ballot from a place other than the one designated for them or from their favorite site. Vote counting will be made in an automated fashion under the proposed approach, saving a significant amount of period and allowing our nation's Commission set for Election to declare the results in a much fast succession. Alongside the passwordbased authentication, we have also utilized the face-based authentication along with the successful implementation of the OpenCV in addition to the password validation. We describe a model for a web voting entity for India in this application using the above said constituents. When contrasted with the conventional voting system, this version of voting systems seems to be considerably much secure and efficient. The delays and frauds occurring during counting of votes can be easily prevented.

Keywords—Voting, Online, Computer Vision, Deep Learning, Haarcascading, OpenCV, and OTP.

I. INTRODUCTION

The public can select their representatives and express their beliefs in the manner in which they will be administered through an online voting system. The election process's credibility must be respected at all costs. Election procedures are secure, and if something goes wrong, the entity would enhance its capabilities of security. Nonetheless, there is a possibility of Maoist attacks, electoral rigging issues in some places, and the possibility of losing their vote and their lives. Therefore, the general people require a much more protective method of voting. Comparing voting in online mode to other voting methods has benefits. The establishment, voting, gathering, disseminating, and counting of those casted votes are only a few of the steps that a voting system in online mode might be indulged. When voting security was examined, the

issue of who gets to count every casted vote was taken care of. The same issue has also been explored more philosophically to consider its actuality and perception. Only because the voting system has such strict security requirements for confidentiality and integrity is it difficult to make it trustworthy. All voters must feel confident in the secrecy of their votes to prevent the sale of votes. Integrity is the guarantee that votes are correctly counted, and election results are accurate. People can cast their ballots in the proposed system with confidence and without any fear. If a voter casts a ballot against an evil candidate, the online voting method nevertheless offers them security by saving their vote in a safe digital format.

A. Background for Research

The currently prevailing voting systems administered by governmental organizations are not resistant enough to meet the hazards posed by the technological developments that have been realized in the last few decades [1]. There is research being undertaken to improvise the voting system with TFT modules, raspberry pi-based servers, biometrics, blockchain, etc. [2, 3]. However, there are still more challenges that need to be met since the electoral voting processes are subjected to an increased volume of illegal activities. As a result, the biometric-based security-enhancing voting system like [4] and other aspects enhancing systems [5] came into practice. Because of these improvised systems, our society has benefited a lot. Despite knowing several voting mechanisms and procedures [6-19] including the aboveindicated processes that were put forth in the past, it is still necessary to make the security aspect of the voting systemmore robust to prevent malpractices [20, 21].

B. Research Contributions

The following are the contributions of our currently pursued research work:

- We generate and register the password of every voting person as "Voter ID" to cast the vote in online mode in a remote fashion.
- We authenticate the registered password while the votingperson casts the vote.

- We enable the voting system to record the voting in the major database of our nation's Commission established for Election if authenticated with the correct password or else the vote will be void and will not be recorded in the major database of our nation's Commission established up for Election.

- We facilitate face-based authentication along with OpenCV in addition to password security to make the voting process more robust.

We successfully propose and test an online voting technology to boost the electoral system's transparency and dependability.

C. Organization of the Paper

The remaining sections of this manuscript have been structured in the following manner: Section II discusses prior works related to voting along with the realized disadvantages. Section III discusses the research preliminaries about CNN and its deployment. Section- IV discusses the built security aspect in our current voting process based on deep learning and computer vision. Section- V gives the results obtained with the various modules of the devised voting system. Section VI gives the concluding remarks for this research work.

II. RELATED WORKS

A. Existing Voting Works

The foundation of every democracy and institution is the voting process. Over the past few decades, the voting process has undergone numerous effective changes. Different voting methods are employed, including the paper ballot voting system, the electronic voting system also known as the electronic voting system, the internet voting system, the SMS and Miss Calls Voting System, and others. We have explored numerous voting systems in this essay, along with their merits and demerits.

[5] The main objective of this study is to develop a voting system that can be used on several platforms and with any operating system. Any government or group may run elections using the online voting method since it is a versatile, platformindependent technology. A smartphone running any operating system with a barcode scanning function is all that is required of the user, along with a national identifying number, such as their Aadhaar card number. Due to the system's online nature, the user may vote from their present location. Voters can cast their ballots without physically going to a polling place, which encourages more people to vote.

