ISSN: 2147-5121 / E-ISSN: 2717-7610

İstanbul Nişantaşı Üniversitesi
Sosyal Bilimler Dergisi

Bilimsel Hakemli Dergi

Yıl: 2024 Cilt: 12 Sayı: 2

İSTANBUL NİŞANTAŞI UNIVERSITY NEW
NUSBD

Yayın Aralığı: Yılda 2 Sayı - Başlangıç: 2013

İstanbul Nişantaşı University
Journal of Social Sciences

Scientific Refereed Journal

Year: 2024 Vol.: 12 No: 2

ARAŞTIRMA MAKALESİ / RESEARCH ARTICLE

DOI: 10.52122/nisantasisbd.1478942

# ASSESSING THE UNRELIABILITY OF ONLINE POLITICAL POLLS: A NOVEL SOFTWARE FOR VOTING APPROACH

**Dr. Öğr. Üyesi Murat IŞIK**

Kırşehir Ahi Evran Üniversitesi

e-posta: muratisik@ahievran.edu.tr

ORCID 0000-0003-3200-1609

**Dr. Öğr. Üyesi Mehmet Ali YALÇINKAYA**

Kırşehir Ahi Evran Üniversitesi

e-posta: mehmetyalcinkaya@ahievran.edu.tr

ORCID 0000-0002-7320-5643

## ABSTRACT

In recent years, the utilization of online polls for political opinion sampling has become prevalent due to their cost-effectiveness and rapid deployment. However, their reliability is frequently questioned due to vulnerabilities inherent in their digital nature. This study explores the susceptibility of online polls to manipulation by examining the efficacy of various security measures employed across 160 online polling platforms during the 2024 municipal elections in Turkey. Using an automated voting application developed for this study on these platforms, a total of 10,000 votes were cast on the subject sites over 143 hours, bypassing 2,547 CAPTCHAs, 5,854 digital fingerprints, and 1,559 Internet Protocol (IP) address verifications, significant security flaws were uncovered. The findings reveal that while measures such as CAPTCHA, digital fingerprinting, and IP validation offer some resistance, they are not foolproof. It is concluded that the most robust method involves verifying users via the e-government platform, enhancing both the credibility and integrity of online polls. This study not only highlights the vulnerabilities of current online polling practices but also provides a roadmap for enhancing security to better reflect genuine public opinion and foster more trustworthy political decision-making processes.

**Anahtar Kelimeler:** online polls, digital fingerprint, IP validation, automatic votes.

**Jel Kodları:** C88, L86.

# ÇEVRİMİÇİ SİYASİ ANKETLERİN GÜVENİLİRLİĞİNİN DEĞERLENDİRİLMESİ: YENİ BİR OYLAMA YAZILIMI KULLANIMI

## ÖZ

Son yıllarda, maliyet avantajı ve hızlı uygulanabilirliği nedeniyle siyasi görüş örneklemesi için çevrimiçi anketlerin kullanımı yaygınlaşmıştır. Ancak, bu anketlerin dijital ortamda olmasından kaynaklanan zaaflar nedeniyle güvenilirlikleri sıklıkla sorgulanmaktadır. Bu çalışma, Türkiye'deki 2024 yerel seçimleri sırasında 160 çevrimiçi anket platformunda uygulanan çeşitli güvenlik önlemlerinin etkinliğini inceleyerek çevrimiçi anketlerin manipülasyona ne kadar açık olduğunu araştırmaktadır. Çalışma kapsamında geliştirilen bir oylama uygulaması ile çalışmaya konu olan sitelerde 143 saatte, 2,547 CAPTCHA, 5,854 dijital parmak izi ve 1,559 IP doğrulaması aşılarak toplamda 10.000 adet oy kullanılmıştır. Bulgular, CAPTCHA, dijital parmak izi ve IP (İnternet Protolü) adresi doğrulama gibi önlemlerin bir miktar direnç sunduğunu, ancak bunların da kusursuz olmadığını ortaya koymaktadır. En güçlü yöntemin kullanıcıların e-devlet platformu üzerinden doğrulanması olduğu sonucuna varılmıştır. Bu çalışma, mevcut çevrimiçi anket uygulamalarının zaaflarını vurgulamakla kalmamakta, aynı zamanda kamuoyunun gerçek fikirlerinin daha iyi yansıtılabilmesi ve daha güvenilir siyasi kararlar alma süreçleri için bir yol haritası sunmaktadır.

**Keywords:** çevrimiçi anketler, dijital parmak izi, IP doğrulama, otomatik oylama

**Jel Codes:** C88, L86.

**Geliş Tarihi/Received:** 05.05.2024 | **Kabul Tarihi/Accepted:** 28.09.2024 | **Yayım Tarihi/Printed Date:** 31.12.2024

**Kaynak Gösterme:** Işık, M. ve Yalçınkaya M.A. (2024). "Assessıng The Unrelıabılıty Of Onlıne Polıtıcal Polls: A Novel Software For Votıng Approach". *İstanbul Nişantaşı Üniversitesi Sosyal Bilimler Dergisi*, 2(12) 539-552.

