

An Antibot-Based Web Voting System for Higher Institutions

Jessen Japheth[1], John Wejin[2(✉)], Sanjay Misra[3], and Jonathan Oluranti[2]

[1] Taraba State University, Jalingo, Taraba, Nigeria
[2] Covenant University, Ota, Ogun, Nigeria
John.wejinpgs@stu.cu.edu.ng,
jonathan.oluranti@covenantuniversity.edu.ng
[3] Ostfold University College, Halden, Norway
Sanjay.misra@hiof.no

Abstract. The Internet has caused an evolution in how people socialize, work, and do business. The emergence and improvement in cloud computing and web technologies make interactions and remote processes possible. This advancement has presented an opportunity for the people and their representatives to meet during the voting process. Voting is making a choice or decision within a particular group. However, the conventional voting process that uses the paper-based approach faces the challenges of multiple voting, overvoting, cost, high voting fraud, and delay in declaring election results due to long counting times. Various methods have been proposed to overcome the multiple challenges prevalent in the traditional voting system. This paper proposes an antibot-based web voting platform that enables voters to vote within any location. It uses the hash technique and the antibot checking features to enforce security and voters' confidentiality. PHP and HTML languages were used to implement the front-end of the system. SQL database and the Apache server were used for the back-end. On implementation and testing, our system shows good security enhancement and a reduction in the time consumed for counting and declaring election results.

Keywords: Anti-bot · E-voting · Cloud computing

1 Introduction

The Internet, which started as an interconnection between four large computers (Mainframes) connecting a few universities and research institutes, has significantly evolved. The modern high-speed global interconnection known as the Internet is a vital commodity for both individuals and governments. In the 21st century, exploring emergent technologies to connect people is rising. This drive has been extended to the frontiers of democracy, as electronic involvement presents an opportunity for people and their representatives to meet during the voting process [1]. Voting is making a choice or decision regarding something within a specific group. Various voting systems have different standards and requirements for the entire process, but the goal remains unchanged, giving utmost consideration to voters' decisions regarding something.

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2022
O. Gervasi et al. (Eds.): ICCSA 2022 Workshops, LNCS 13381, pp. 650–661, 2022.
https://doi.org/10.1007/978-3-031-10548-7_47

Conventional voting systems have been identified as ineffective in terms of their requirements: ballot paper, voting in proxy, lack of transparency in counting of votes (a severe issue for Nigeria), and over-dependence of the voting process on a centralized committee [2]. In modern times, the digitization of the electioneering and voting process is becoming increasingly adopted by various countries and organizations. The most prominent example is digital voting for local authorities in countries like Estonia, the USA, Switzerland, Netherlands, India, Namibia, and Nigeria. Though this means of voting addresses the inefficiency in the conventional voting system, the electronic system still faces some challenges, especially in vulnerabilities regarding the central checking of all results, and recently the use of software-bot for anonymous voting [3].

This paper proposes an anti-robot voting system for voting in educational institutions. It prevents anonymous voting through a soft bot and securely protects the e-voting platform and process. The rest of the paper is structured as follows. An overview of the voting system and the hashing system are presented in Sects. 2 and 3. Related works are discussed in Sect. 4, and the proposed system is presented in Sect. 5. Results and discussions are presented in Sect. 6, while the conclusion and future works are presented in Sect. 7.

2 Types of Voting System

Voting has been identified as a duty and a fundamental right of citizens in a given country. It gives the people the privilege to decide who champions the affairs of their nation within a specified democratic dispensation or period. There are various means of voting processes or methods in the world. These methods are based on the agreement of the majority of the people via their various representatives. The well-known techniques commonly employed by various governments are as follows.