[22] This study looked at the problems of limited access and voter impersonation during the 2018 Kabarak University student elections. Therefore, the major goal of this investigation was to modernize the electronic voting method in offline mode by creating a safe web-based voting platform

as well as implementing the same in time for Kabarak University's 2019 student elections.

For medium-sized online elections, the work described a secure electronic voting method in this study (SELES) [23]. While avoiding any private voting channels, our system successfully provides a safe and secure protocol for communication which paves the way for a secured voting process and prevents different frauds like double voting and other fraud activities. SELES achieves all the common characteristics of traditional voting systems, including precision, democracy, confidentiality, verifiability, ease of use, and adaptability, and identifies duplicate voting. SELES has also been built to handle communication errors, resulting in a certain level of robustness.

The primary goal of this essay [24] is to offer India a straightforward and secure mechanism for voting in elections. It is more secure than an internet voting system because it is app-based. This system makes use of the user fingerprints to identify the users uniquely, and fingerprint information is used to retrieve Aadhar information. The senior population, people with disabilities, patients, the military, and immigrants can all benefit from this material. Voting is open to everyone, regardless of location. Results will be made public as soon as the voting procedure is over. This contributes to the advancement of Make in India and Digitalize India.

To expand the number of voters participating in the election process, [25] this article proposes a novel online voting system for Indian government elections. The suggested strategy uses two strategies. 2) OTP (one-time-password) method, a novel potential verifiability mechanism The voter's identity can be verified by the candidate using the candidate verifiability in conjunction with the OTP, which serves as an additional authentication element.

B. Realized Disadvantages

Voting people in the currently prevailing method needs to visit the polling sites in person and need to record their votes in the ballot machines in a manual fashion. This manual process incurs increased time and there are chances for the casted votes to be rigged. Furthermore, the polling site workers are found to majorly influence the operation and effectiveness of the vote casting itself. Some of the other common disadvantages present in the existing works are said in the following pointers:

- Chance of frauds.
- Time-consuming.
- Difficult to handle.
- Expensive.
- Difficult to scale.

C. Recent Research Progress in the Voting Systems

With the prospects provided by verification supporting voting systems as in [26-32], the range of intrusion into any type of voting system was able to decrease. As a result, many research scholars have started shifting their interest toward the deployment of state-of-the-art methodologies like MLMachine Learning and DL- Deep Learning in this verificationsupporting voting system as in [33-37]. For instance, a university-specific safer voting structure was devised by [38] with a special concentration on the aspects of intelligent contracts as well as privacy, and [39] made use of the blockchain for enrolling the voting persons to ensure that nil unauthorized voting persons poll a vote and assure the uprightness of the stored data in the data center with due storage of the root hash onto the blockchain. Likewise, [40] made use of the QR-codes-empowered coded coting strategy for increasing the security prospects of the verification supporting voting systems without relying much on the trustworthiness of the voting persons polling the votes.

As the years passed on, the researchers started pioneering practically secure voting systems with special attention given to the requirements like receipt-freeness, convenience, eligibility, and privacy along with the verifiability which was already in force. By adopting these kinds of voting systems, it has become possible to create much protection imparting digitalized voting systems without compromising on functionality [41].

As an upgrade to the above instances of safeness ensuring voting systems, [42] devised a more promising solution for voting by inculcating the techs of bio-metrical identifications using the unique identities of fingerprints as well as the face.

III. METHODS

In this proposed section, we will discuss the mathematical models that can be used for the online voting system using face recognition with Harcascade and CNN. The proposed models will help to ensure the security and accuracy of the voting system.

One possible model for the online voting system is a probabilistic model. This model can be used to predict the probability of a voter's face matching with the database of registered voters. The model can take into account various factors such as the quality of the image, the angle of the face, and the lighting conditions. Another possible model is a machine learning model based on convolutional neural networks (CNN). CNNs have been proven to be effective in image recognition tasks and can be used to identify faces in images. The model can be trained on a large dataset of images of registered voters and can then be used to classify new images as either matching or not matching with the registered voters' database.

In the currently taken up deep learning & computer vision integrated smart voting system; we have attempted to create a much more protective web voting scenario that can be

free from illegal means alongside the smooth casting of votes by the voters. The server components of the proposed system contain an authority distribution that prevents the server from being able to rig the results. The proposed online voting technology is anticipated to boost the electoral system's transparency and dependability. It identifies people using computer vision techniques. Fig. 1 . represents the flow of the proposed methodology.