## GİRİŞ

In Turkey, political parties use online polls for public opinion during the candidate selection process. Almost every city and district sometimes conducts one or multiple polls. Online polls can be defined as online surveys of public opinion, or a sample thereof, aimed at acquiring information about specific topics (Basso and Miraglia, 2008: 149). In the age of digital democracy, online political polls have emerged as pivotal tools for gauging public opinion on a myriad of political issues (Martin and Geiger, 1999: 15; Pekar et al., 2022: 1; Stantcheva, 2023: 205; Yudin, 2020: 2). These polls are often heralded for their ability to quickly and efficiently collect data from a broad audience, potentially offering insights into the political landscape that traditional polling methods might miss. In Turkey, online polls are utilized prior to the candidate selection process by political parties during preliminary candidate nomination phases. Throughout this phase, a significant portion of online local news outlets, alongside prominent online news platforms and specialized websites, administer polls with the intent of discerning public sentiment. Subsequently, certain platforms transform these polls into formal election polls.

While the migration of public opinion polls to online platforms has often lowered costs and enhanced timeliness, it has also introduced new vulnerabilities (Kennedy et al., 2021: 1050). The reliability of online political polls has come under scrutiny due to concerns about sampling biases, the anonymity of the internet, and the ease with which results can be manipulated or misrepresented. The allure of online political polls lies in their accessibility and the immediacy with which they can capture shifts in public opinion. As the internet has become increasingly integrated into daily life, researchers and political strategists have turned to online platforms as a viable alternative to traditional polls (Hargittai and Karaoglu, 2018: 2). Yet, this shift towards digital polling methods brings with it a host of challenges that threaten the accuracy and credibility of their findings.

Moreover, the perceived credibility of online polls and the way they are reported in the media play a significant role in shaping public trust and engagement with these tools. Greater transparency and methodological rigor are needed in the conduct and presentation of online polls to ensure they contribute constructively to the democratic process. In light of these challenges, it is imperative to critically evaluate the reliability of online political polls and to develop standards and practices that enhance their accuracy and trustworthiness. In this study, 10,000 votes were automatically applied to 160 online political polls during the 2024 municipal elections in Turkey. Following this successful voting process, conclusions were drawn regarding necessary measures to increase trust in online political polls.

The study has two primary objectives. The first is to demonstrate that online polls for collecting public opinions are vulnerable to attacks and can be easily manipulated. The second is to propose measures for securely gauging public opinion without manipulation during the candidate selection process in elections.

### 1. Related Works

Yeargain (2020) demonstrates that fake polls are increasingly prevalent online, aiming to manipulate political betting markets. This manipulation allows their creators to profit from the misinformation at the expense of those deceived.

Mohammadi and Abbasimehr (2010) show that polls can suffer from a variety of attacks, such as those using automated web tools to alter results. They concluded that the security of Internet polls must be enhanced to increase the reliability of their outcomes. Their proposed method involves using CAPTCHA validation.

Qureshi et al. (2019) proposed a new e-polling system, SeVEP, to mitigate security risks. Their system features flexible polling, device fingerprinting for multifactor authentication across various voter devices, zero-watermarking of polling code sheets, and the generation of polling tags. However, the requirement for authentication factors (possession, biometric) necessitates additional time and the installation of programs on voter devices. They also implement a random 3-digit code selected by the user to preserve voter privacy.

Prabhu et al. (2021) propose a new smart embedded voting system as an alternative to traditional official election polls. Their system, based on the Arduino platform, allows users to vote either online or offline. For offline voting, users must present an official ID card equipped with RFID. Online voting utilizes face recognition technology.

Natarjan and et al. (2024) introduce a solution that uses both Android and web applications to securely store and verify voter identities, addressing the increased vulnerability to fraudulent election practices. The process includes a One-Time Password (OTP) authentication mechanism with the voter's unique ID for login, which is cross-checked with a centralized database. Additionally, an admin-generated OTP provides an extra layer of verification.

Mondal et al. (2023) proposed a Referendum Poll System (RPS) based on blockchain technology. Their aim is to enable people to express their opinions directly, re-engaging them with politics and democracy. The process involves voter registration using cryptocurrency wallet systems and biometric ID.

Sivasakthi et al. (2021) proposed a web application using MongoDB, Express, React, and Node for the voting process instead of electronic voting machines. Voter verification is based on a secret PIN provided by the election commission. The designed program is intended for use in real voting. Every voter needs a PIN to vote.

Sai and Kumar (2022) designed a new online voting application using Java and SQL. A user logs in to this online voting process by providing their first name, last name, email address, password, and thumbprint.

In the related literature, various online voting processes employing different systems have been documented (Das et al., 2016; Shalini et al., 2020); however, these introduce distinct security vulnerabilities (Park et al., 2021). In this study, security measures employed by 160 online polling sites were examined, and an automated voting software capable of bypassing these measures was developed. The objective of this study is to demonstrate that the accuracy of such online polls is quite low and to present possible security enhancements.

## 2. Manipulating Online Polls

The methods for casting fraudulent votes in polls can be categorized into two classes: Chatrooms and Bots. This study is predicated focusing on bots.

Chatroom: Certain unethical entities provide a substantial influx of votes by utilizing chatrooms, wherein multiple devices are present and concurrently operated by a singular software application. Figure 1 illustrates a chatroom that has been constituted through the employment of multiple mobile devices.

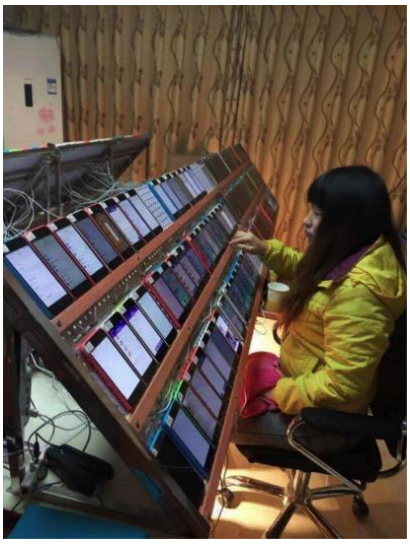

**Figure 1:** Chatrooms (Köse, 2019)

In these chatrooms, all devices can be controlled by a user via a specific software, which replicates a specific action across all devices. Consequently, this mechanism enables the realization of a significant number of votes in the polls.