1. Paper-Based Voting System
   The paper type of voting was the earliest or most traditional voting system employed by various nations, especially in developing countries of the African continent. In this method, the voters vote using papers on which different political parties and their candidates are written. The eligible voters will select the party or candidate using the agreed marker (usually with the thumb or a stamp), then fold the ballot paper, and drop it in a ballot box positioned in a given location where individuals and party representatives can see it or monitor. The votes are then counted after the election at the polling station in the hearing and observation of party officials, collated, and signed by party representatives for onward transmission to the central collation center. The paper-based voting system comes with the advantage of voting ease. The voter only needs to make a mark beside his candidate of choice to vote [4]. However, many disadvantages come with this method of voting system. Theses are:

   - Time Demanding: The paper-based system allows voting one at a time. This is time tasking.

- Delay in Counting. The election results usually take a long time (sometimes days) before they are declared. This is because counting is done manually in every polling station.
- Ballot Fraud: The ballot papers can be easily copied and altered to conceal any change.
- Hoodlums can quickly snatch ballot papers.
- The cost of printing ballot papers adds to the cost of paper-based voting systems.

2. Electronic Voting Machine (EVM) Method
   The electronic voting machine was proposed and implemented to overcome the drudgery prevalent in the paper-based voting method. The EMV consists of two essential parts: the control unit and the ballots unit. The ballot unit has buttons that enable candidates to vote. Unused buttons are usually covered within the control unit. It is capable of recording about 3840 votes. With EVM, only eligible voters can vote, which happens only once. Thus, over-voting and multiple voting challenges at different polling stations are eliminated. The demerits of such a voting system, as enumerated in [4], are:

   - Transparency: Voters are critical of the EVM machine because they lack knowledge of the working principle of the voting procedure within the machine.
   - The tendency for Fraud: Digital systems can be hacked by individuals who know the working principle of a particular system. Access to the EVM storage can alter votes within the system.
   - Power: An electronic system depends on power to function. EVM voting system deployment becomes difficult or nearly impossible in areas where electric power supply is erratic.
   - Cost: The cost of obtaining an EVM and its maintenance in the event of mechanical or software failure is highly expensive.

3 Common Security Approach for E-Voting Systems

3.1 Hashing

Hash functions are vital in most information systems. The hash function is a mathematical expression that converts streams of characters and maps them to a value of a particular length. This value is usually a smaller version of the original streams of characters. The hashing algorithm retrieves data at a shorter time from a database and is also commonly used for either encryption or decryption of signatures or keys [5]. Furthermore, hashing can be used for password storage to identify users that can have access to use a particular system. A logon scenario that explains hashing in our proposed system is shown in Fig. 1. The password is wrapped, making it have a table pair consisting of the user ID and the h(p) table. This makes it difficult for a hacker to access a system [6]. Various researches make use of hashing to enforce security. In [7], hashing was employed for constant checking of application vulnerability, an optimized hashing technique based on Convolutional Neural Network (CNN) was developed in [8], speech encryption [9], etc.

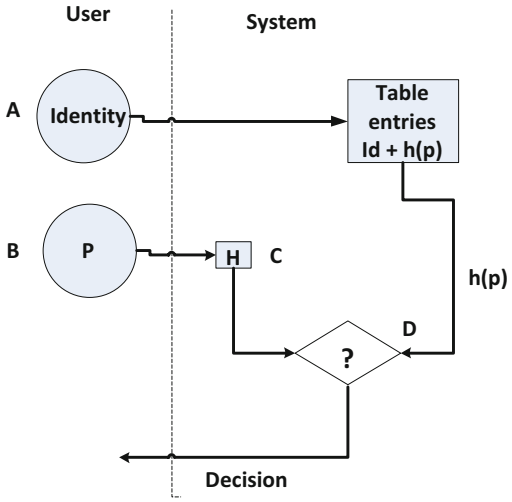

Fig. 1. Hashing operation in password application

3.2 Homomorphic Encryption

Homomorphic encryption techniques have become prominent cryptographic approach, especially for processes that are cloud-based. Unlike other cryptographic techniques that act on data at inertia or in transit, homomorphic encryption acts on data that is in use. It provides computation on data that has been encrypted, thus, enabling confidentiality in data as it is being processed or used. This security approach allows mostly two key algebraic operation on encrypted text namely, addition and multiplication. Other mathematical operations are resultants of the combination of these two operations [25]. Based on the function or number of mathematical operations on an encrypted data, homomorphic security technique can be grouped into the following:

- Additive homomorphic technique: Only addition operation is allowed on the encrypted data.
- Partial homomorphic technique: Allows for addition and limited number of multiplication operation.
- Fully homomorphic technique: Allows for both addition and multiplication operations in unlimited fashion.