A. Facial Recognition

For the sake of authenticating the users via the properly functioning ID validation services, it is much essential to match the real-time face of the human beings with that of a video or image in the digital format (these videos and images are usually contained in the considered face database) by making use of a face pattern recognition system. The major functionality served by these kinds of systems is that they detect and quantify the attributes of any human face by interpreting the concerned video or image.

B. OpenCV Neural Network

A collection of Python bindings known as OpenCVPython was produced for the sake of sorting out the problems encountered while working with computer vision. A scientist named "Guido van Rossum" was responsible for the creation of a common purpose-serving programming language known as "Python". This programming language developed by him went on to become much famous owing to its simplicity and interpretable source code.

C. Password feature

As a basic security feature, we have enabled the voting system to record the voting in the major database of our nation's Commission established for Election if authenticated with the correct password, or else the vote will be void and won't be recorded in the major database of our nation's Commission established for Election. This is possible only after proper registration of the password for a voting person alongside other security aspects.

D. Advantages

The advantages of the proposed system are listed as follows:

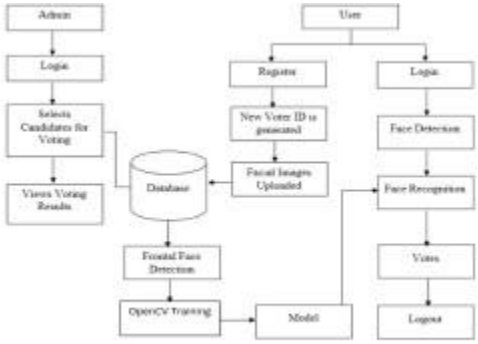

Fig. 1. The flow of the proposed methodology

- Time consumption is reduced.
- Fraud/gambling can be reduced.
- Privacy and security.
- Highly convenient.
- Easy to scale up.
- Inexpensive.

IV. RESULTS AND DISCUSSION

In this section, both the analysis and the result screenshots are presented.

A. Analysis

In this sub-section, we will present the quantitative, qualitative, and comparative analysis of the online voting system using face recognition with Harcascade and CNN.

1) Quantitative Analysis

The Deep Learning & Computer Vision Integrated Smart Voting System (DL-CV-IVS) is designed to automate the voting process using advanced technologies such as machine learning and computer vision. The following quantitative analysis can be used to evaluate the performance of the system:

- Accuracy: The accuracy of the systemcan be measured by comparing the results of the automated voting process with the manual voting process. The percentage of matching votes can be used to calculate the accuracy of the system.
- Speed: The speed of the DL-CV-IVS can be measured in terms of the time taken to complete the voting process. This can be compared with the time taken for manual voting to determine the efficiency of the system.
- Reliability: The reliability of the system can be measured by evaluating the number of errors and discrepancies in the voting results. The lower the number of errors, the higher the reliability of the system.

2) Qualitative Analysis

The qualitative analysis of the DL-CV-IVS can be based on the following factors:

- User Experience: The user experience of the DL-CVIVS can be evaluated based on how easy it is to use and¬ navigate the system. The system should have a userfriendly interface and clear instructions for users.
- Security: The security of the DL-CV-IVS is crucial in¬ ensuring the integrity of the voting process. The system should have measures in place to prevent unauthorized access and tampering of votes.

- Transparency: The DL-CV-IVS should provide¬ transparency in the voting process by allowing observers to monitor the process and providing access to voting results.

3) Comparative Analysis

To evaluate the effectiveness of the DL-CV-IVS, a comparative analysis can be done by comparing the system with traditional manual voting systems. The following factors can be used for the comparison:

- Accuracy: The accuracy of the DL-CV-IVS can be¬ compared with the accuracy of manual voting systems.
- Speed: The speed of the DL-CV-IVS can be compared¬ with the speed of manual voting systems. Reliability: The reliability of the DL-CV-IVS can be¬ compared with the reliability of manual voting systems.
- User Experience: The user experience of the DL-CVIVS can be compared with the user experience of¬ manual voting systems. Security: The security of the DL-CV-IVS can be¬ compared with the security of manual voting systems.
- Transparency: The transparency of the DL-CV-IVS can¬ be compared with the transparency of manual voting systems.

The results of the comparative analysis can help determine the advantages and disadvantages of using the DL-CV-IVS over traditional manual voting systems.