Bots: Automated poll completion methodologies which act like human users in order to vote repeatedly (Basso and Miraglia, 2008: 149) are engineered to enhance the efficacy and streamline the data collection process across diverse fields. These methodologies employ advanced software solutions to automate the response mechanism to polls, thereby diminishing the requisite time and labor for manual intervention. The technological infrastructure underpinning these systems encompasses a broad spectrum, ranging from web-based applications and mobile device integration to sophisticated algorithms dedicated to the analysis and interpretation of poll data.

Of course, there could be many security measures to prevent the bots. In this study, all security measures encountered during the participation in 160 online polls will be delineated, alongside the methodologies employed to surmount these obstacles. Furthermore, this study will propose a criterion for the standardization of online poll methodologies.

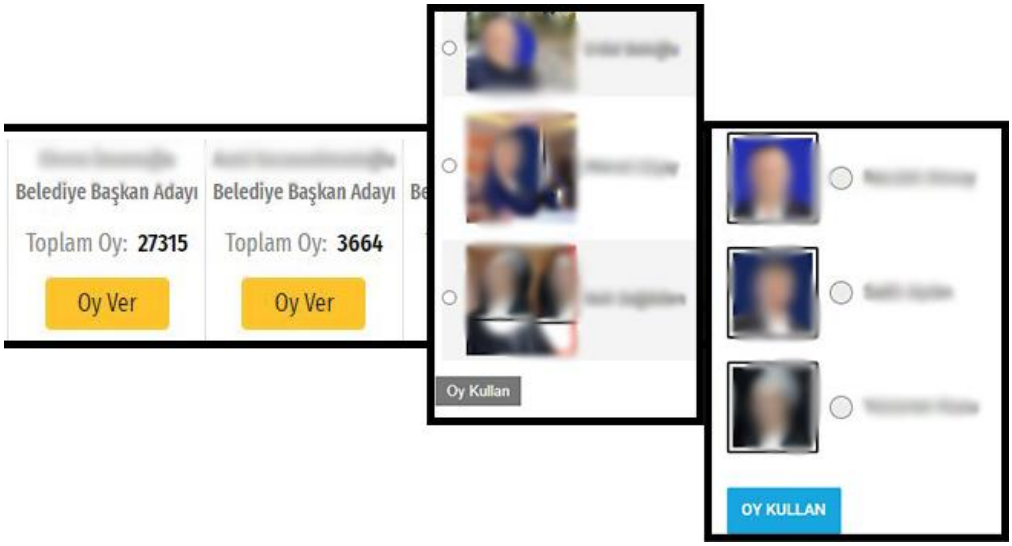


**Figure 2:** Screenshots from some polls

Figure 2 displays sample screenshots from some online political polls. From the figure and the source codes of the pages, it can easily be observed that the general structure is nearly identical across all, comprising a list of candidates and a voting button triggered by JavaScript functions. All of the 160 online poll sites examined contain at least one of the previously discussed security measures. The design of these polls aims not only to secure the voting process but also to encourage engagement from a broad user base. The application of compulsory CAPTCHA with each website visit can sometimes be irritating. Here, a balance must be carefully maintained between preventing the same individual from voting multiple times and enabling rapid voting, so that a greater number of participants can complete the poll.

## 3. Method

An application was developed to automate voting and manipulate online political polls in Turkey during the 2024 municipal elections. The selection of the 160 online polling platforms analyzed in this study was based on their popularity and frequent usage, both at the national and local levels. Platforms with the highest voting activity were utilized to ensure a representative sample. These endeavors pursued two primary objectives: firstly, to demonstrate the unreliability of online political polls, and secondly, to propose standards to enhance the credibility of these

online polls. In the process of automatically casting votes in online polls, the encountered security measures are listed below.

- Digital Fingerprint validation: Digital fingerprints can be understood as remnants of information that we unwittingly leave behind while navigating the online sphere. Digital fingerprints function as unique identifiers that enable the identification and monitoring of individuals' online behaviors. Digital fingerprints encompass a collection of data that serves as a unique identifier, derived from the characteristics and preferences of the web browser being utilized. Such information may include details like the browser version, installed plugins, the availability of specific fonts (Iqbal et al., 2021: 1145 ve 1147; Laperdrix et al., 2020: 4 ve 5; Fifield and Egelman, 2015: 4), Cookies (Boda et al., 2012: 33 ve 34), IP address (Nikiforakis et al., 2013: 544 ve 545), port configurations, communication data, user account associated with the device, including the username and user ID (Nikiforakis et al., 2013: 546), operating system details (Anderson and McGrew, 2017: 3 ve 4) such as its version and architecture and so on.
- Captcha validation: CAPTCHA is an acronym that stands for "Completely Automated Public Turing test to tell Computers and Humans Apart". It is designed to determine if an online user is really a human or a bot.
- IP validation: Despite IP validation constituting an element of the digital fingerprint framework, it is observed that some online polls resort solely to IP verification instead of utilizing the full scope of the digital fingerprint. The underlying intention of this approach is to prevent an IP that has voted successfully from casting another vote for a specified duration.