Homomorphic encryption technique find application in e-voting during the ballot counting process. The e-counting process can use homomorphic encryption e.g. the addition operation to calculate votes without the choice of the voters being known or disclosed, thus, enabling confidentiality and privacy in the voting process.

4 Related Works

In [10], the authors reviewed the state of implementation of e-voting around the world, especially in Estonia and Switzerland. Based on their analysis of the Indian scenario, a

design for internet voting was implemented using SQL. Testing and evaluation of the proposed system, SQL injection, possible defense mechanisms, and future directions for e-voting were presented. The authors in [11] conducted a review on e-voting. The authors focused on the e-voting experience of Estonia and Namibia. Their study reveals that Information Communication Technology (ICT), political dimensions, and voters' illiterate level are critical challenges to the successful use of e-voting, especially in developing nations. A blockchain approach to securing e-voting data was proposed in [12].

The proposed framework uses a hashing technique to dynamically adjust the blockchain, making it challenging to access unauthorized individuals. To optimize and ensure a secure decentralized decision approach over blockchain for e-voting purposes, the authors in [13] proposed a privacy protocol for online voting. It allows connected peers to choose their candidates over their blockchain network without using a third party, ensuring privacy, fraud detection, and corrections. A mobile-based approach to e-voting was implemented in [14]. The authors employed a proxy-based signature scheme that provides security features such as privacy, voters' protection, and message verification. Evaluation of the system reveals a reduction in computational cost and enhanced security. The concealment of voters' identities during an election is critical in the election process. This is usually known as secret suffrage. The authors in [15] investigated how the various proposals of e-voting adhere to the secrecy of voters during elections. The authors in [16] proposed a homomorphic encryption approach to ensure the online system of voting security. Voter confidentiality is ensured by enforcing security on ballots using encryptions. Evaluation reveals that the system has a good time submission verification rate and high voter confidentiality. Blockchain and machine learning are highly accepted in securing e-voting platforms and systems [17–24].

5 Proposed Approach

To actualize implementing the proposed antibot web-based voting system, we adopted the design in [2] and modified it to suit our designs and functionalities. The proposed design considered using antibot techniques and keys to enable security in the voting system. The proposed system has 5 phases: eligible voters' registration, vote casting, end of the day stage, collection stage, and final repository stage. These stages are briefly described below.

- Voters Registration Stage
  Unlike other systems that allow systems to register voters directly, our system first has, before the voters' registration via the web interface, a complete list of eligible voters is included in the database (in this case, the number of students). This enables the system to check the status of the voter (students or not students) before generating keys that will be used in the voting process.
- Vote Casting
  This is the phase where the voting takes place. The voter visits the voting site, where he will be prompted to enter his student ID and the key generated during the voter registration phase. On successful login, the various contesting positions with the names

of candidates are displayed for the voter to elect the candidate of their choice. After selecting their choices, the voter clicks on the vote button to submit his vote. A prompt is activated to help verify voters of their choice before submission. On submission, a hash key is generated for the candidate. The key enables the voter to log in to check the election results.

- Collation Stage
  To reduce fraud and ensure transparency, collation of results is done by a neutral party in the presence of candidates' representatives. However, this phase is conducted using an offline means.
- Voting close
  At this phase, the election process is ended after the set time for the election has ended. During this period, the voter can log in to vote. However, voters can check the election results using the hash key generated after voting. Data gathering and compilation are done automatically. System checks are carried out (verification of hashes against several voters and votes count). After the confirmation, the election committee and various representatives sign and ratify the election process.