4) Numeric Validation

To justify the novelty of the Deep Learning & Computer Vision Integrated Smart Voting System (DL-CV-IVS) compared to traditional manual voting systems, statistical analysis (numeric validation) is conducted on data collected from both systems. These statistical comparisons are deduced with regards to the same metrics as accuracy, speed, reliability, user experience, security, and transparency. With this numeric validation conducted by us, the devised Deep Learning & Computer Vision Integrated Smart Voting System was found to be effective than the manually operated ones.

B. Result Screenshots

The results screenshots of the proposed smart voting system are provided in this section.

Fig. 2. portrays the screenshot of the home page of the proposed smart voting system. The home page of the smart voting system consists of three different options such as administrator, user registration, and update details

Fig. 2. Screenshot of the Home Page

The system's primary administrator is the person in charge. Fig. 3. depicts the screenshot of the admin login page. It can be seen from the following figure that the admin can log in to the smart voting system by entering the appropriate email id and password.

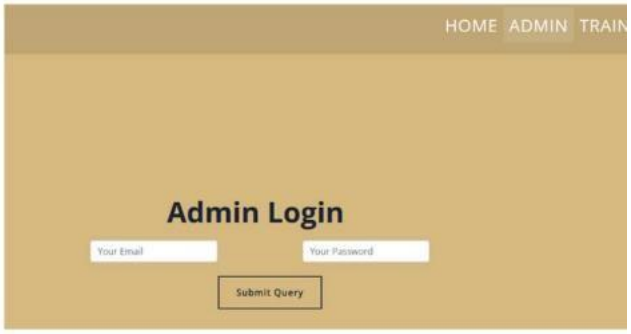

Fig. 3. Screenshot of the Admin Login Page

The main functions of the admin are:

- Login: Log into the system.
- View: Examine the outcomes of the vote.
- Logout: He logs off of the system once the procedure is finished.

Fig. 4. represents the screenshot of the admin controls page. It can be seen from the figure that the admin is taken to this page after logging in. Here, the administrator is given two different controls such as new nominee and view results.

Fig. 4. Screenshot of the Admin Controls Page

Fig. 5. gives the screenshot of the add new nominee page. The admin is taken to this page after selecting the new

nominee control. Here the admin can add new nominees which is nothing but the selection of new candidates who will be contesting for the election. As seen from the figure, the nominee can be added by mentioning the name of the contesting candidate, the name of the party, and selecting the symbol of the party.

Fig. 5. Screenshot of the New Nominee Page

Fig. 6 shows the screenshot of the new voter registration page. The user is the potential voter, often known as an interested party. The voter can be registered in the smart voting system by giving respective fields like first name, middle name, last name, Aadhaar number, voter id, and email id as shown in the below figure. Then email verification must be done after entering the details for the successful registration of the voter.

Fig. 6. Screenshot of the New Voter Registration Page

Fig. 7. provides the screenshot of the update page. The voters can update their details if any changes exist. Similar to the registration process, the voter can update the details in the smart voting system by giving respective fields like first name, middle name, last name, Aadhaar number, voter id, and email id as shown in the below figure. Then email verification must be done after entering the details for the successful updation of the voter details.

Fig. 7. Screenshot of the Update Page

Fig. 8 indicates the screenshot of the model training page. After the data is collected, click on the train option in the top right corner of the page for model training as shown in the following figure. The training of the model might take some time to complete. Once the training of the model is completed, the page will be automatically redirected to the home page.

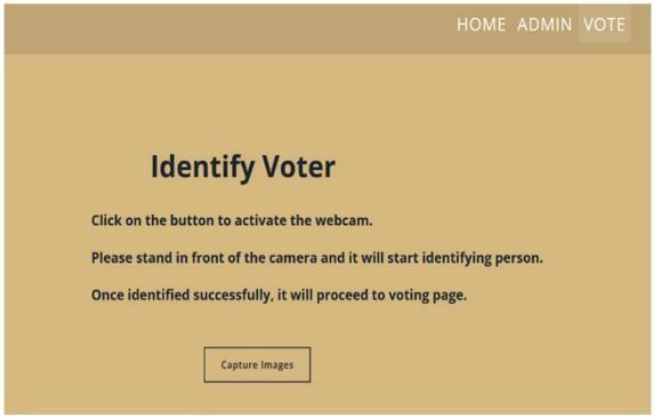

Fig. 8. Screenshot of the Model Training Page

Fig. 9. represents the screenshot of the voter detection page. The voter should stand in front of the webcam since the smart voting system demands the voter to enter the face for accessing the smart voting system. The voter is taken to the voting page only after the successful identification of the voter.