Throughout the development stage of the software, the Python programming language was utilized, incorporating the BeautifulSoup and Selenium libraries for its construction. The Google Chrome browser was chosen for web interaction. The algorithmic operation of the software is illustrated in Figure 3, delineating its procedural logic. The configuration of the software's workflow is tailored to comply with the security protocols implemented on the polling website. Additionally, the time spent submitting a vote is subject to variation based on the specific webpage in question.

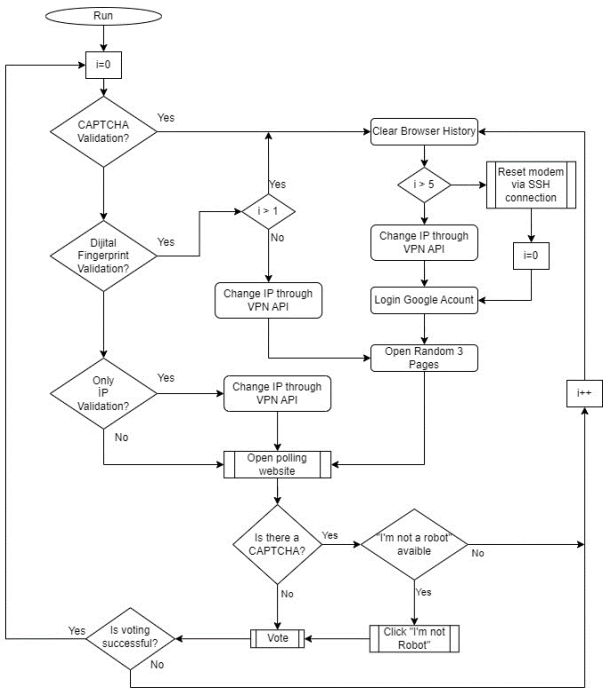


**Figure 3:** The algorithmic operation of the software after users' actions recorded

Upon its initial execution, the developed program requires a one-time record. That is, once the user runs the program and casts a vote for the desired candidate, the system will thereafter operate automatically. The flowchart presented in Figure 3 illustrates the process following the registration. The very first step after users' actions recorded that is not presented in the chart is to determine if the web site uses CAPTCHA validation or Digital Fingerprint validation or IP validation.

The program is designed to pause for a random duration of 2-8 seconds between each workflow step. In phases entailing the alteration of IP addresses, it has been ensured that the newly acquired IP addresses originate from Turkey. For the process steps where three web pages are to be opened randomly, a list of URLs has been prepared. This list contains three groups of web addresses: the first group consists of sites with a .gov extension, the second group includes sites with an .edu extension, and the final group comprises sites with a .com extension that contain an HTML form. In the final part of the step where three web pages are opened, the relevant form entry is filled out and submitted, thereby ensuring the augmentation of browser cookies with specified datasets.

For CAPTCHA validation, at every iteration, the browser history is cleared, and a new IP address is obtained to generate a new digital identity. Subsequently, a login to a Google account is performed, and three web pages from a pre-prepared list are randomly opened. For Digital Fingerprint validation, it is not necessary to clear the browser history every time. The process comprises two subsequent steps: changing the IP address and opening three random websites. In the context of IP validation, the process involves only changing the IP address. The spent time for each vote process varies are depending on the web address where the poll is hosted and the security measures that the web site implemented. If the voting process has been attempted more than five times and has failed, a reset is initiated by establishing an SSH connection to the modem.

```
try:
    # Stage - 1
    options = webdriver.ChromeOptions()
    options.binary_location = operaLocation
    options.add_experimental_option('w3c', True)
    driver = webdriver.Opera(executable_path=driverLocation, options=options)
    time.sleep(round(random.uniform(2,8), 0))

    driver.get(self.url)
    time.sleep(round(random.uniform(2,8), 0))

    scriptToRun = getTheScript()

    driver.execute_script(scriptToRun)
    time.sleep(round(random.uniform(2,8), 0))

    driver.quit()
```

```
import time
from selenium import webdriver
from selenium.webdriver.chrome import service
from selenium.webdriver.common.by import By

webdriver_service = service.Service(driverLocation)
webdriver_service.start()

options = webdriver.ChromeOptions()
options.add_argument('user-data-dir=' + profileLocation)
options.binary_location = operaLocation
options.add_experimental_option('w3c', True)

driver = webdriver.Remote(webdriver_service.service_url, options=options)

linkToProcess = getTheLink()

driver.get(linkToProcess)

recordTheProcess()

time.sleep(round(random.uniform(2,8), 0))
driver.quit()
```

**Figure 4:** The code blocks from the program – 1

Figure 4 shows a code block from the designed program. The left side of the code block is used to cast a vote for the desired candidate and is triggered after CAPTCHA validation is successfully passed. The right side of the code block is used to start the recording process of voting. The application runs in the command line, so all the results are printed there.

```python
VPN_API_URL = "************"
API_KEY = "**********"
VPN_SERVER_LOCATION = randomLocation()

def authenticate_vpn(api_key):
    response = requests.post(f"{VPN_API_URL}/authenticate", data={"api_key": api_key})
    response.raise_for_status()
    return response.json()["token"]

def connect_vpn(token, location):
    headers = {"Authorization": f"Bearer {token}"}
    response = requests.post(f"{VPN_API_URL}/connect", headers=headers, data={"location": location})
    response.raise_for_status()
    return response.json()["ip"]
```

**Figure 5:** The code blocks from the program – 2

Figure 5 shows another code block from the designed program. This block is used to change the IP number through a Virtual Private Network (VPN) Application Programming Interface (API). A VPN service that provides a command-line interface (CLI) and easily integrates with Python was purchased for the study. The code block shows only a part of the VPN connection functions.