5.1 Proposed System Flowchart

The voting process using the proposed system is shown in Fig. 2. The voters' eligibility is first checked using the record on the database. The user-generated user ID and password are used as login details for the voters, and an electronic ballot sheet for voting on successful login. Successful voting is saved on the database, the vote count is updated, and a confirmation message is displayed to assure the voter that his vote has been accepted.

5.2 The Antibot Security Process

The proposed system uses a two-way verification process namely, the voter/password authentication and the antibot security mechanism. During the registration of voters, an automated voter's ID based on Extended Binary Coded Decimal (EBCD) is generated for each voter. The voter then creates a unique password they can recall. These two security keys are first verified during the login process as shown in Fig. 3. On successful authentication, the system activates the antibot mechanism that checks for soft-bots. In modern days, it has become common for malicious programs (commonly referred to as soft-bots) that automates task to find presence over the internet. These bots can generate fraudulent accounts, ticket purchase, and even infiltrate a voting process by acting as legitimate voters. This motivates the integration of antibot mechanism in the proposed electronic voting system. In our proposed solution, we adopted the google authenticator and API security features to implement the antibot mechanism. We first created an account on google console and then used the checkbox antibot feature of the google authenticator. The google SDK shell was run on the server to enable offline authentication and verification.

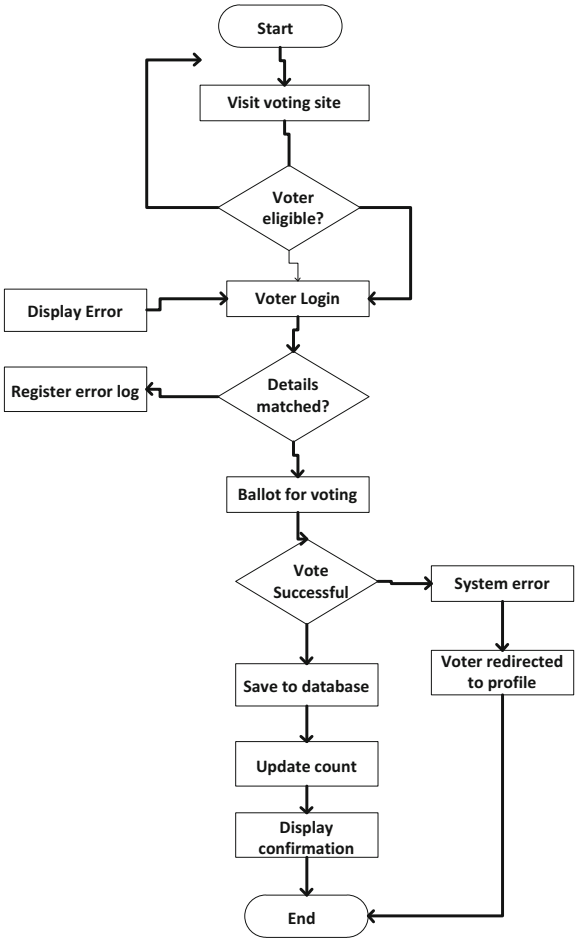

Fig. 2. Proposed voting system flowchart

6 Results and Discussion

SQL and Apache servers were employed to implement the proposed system for the back-end design and the server. PHP and HTML were used to implement the front-end. The hardware component consists of a Windows 10-based PC of 5G dual core intel processor with 250G. After the design and implementation, the antibot web-based system was deployed on the school's network and tested by running a departmental election. The results from the implementation are shown in this section.

Figure 3 shows the login page for the voters to sign in and vote. The users insert their login details as provided, and on verification and authentication, the voter is ready to begin voting. The antibot mechanism is integrated with the user login authentication process. At login, the voter is also verified to ascertain their soft-bot status by the system, as depicted in Fig. 3.