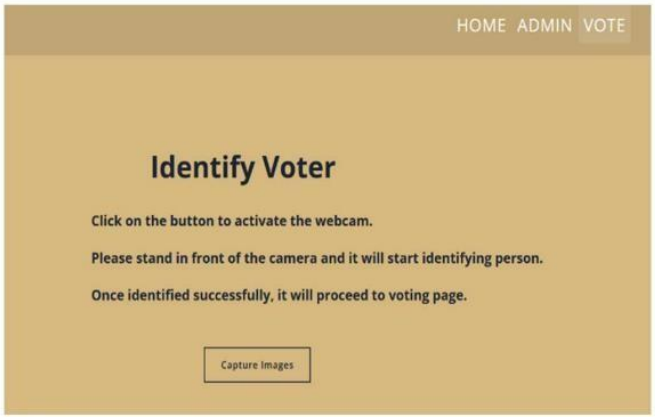

Fig. 9. Screenshot of the Voter Detection Page

By implementing a new registration feature that takes in frontal facial images, you are likely to improve the security and accuracy of the system. This is because facial recognition is a reliable and difficult-to-forge method of authentication. By training the models again after each new registration, you are ensuring that the system can accurately detect and recognize each new user.

V. CONCLUSION

We've created a working online voting system by making the user interface with Flask and Python. Computer vision was used in both photo pre-processing and video streaming. The system had showed a new registration feature

that takes frontal selfies of the individual enrolling. The user should utilize a One-Time Password to confirm their email IDs to finish the process of registration. The administrator had retrained the models to detect and recognize the new user after registration. As a result, nobody would be able to cast more than one vote. Unless they have already voted, a registration was allowed to be finished, thereby recognition of the user was made possible based on the facial attributes. Frontal Face Haarcascading is used to create facial embeddings.

REFERENCE
S

1) A. Rodríguez-Pérez, "Secret suffrage in remote electronic voting systems," in 2017 Fourth International Conference on eDemocracy & eGovernment (ICEDEG), 2017, pp. 277-278: IEEE
2) A. Jagtap, V. Kesarkar, and A. Supekar, "Electronic voting system using biometrics, raspberry pi and TFT module," in 2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI), 2019, pp. 977-982: IEEE.
3) F. Þ. Hjálmarsson, G. K. Hreiðarsson, M. Hamdaqa, and G. Hjálmtýsson, "Blockchain-based e-voting system," in 2018 IEEE 11th international conference on cloud computing (CLOUD), 2018, pp. 983-986: IEEE.
4) R. Rezwan, H. Ahmed, M. Biplob, S. Shuvo, and M. A. Rahman, "Biometrically secured electronic voting machine," in 2017 IEEE Region 10 Humanitarian Technology Conference (R10-HTC), 2017, pp. 510-512: IEEE.
5) Z. Usmani, K. Patanwala, M. Panigrahi, and A. Nair, "Multi-purpose platform independent online voting system," in 2017 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), 2017, pp. 1-5: IEEE.
6) D. J. I. s. Chaum and privacy, "Secret-ballot receipts: True voterverifiable elec
7) O. S. o. State, "https://verifiedvoting.org/wp-content/uploads/2020/08/01-compuware112103.pdf," (Accessed January 25, 2023), 2023.
8) J. Daemen, V. Rijmen, J. Daemen, and V. J. T. D. o. R. A. T. A. E. S.Rijmen, "The advanced encryption standard process," pp. 1-8, 2002.
9) S. K. Nikodimos Eustathiou, Stavros Valsamidis, Alexandros Karakos∗, "https://spooky.math.uoi.gr/~skontog/papers/duthtr-05-08.pdf," (Accessed on January 25, 2023), 2023.
10) D. L. Dill, R. Mercuri, P. Neumann, and D. J. V. V. Wallach,"Frequently Asked Questions about DRE Voting Systems," 2003.
11) F.E.Commission"https://www.fec.gov/resources/updates/agendas/2001/mtgdoc01-62/v1/v1s3.pdf," (Accessed on January 25, 2023), 2023.
12) E. F. Foundation, "Cracking DES: Secrets of encryption research,wiretap politics and chip design," ed: O'Reilly & Associates, Inc., 1998.
13) C. Lambrinoudakis, D. Gritzalis, V. Tsoumas, M. Karyda, and S.Ikonomopoulos, "Secure electronic voting: The current landscape," inSecure electronic voting: Springer, 2003, pp. 101-122.