## 4. Results

In this study, 10000 votes have been automatically applied to 160 online political polls during 2024 municipal elections in Turkey. The objective of the online polls examined in this study is to collect data on public opinions during the candidate nomination phase, thereby facilitating the transition from prospective to officially nominated candidates. For this reason, after the mayoral candidates were determined, the voting process was conducted in a manner that maintained a proportional balance among the candidates.

**Table 1.** Evaluation of Online Voting Process

| | CAPTCHA | Digital Fingerprint | IP Validation | Total |
|---|---|---|---|---|
| Number of Polls | 62 | 66 | 32 | 160 |
| Unsuccessful Votes | 6559 | 1463 | 332 | 8354 |
| Successful Votes | 2587 | 5854 | 1559 | 10000 |
| Reset through SSH | 2174 | 630 | 32 | 2836 |
| Average Vote Time (sec) | 97 | 39 | 28 | 164 |
| Total Vote Time (hr) | 70 | 61 | 12 | 143 |

Table 1 presents an evaluation of the online voting process through an analysis of 160 online political polls. Among these, CAPTCHA was utilized in 62 polls, Digital Fingerprint in 66 polls, and IP Validation in 32 polls. The count of unsuccessful votes indicates the number of votes blocked due to the security measures of the polls. The number of resets through SSH connections reflects the instances where the modem had to be reset, in that situation the process that significantly delayed because of the establishment of a new internet connection. The Average Vote Time, measured in seconds, was calculated by dividing the total time spent by the number of successful votes. The Total Vote Time, presented in hours, indicates the total time spent on the voting process.

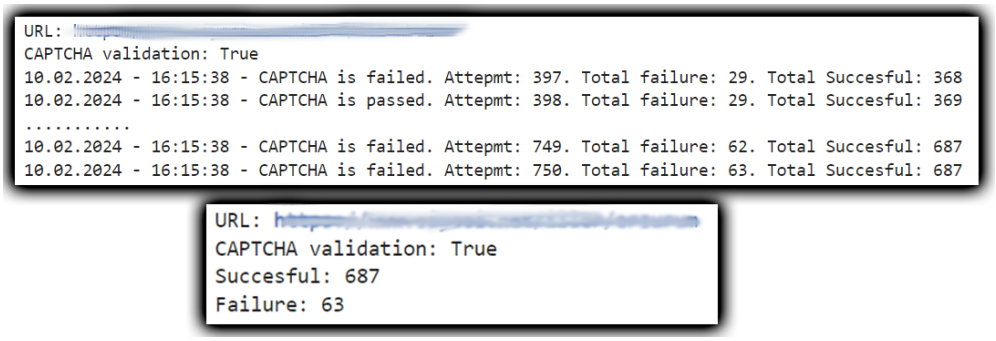


**Figure 6:** The command line output from the program

Figure 6 presents a command line output of the program for an online polling website. The output at the top of the figure shows the printed output produced by the program on the command line during its execution. It should be noted that the voting process is a repetition of the previously recorded voting process. Therefore, the output here indicates the number of successful or failed attempts after the automatic voting procedure is started. Additionally, the output also shows that the online poll uses CAPTCHA protection. The output at the bottom of the figure shows the results after the desired number of trials or successful votes are reached for the specific online poll.

## 5. Discussions

First and foremost, the fact that a total of 10,000 votes could be cast within 143 hours using just a single computer demonstrates that the 160 online survey sites examined are considerably insecure. Utilizing such polls for public opinion polling and in the determination of candidates from among prospective nominees is highly unreliable. Indeed, this study illustrates that online surveys can easily be manipulated. Furthermore, if the study were to continue using several computers, the number of votes that could be utilized would reach colossal proportions.

The most challenging security method encountered was CAPTCHA verification. However, such verification methods are generally controlled by a threshold value. Setting the threshold value too high requires verification at every user entry, while setting it too low allows entries with almost no verification. Yet, even with a high threshold setting, there are many ways to circumvent it (Gajani et al., 2023; Shao et al., 2022; Tsingenopoulos et al., 2022; Wang et al., 2023; Wang and Lu, 2016). This indicates that CAPTCHA cannot serve as the ultimate verification method on online poll websites.

Another challenge encountered is the Digital Fingerprint. However, the name looks very secure, the method consists of some specific features of operating system or web browser such as operating system info, browser type, screen resolution, installed fonts and plugins etc. The fundamental characteristics used in the creation of a digital fingerprint can very easily be altered instantaneously. In this study, by merely changing a few parts of these characteristics, this security method could be bypassed. In cases where this proves insufficient, altering additional features will readily overcome this security measure.

The simplest protection method encountered was IP validation. It was found to be possible to renew the IP address using simple VPN API. At this stage, it was observed that the IP addresses used sometimes appeared several times in succession. However, such occurrences were encountered infrequently enough to be considered negligible. Without establishing certain standards, the use of such polls for public opinion assessments can be significantly misleading and unreliable. This study explores four distinct methods designed to ensure that each individual casts only one vote.

1. Restricting voting privileges exclusively to registered users.
2. Implementing verification via SMS.
3. Employing a verification process through an official platform such as e-government.