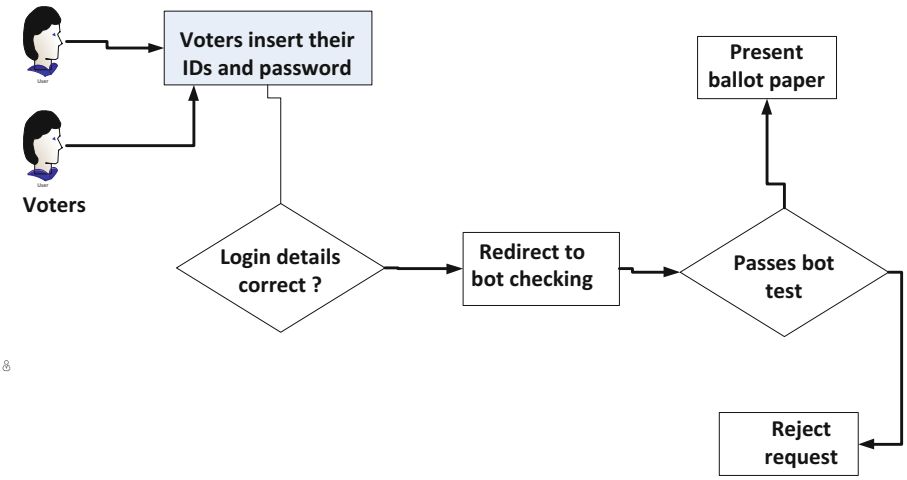

Fig. 3. The proposed security approach

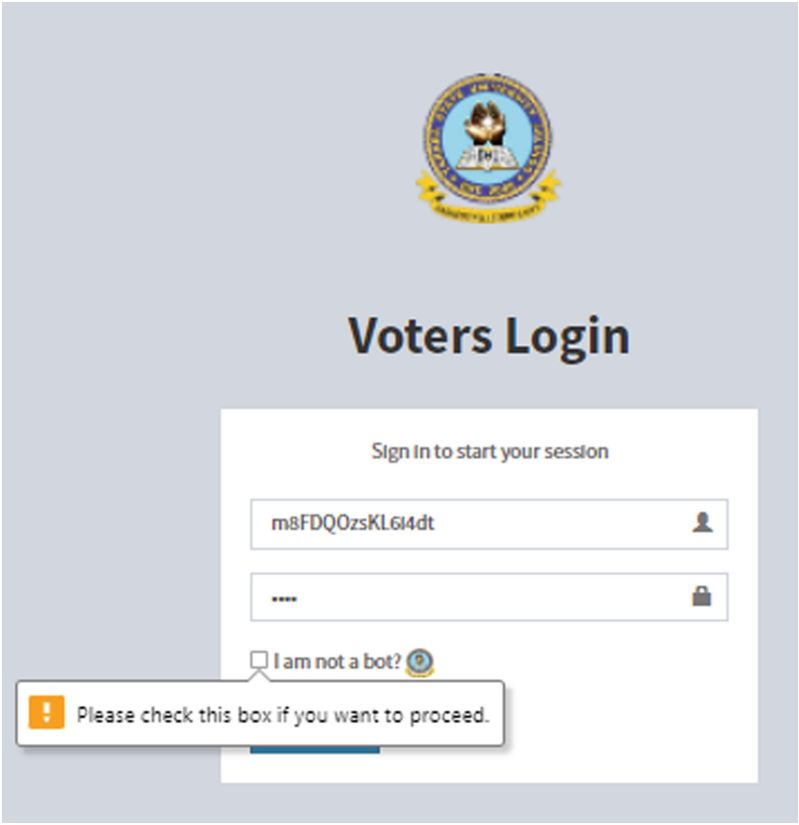

Fig. 4. Voters' login page

Upon successful voter login and bot checking, the voter is presented with a page that holds the various candidates' positions and names, as depicted in Fig. 4. The voting page serves as the electronic ballot sheet that enables voters to vote. When a voter is done with selecting their candidates, a voting review page is presented in Fig. 5 to help check selection before the final submission of choice. The "vote successfully submitted" page as depicted in Fig. 6 is displayed so that the voter is assured of vote submission. The voting tracking page of the system is shown in Fig. 7.