14) B. Harris, Black box voting: Ballot tampering in the 21st century.Aware Journalism, 2004.
15) D. J. W. D. h. h. d. u. e. Jones, "Problems with Voting Systems and the Applicable Standards. Testimony before the US House of Representatives Committee on Science," 2001.
16) D. W. J. T. U. O. I. D. o. C. S. Jones, "The case of the Diebold FTP site," 2003.
17) A. J. J. d. s. m. Kerckhoffs, "A. Kerckhoffs, la cryptographie militaire, Journal des Sciences Militaires IX, 38 (1883)," vol. 9, p. 38, 1883.
18) H. Krawczyk, "The order of encryption and authentication for protecting communications (or: How secure is SSL?)," in Annual International Cryptology Conference, 2001, pp. 310-331: Springer.
19) R. T. Mercuri, Electronic vote tabulation checks and balances.University of Pennsylvania, 2001.
20) T. Kohno, A. Stubblefield, A. D. Rubin, and D. S. Wallach, "Analysis of an electronic voting system," in IEEE Symposium on Security and Privacy, 2004. Proceedings. 2004, 2004, pp. 27-40: IEEE.
21) T. Jim, J. G. Morrisett, D. Grossman, M. W. Hicks, J. Cheney, and Y.Wang, "Cyclone: a safe dialect of C," in USENIX Annual Technical Conference, General Track, 2002, pp. 275-288.
22) M. M. THIGA, "Increasing Participation and Security in Student Elections through Online Voting: The Case of Kabarak University," in 2020 IST-Africa Conference (IST-Africa), 2020, pp. 1-7: IEEE.
23) C. Garcia-Zamora, F. Rodriguez-Henriquez, and D. Ortiz-Arroyo, "SELES: an e-voting system for medium scale online election," in Sixth Mexican International Conference on Computer Science (ENC'05), 2005, pp. 50-57: IEEE.
24) B. Madhuri, M. Adarsha, K. Pradhyumna, and B. Prajwal, "Secured smart voting system using aadhar," in 2017 2nd international conference on emerging computation and information technologies (ICECIT), 2017, pp. 1-3: IEEE.
25) G. Manikandan, G. Anandaraju, and B. Karthikeyan, "A Candidate Aware Internet Voting System For Indian Scenario," in 2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS), 2020, pp. 783-786: IEEE.
26) J. Weber and U. J. R. A. Hengartner, "Usability study of the open audit voting system helios," vol. 3, p. 2012, 2009.
27) K. Gjøsteen and A. S. J. A. o. T. Lund, "An experiment on the security of the Norwegian electronic voting protocol," vol. 71, pp. 299-307,2016.
28) K. Marky, O. Kulyk, K. Renaud, and M. Volkamer, "What did I really vote for? On the usability of verifiable e-voting schemes," in Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems, 2018, pp. 1-13.
29) C. Z. Acemyan, P. Kortum, M. D. Byrne, and D. S. J. H. f. Wallach,"Summative usability assessments of STAR-Vote: a cryptographically secure e2e voting system that has been empirically proven to be easy to use," vol. 64, no. 5, pp. 866-889, 2022.
30) V. Distler, M.-L. Zollinger, C. Lallemand, P. Roenne, P. Ryan, and V. Koenig, "Security–visible, yet unseen? how displaying security mechanisms impacts user experience

and perceived security," in Proceedings of ACM CHI Conference on Human Factors in Computing Systems (CHI2019), 2019.

31) K. Marky, M.-L. Zollinger, P. Roenne, P. Y. Ryan, T. Grube, and K. J. A. T. o. C.-H. I. Kunze, "Investigating usability and user experience of individually verifiable internet voting schemes," vol. 28, no. 5, pp. 1-36, 2021.
32) O. Kulyk, M. Volkamer, M. Müller, and K. Renaud, "Towards improving the efficacy of code-based verification in internet voting,"in Financial Cryptography and Data Security: FC 2020 International Workshops, AsiaUSEC, CoDeFi, VOTING, and WTSC, Kota Kinabalu, Malaysia, February 14, 2020, Revised Selected Papers 24,2020, pp. 291-309: Springer.