4. Recording the MAC address.

Implementing robust security measures and maximizing user reach in online polls involves a trade-off. To encourage broader participation, these polls must balance the rigor of security protocols with the time required for voting. In this context, restricting access to registered users is particularly disadvantageous—a drawback that is sequentially followed by SMS verification and then the e-government verification method. Moreover, the potential for being profiled through these methods may deter users from participating in the voting process. The final method, recording the MAC address, requires downloading and executing an external program on the user's device during the voting process, as obtaining the MAC address is otherwise unfeasible. Besides the complexity and perceived insecurity of this process, it is crucial to recognize that the primary utility of recording the MAC address is to prevent multiple votes from the same machine rather than from the same individual.

**Tablo 2.** The key points of similar studies

| No | Study | Key Point |
|---|---|---|
| 1 | (Natarajan, 2024) | They used an Android app and web applications to securely store and verify voter identities. Their system requires a One-Time Password (OTP) using the voter's ID. |
| 2 | (Mondal et al., 2023) | The study is based on blockchain technology and requires a registration process that includes biometric ID and a cryptology wallet. |
| 3 | (Sivasakthi et al., 2021) | They proposed a web application. Every voter needs a PIN from voiting comitee to vote. |
| 4 | (Sai and Kumar, 2022) | They designed an applicaiton using Java and SQL. Every voter needs to login using first name, last name, email address, password, and thumbprint to vote |
| 5 | (Qureshi et al., 2019) | They proposed a new e-polling system, SeVEP. The user validation needs biometric data of the voter and a program has to be installed to user device. |
| 6 | (Prabhu et al., 2021) | They designed a new smart embedded voting system using Arduino platform. The verification process utilizes official ID card equipped with RFID and face recognition technology. |
| 7 | (Mohammadi and Abbasimehr, 2010) | In the study, they stated that online polls can suffer from a variety of attacks. They proposed using using CAPTCHA validation. |
| 8 | (Yeargain, 2020) | In the study, they proved that the fake polls causes manipulation. |

Table 2 presents the key points of similar studies to provide a comprehensive comparison between them and the proposed study. First of all, nearly all studies (Number 1 to 6 in the table) have been specifically developed for use in traditional voting processes rather than for public consultations. They are not suitable for online surveys in Turkey due to their time-consuming and cumbersome nature, which could frustrate users with requirements such as biomedical data, PIN numbers, or OTPs from various sources. Nevertheless, the voting processes involve very difficult and time-consuming steps, which can discourage participation. Therefore, it is not

suitable for gathering public opinion online. Study 8 from the table proves that misinformation or fake polls can manipulate people's ideas. Our study has proven that in Turkey, a significant number of online polls used to gauge public opinion during elections rely solely on CAPTCHA validation, IP validation, or digital fingerprinting, which can be easily manipulated.

The aim of the presented study is to ensure that public opinions are collected safely without manipulation during the candidate selection process in elections. The key here is to ensure a balance between implementing robust security measures and maximizing user access in online polls for gauging public opinion. The aspect that distinguishes the presented study from those examined in the literature is its intended use. Almost all similar papers focus on transferring the classical voting process to an electronic environment and are therefore equipped with extreme security measures that may frustrate the user when it comes to simply giving an opinion to determine the candidate.

## CONCLUSIONS

In Turkey, online polls are frequently used to gauge public opinion during the selection process for political candidates. However, the reliability of these polls remains a significant topic of debate. This study analyzed 160 online polling sites using 10,000 votes to demonstrate that polls could be manipulated with minimal effort. It concluded that the most reliable method involves verifying users through an official platform, such as e-government, with a guarantee that users will not be profiled. Serious concerns regarding the security and accuracy of other methods being considered effectively address the disadvantage of time expenditure associated with this proposed method. Online polling sites should be assigned security scores based on the level of security methods they employ. This approach would provide participants in online polls with a better understanding of how much trust they can place in the results. The recommended order of security methods, considering the trade-off between robust security measures and maximizing user reach in online polls, includes employing a verification process through an official platform like e-government; implementing verification via SMS; restricting voting privileges exclusively to registered users; recording the MAC address; and validating CAPTCHA, digital fingerprints, and IP addresses.

Using the automated application program developed in this study, it has been demonstrated that online survey sites are highly vulnerable to attacks and that their results can be easily manipulated when collecting public opinions. This finding suggests that the information on online poll sites may not be reliable. The study also provides insights into methods that can be used to enhance confidence in this context.

In conclusion, a reliable online poll must utilize a process through an official platform such as e-government, with a guarantee that users will not be profiled, considering the trade-off between robust security measures, and maximizing user reach. Other strategies either employ methods that may annoy users, potentially deterring participation, or possess distinct security vulnerabilities.

## REFERENCES

Anderson, B., & McGrew, D. (2017). OS fingerprinting: New techniques and a study of information gain and obfuscation. *2017 IEEE Conference on Communications and Network Security (CNS).* https://doi.org/10.1109/CNS.2017.8228665

Basso, A., & Miraglia, M. (2008). Avoiding massive automated voting in internet polls. *Electronic Notes in Theoretical Computer Science, 197*(2), 149-157. https://doi.org/10.1016/j.entcs.2007.12.024

Boda, K., Földes, Á. M., Gulyás, G. G., & Imre, S. (2012). User tracking on the web via cross-browser fingerprinting. *Information Security Technology for Applications: 16th Nordic Conference on Secure IT Systems, NordSec 2011.* https://doi.org/10.1007/978-3-642-27937-9_5

Das, A., Dutta, M. P., & Banerjee, S. (2016). VOT-EL: Three-tier secured state-of-the-art EVM design using pragmatic fingerprint detection annexed with NFC-enabled voter-ID card. *2016 International Conference on Emerging Trends in Engineering, Technology and Science (ICETETS).* https://doi.org/10.1109/ICETETS.2016.7603021