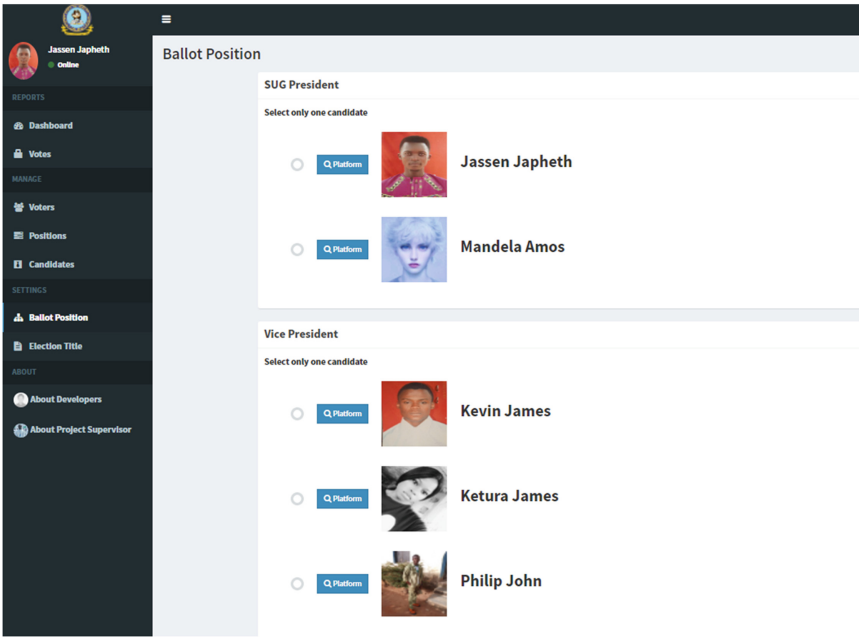

Fig. 5. Electronic ballot sheet

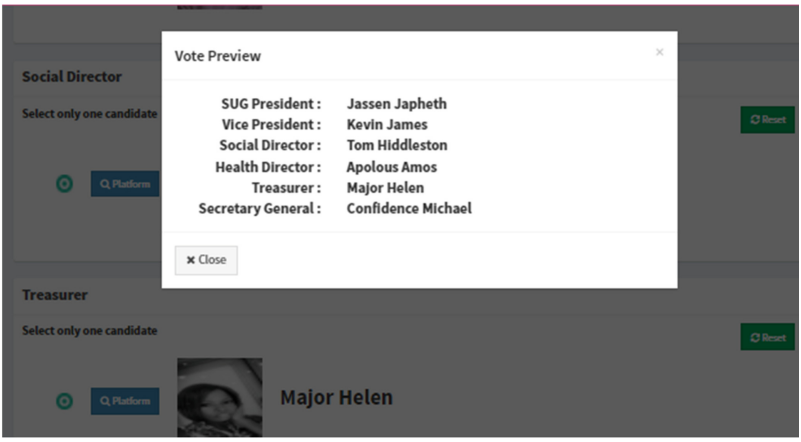

Fig. 6. Voting preview page

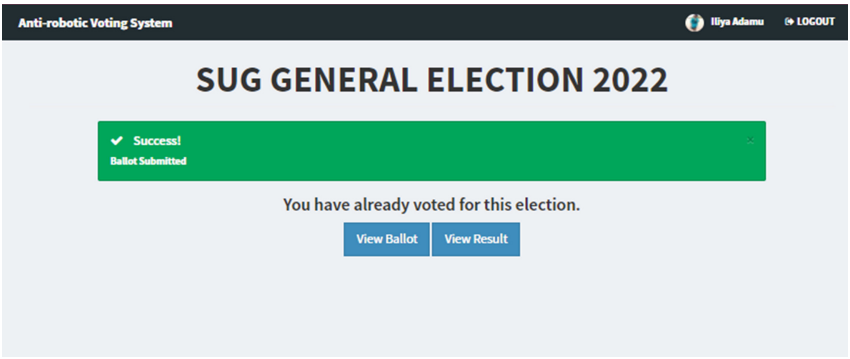

Fig. 7. Vote submission page

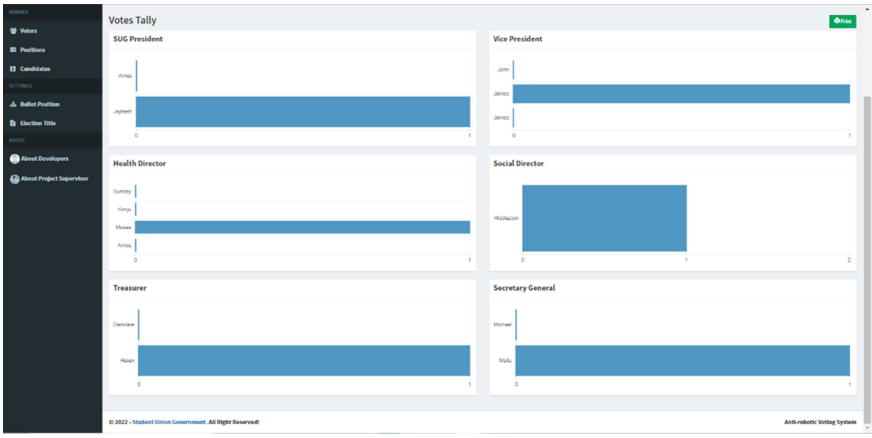

Fig. 8. Voting tracking page

7 Conclusion

This paper proposes an antibot-based web voting platform that enables voters to vote within their comfort zones. The proposed system uses the hash technique and the antibot checking features to enforce security and voters' confidentiality. This system eliminates the possibility of non-human voting that threatens the fidelity of the e-voting system. Furthermore, the eligibility of voters and their submissions are easily verified. Voters can track the result process by having a unique login that enables only registered, accredited, and voted individuals to track the progress. Using a machine learning approach that holds the potential for a more secure and efficient e-voting system is a good research direction.

References

1. Zissis, D., Lekkas, D.: Securing e-Government and e-Voting with an open cloud computing architecture. Gov. Inf. Q. **28**(2), 239–251 (2011). https://doi.org/10.1016/j.giq.2010.05.010