Köse, E. (2019). "App Store'daki uygulamaların indirilme sayıları işte böyle manipüle ediliyor." Retrieved from https://www.log.com.tr/app-storedaki-uygulamalarin-indirilme-sayilari-iste-boyle-manipule-ediliyor/

Fifield, D., & Egelman, S. (2015). Fingerprinting web users through font metrics. *Financial Cryptography and Data Security: 19th International Conference, FC 2015.* https://doi.org/10.1007/978-3-662-47854-7_10

Gajani, Y. K., Bhardwaj, S., & Thenmozhi, M. (2023). Guarding against bots with art: NST-based deep learning approach for CAPTCHA verification. *2023 International Conference on Recent Advances in Electrical, Electronics, Ubiquitous Communication, and Computational Intelligence (RAEEUCCI).* https://doi.org/10.1109/RAEEUCCI2023.9912054

Hargittai, E., & Karaoglu, G. (2018). Biases of online political polls: Who participates? *Socius, 4.* https://doi.org/10.1177/2378023118791080

Iqbal, U., Englehardt, S., & Shafiq, Z. (2021). Fingerprinting the fingerprinters: Learning to detect browser fingerprinting behaviors. *2021 IEEE Symposium on Security and Privacy (SP).* https://doi.org/10.1109/SP50901.2021.00051

Kennedy, C., Hatley, N., Lau, A., Mercer, A., Keeter, S., Ferno, J., & Asare-Marfo, D. (2021). Strategies for detecting insincere respondents in online polling. *Public Opinion Quarterly, 85*(4), 1050-1075. https://doi.org/10.1093/poq/nfab057

Laperdrix, P., Bielova, N., Baudry, B., & Avoine, G. (2020). Browser fingerprinting: A survey. *ACM Transactions on the Web (TWEB), 14*(2), 1-33. https://doi.org/10.1145/3386040

Martin, S., & Geiger, S. (1999). Building relationships? The marketing of political parties in cyberspace. *Academy of Marketing Special Interest Group Political Marketing Conference.*

Mohammadi, S., & Abbasimehr, H. (2010). A high-level security mechanism for internet polls. *2010 2nd International Conference on Signal Processing Systems.* https://doi.org/10.1109/ICSPS.2010.5555606

Mondal, S., Rana, R., Pawar, L., Vishwakarma, A., & Lokhande, P. S. (2023). Referendum poll system: A blockchain-based solution for direct democracy. *Available at SSRN.* https://doi.org/10.2139/ssrn.4398651

Natarajan, V. (2024). Online voting system using AES algorithm with OTP validation. *International Research Journal on Advanced Engineering Hub (IRJAEH), 2*(02), 57-61.

Nikiforakis, N., Kapravelos, A., Joosen, W., Kruegel, C., Piessens, F., & Vigna, G. (2013). Cookieless monster: Exploring the ecosystem of web-based device fingerprinting. *2013 IEEE Symposium on Security and Privacy.* https://doi.org/10.1109/SP.2013.28

Park, S., Specter, M., Narula, N., & Rivest, R. L. (2021). Going from bad to worse: From internet voting to blockchain voting. *Journal of Cybersecurity, 7*(1), 1-15. https://doi.org/10.1093/cybsec/tyaa025

Pekar, V., Najafi, H., Binner, J. M., Swanson, R., Rickard, C., & Fry, J. (2022). Voting intentions on social media and political opinion polls. *Government Information Quarterly, 39*(4), 101658. https://doi.org/10.1016/j.giq.2021.101658

Prabhu, S. G., Nizarahammed, A., Prabu, S., Raghul, S., Thirrunavukkarasu, R., & Jayarajan, P. (2021). Smart online voting system. *2021 7th International Conference on Advanced Computing and Communication Systems (ICACCS).* https://doi.org/10.1109/ICACCS51430.2021.9441917

Qureshi, A., Megias, D., & Rifà-Pous, H. (2019). SeVEP: Secure and verifiable electronic polling system. *IEEE Access, 7,* 19266-19290. https://doi.org/10.1109/ACCESS.2019.2897252

Sai, M. H., & Kumar, V. A. (2022). Online voting system using Java and SQL. In *Proceedings of the International Conference on Advanced Computing and Communication Systems (ICACCS)* (pp. 910-913).

Shalini, S., Rachel, A. S., & Roshinee, A. (2020). Tracking real-time vehicle and locking system using LabVIEW applications. *2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS).* https://doi.org/10.1109/ICACCS48705.2020.9074241

Shao, R., Shi, Z., Yi, J., Chen, P.-Y., & Hsieh, C.-J. (2022). Robust text CAPTCHAs using adversarial examples. *2022 IEEE International Conference on Big Data (Big Data).* https://doi.org/10.1109/BigData55660.2022.10020482

Sivasakthi, T., Shivani, V., Palani, U., Vasanthi, D., Roshini, S., & Saundariya, K. (2021). Development of E-polling website using MERN. *2021 Smart Technologies, Communication and Robotics (STCR).* https://doi.org/10.1109/STCR53369.2021.9682226

Stantcheva, S. (2023). How to run surveys: A guide to creating your own, identifying variation, and revealing the invisible. *Annual Review of Economics, 15,* 205-234. https://doi.org/10.1146/annurev-economics-091622-010157

Tsingenopoulos, I., Preuveneers, D., Desmet, L., & Joosen, W. (2022). CAPTCHA me if you can: Imitation games with reinforcement learning. *2022 IEEE 7th European Symposium on Security and Privacy (EuroS&P).* https://doi.org/10.1109/EuroSP53844.2022.00019

Wang, P., Gao, H., Xiao, C., Guo, X., Gao, Y., & Zi, Y. (2023). Extended research on the security of visual reasoning CAPTCHA. *IEEE Transactions on Dependable and Secure Computing, 20*(6), 4976-4992. https://doi.org/10.1109/TDSC.2022.3147489

Wang, Y., & Lu, M. (2016). A self-adaptive algorithm to defeat text-based CAPTCHA. *2016 IEEE International Conference on Industrial Technology (ICIT).* https://doi.org/10.1109/ICIT.2016.7474812

Yeargain, T. (2020). Fake polls, real consequences: The rise of fake polls and the case for criminal liability. *Missouri Law Review, 85,* 129. Retrieved from https://scholarship.law.missouri.edu/mlr/vol85/iss1/7

Yudin, G. (2020). Governing through polls: Politics of representation and presidential support in Putin's Russia. *Javnost-The Public, 27*(1), 2-16. https://doi.org/10.1080/13183222.2020.1675434

**EXTENDED ABSTRACT**
*GENİŞLETİLMİŞ ÖZET*

# ÇEVRİMİÇİ SİYASİ ANKETLERİN GÜVENİLİRLİĞİNİN DEĞERLENDİRİLMESİ: YENİ BİR OYLAMA YAZILIMI KULLANIMI

Türkiye'de siyasi parti aday adaylık süreçlerinin sonlanması ve adayların belirlenmesinde çeşitli faktörler etkili olmaktadır. Bu faktörlerden en belirgin olanlarından biri, online olarak düzenlenen siyasi anketlerdir. Günümüzde birçok siyasi parti ve bazı özel kuruluşlar (yerel haber web sayfaları gibi) bu tür anketleri kullanarak kamuoyu görüşünü belirlemeye çalışmaktadırlar. Özellikle son yıllarda, maliyet avantajı ve hızlı uygulanabilirliği sayesinde online siyasi görüş örneklemesi anketlerinin kullanımı artmıştır. Ancak, dijital ortamda gerçekleştirilmelerinden kaynaklanan zaaflar, bu anketlerin güvenilirliklerinin sıklıkla sorgulanmasına neden olmaktadır.

Bu çalışma, Türkiye'deki 2024 yerel seçimleri öncesinde 160 çevrimiçi anket platformunu incelemiştir. Araştırmada, bu platformlarda kullanılan çeşitli güvenlik önlemlerinin etkinliği analiz edilmiş ve bir oylama uygulaması geliştirilerek, belirtilen online anket sitelerinde tek bir bilgisayar kullanılarak 143 saat içinde 10.000 adet oy kullanılmıştır. Bu süreç, online anketlerin güvenliği konusunda ciddi endişeleri gündeme getirmiştir.

Analiz sonuçları, CAPTCHA, dijital parmak izi ve IP doğrulama gibi sıklıkla rastlanan güvenlik yöntemlerinin önemli zaaflar içerdiğini göstermiştir. Bu güvenlik önlemleri bazı dirençler sunmuş olsa da, çalışmada elde edilen bulgular bu önlemlerin manipülasyona karşı tam olarak etkili olmadığını ortaya koymuştur. Bu durum, kullanılan online anketlerin güvenilir olmadığını ve elde edilen sonuçların manipülasyona açık olduğunu göstermektedir.

Çalışma, e-devlet platformu üzerinden kullanıcı doğrulaması sağlayan bir yöntemin, online anketlerde bilgi güvenliğini garanti altına almanın ve sonuçların güvenilirliğini artırmanın en etkili yolu olduğunu önermektedir. Bu yöntem, maliyet ve hız avantajı sunan online anketlerin kullanılmasını daha güvenli hale getirebilir ve kamuoyu görüşlerinin daha doğru bir şekilde yansıtılmasına olanak tanıyabilir.

Sonuç olarak, bu çalışma Türkiye'deki online siyasi anket uygulamalarının mevcut durumunu ve bu anketlerin güvenilirliğini artırma yollarını detaylı bir şekilde incelemektedir. Çalışma, online anketlerde kullanılan güvenlik önlemlerinin etkinliğini artırmak ve gerçek kamuoyu görüşlerini daha doğru bir şekilde yansıtabilmek için yol gösterici niteliktedir.

# KATKI ORANI BEYANI VE ÇIKAR ÇATIŞMASI BİLDİRİMİ

| | |
|---|---|
| **Sorumlu Yazar** *Responsible/Corresponding Author* | Murat IŞIK |
| **Makalenin Başlığı** *Title of Manuscript* | ASSESSING THE UNRELIABILITY OF ONLINE POLITICAL POLLS: A NOVEL SOFTWARE FOR VOTING APPROACH |
| **Tarih** *Date* | 31.12.2024 |
| **Makalenin türü (Araştırma makalesi, Derleme vb.)** Manuscript Type (Research Article, Review etc.) | Research Article |

**Yazarların Listesi /** *List of Authors*

| *Sıra No* | **Adı-Soyadı** *Name - Surname* | **Katkı Oranı** *Author Contributions* | **Çıkar Çatışması** *Conflicts of Interest* | **Destek ve Teşekkür (Varsa)** *Support and Acknowledgment* |
|---|---|---|---|---|
| 1 | Murat IŞIK | %50 | YOKTUR. | YOKTUR. |
| 2 | Mehmet Ali YALÇINKAYA | %50 | YOKTUR. | YOKTUR. |