2. Rodiana, I.M., Rahardjo, B., Aciek Ida, W.: Design of a public key infrastructure-based single ballot e-voting system. In: 2018 International Conference on Information Technology Systems and Innovation (ICITSI), pp. 6–9, October 2018. https://doi.org/10.1109/ICITSI.2018.8696083
3. Kurbatov, O., Kravchenko, P., Poluyanenko, N., Shapoval, O., Kuznetsova, T.: Using ring signatures for an anonymous e-voting system. In: 2019 IEEE International Conference on Advanced Trends in Information Theory (ATIT), pp. 187–190, December 2019. https://doi.org/10.1109/ATIT49449.2019.9030447
4. Harshitha, V.N.: MyVote - an effective online voting system that can be trusted. Glob. J. Comput. Sci. Technol. (2021). https://computerresearch.org/index.php/computer/article/view/2012. Accessed 28 Feb 2022
5. "What is Hash Function? - Definition from Techopedia. Techopedia.com. http://www.techopedia.com/definition/19744/hash-function. Accessed 28 Feb 2022
6. Cryptography Hash Functions. https://www.tutorialspoint.com/cryptography/cryptography_hash_functions.htm. Accessed 28 Feb 2022
7. Vijayakumar, K., Arun, C.: Continuous security assessment of cloud based applications using distributed hashing algorithm in SDLC. Clust. Comput. **22**(5), 10789–10800 (2017). https://doi.org/10.1007/s10586-017-1176-x
8. Su, S., Zhang, C., Han, K., Tian, Y.: Greedy hash: towards fast optimization for accurate hash coding in CNN. In: Advances in Neural Information Processing Systems 2018, vol. 31 (2018). https://proceedings.neurips.cc/paper/2018/hash/13f3cf8c531952d72e5847c4183e6910-Abstract.html. Accessed 28 Feb 2022
9. Zhang, Q., Zhou, L., Zhang, T., Zhang, D.-H.: A retrieval algorithm of encrypted speech based on short-term cross-correlation and perceptual hashing. Multimed. Tools Appl. **78**(13), 17825–17846 (2019). https://doi.org/10.1007/s11042-019-7180-9
10. Singh, V.P., Pasupuleti, H., Babu, N.S.C.: Analysis of internet voting in India. In: 2017 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), pp. 1–6, March 2017. https://doi.org/10.1109/ICIIECS.2017.8276137
11. Mpekoa, N., van Greunen, D.: E-voting experiences: a case of Namibia and Estonia. In: 2017 IST-Africa Week Conference (IST-Africa), pp. 1–8, May 2017. https://doi.org/10.23919/ISTAFRICA.2017.8102303
12. Shahzad, B., Crowcroft, J.: Trustworthy electronic voting using adjusted blockchain technology. IEEE Access **7**, 24477–24488 (2019). https://doi.org/10.1109/ACCESS.2019.2895670
13. Zhang, W., et al.: A privacy-preserving voting protocol on blockchain. In: 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), pp. 401–408, July 2018. https://doi.org/10.1109/CLOUD.2018.00057
14. Chiou, S.-Y., Wang, T.-J., Chen, J.-M.: Design and implementation of a mobile voting system using a novel oblivious and proxy signature. Secur. Commun. Netw. **2017**, e3075210 (2017). https://doi.org/10.1155/2017/3075210
15. Rodríguez-Pérez, A.: Secret suffrage in remote electronic voting systems. In: 2017 Fourth International Conference on eDemocracy eGovernment (ICEDEG), pp. 277–278, April 2017. https://doi.org/10.1109/ICEDEG.2017.7962550
16. Yang, X., Yi, X., Nepal, S., Kelarev, A., Han, F.: A secure verifiable ranked choice online voting system based on homomorphic encryption. IEEE Access **6**, 20506–20519 (2018). https://doi.org/10.1109/ACCESS.2018.2817518
17. Djanali, S., Nugraha, D.P., Studiawan, H., Pratomo, B.A.: Vote identification and integrity of ballot in paper-based e-voting system. Electron. Gov. **14**(3), 240–254 (2018). https://doi.org/10.1504/EG.2018.093416
18. Abou-Rizka, M., Shedeed, A.: Secure E-voting scheme through polling stations, vol. 1–3, pp. 250–256 (2009)

19. Roopak, T.M., Sumathi, R.: Electronic voting based on virtual ID of Aadhar using blockchain technology, pp. 71–75 (2020). https://doi.org/10.1109/ICIMIA48430.2020.9074942
20. Taş, R., Tanriöver, Ö.Ö.: A manipulation prevention model for blockchain-based E-voting systems. Secur. Commun. Netw. **2021** (2021). https://doi.org/10.1155/2021/6673691
21. Baudier, P., Kondrateva, G., Ammi, C., Seulliet, E.: Peace engineering: the contribution of blockchain systems to the e-voting process. Technol. Forecast. Soc. Change **162**, 120397 (2021). https://doi.org/10.1016/j.techfore.2020.120397
22. Anwar ul Hassan, Ch., et al.: A liquid democracy enabled blockchain-based electronic voting system. Sci. Program. **2022** (2022). https://doi.org/10.1155/2022/1383007
23. González, C.D., Mena, D.F., Muñoz, A.M., Rojas, O., Sosa-Gómez, G.: Electronic voting system using an enterprise blockchain. Appl. Sci. **12**(2), 531 (2022). https://doi.org/10.3390/app12020531
24. Xu, D., Shi, W., Zhai, W., Tian, Z.: Multi-candidate voting model based on blockchain. IEEE/CAA J. Autom. Sin. **8**(12), 1891–1900 (2021). https://doi.org/10.1109/JAS.2021.1004207
25. Challa, R.: Homomorphic encryption: review and applications. In: Borah, S., Balas, V.E., Polkowski, Z. (eds.) Advances in Data Science and Management. LNDECT, vol. 37, pp. 273–281. Springer, Singapore (2020). https://doi.org/10.1007/978-981-15-0978-0_27