Comparative E-Voting Security Evaluation: Multi-Modal Authentication Approaches

Elsi Ahmadieh, Nour El Madhoun

Comparative E-Voting Security Evaluation: Multi-Modal Authentication Approaches

Elsi Ahmadieh*, Nour El Madhoun†‡
* Lebanese University, Faculty of Technology, Department Communications and Computer Networks Engineering, Beirut, Lebanon
† LISITE Laboratory, ISEP, 10 Rue de Vanves, Issy-les-Moulineaux, 92130, France
‡ Sorbonne Université, CNRS, LIP6, 4 place Jussieu 75005 Paris, France
E-mails: elsiahmadieh@gmail.com; nour.el-madhoun@isep.fr
nour.el_madhoun@sorbonne-universite.fr;

***Abstract*—The decentralized, distributed ledger, a fundamental aspect of blockchain technology, plays a pivotal role in various sectors, including electronic voting (e-voting) systems. When considering e-voting, the significance of blockchain technology in boosting the security, transparency, and integrity of the entire process is evident. This ranges from the initial steps of user registration and authentication to the final stages of voting and result validation. Unlike conventional voting systems, which are plagued by issues such as fraud, tampering, and a lack of transparency in the result tallying and viewing processes, not to mention the delays, blockchain-enabled e-voting mitigates these challenges within government frameworks. It ensures a secure, tamper-proof, and transparent procedure, where each vote is recorded as an immutable transaction, thereby enhancing the process's reliability. This paper explores the integration of voice recognition and fingerprinting using blockchain technology for enhancing the security of e-voting systems, comparing alternative authentication methods, and emphasizing the need for a multi-modal approach to achieve better security and reliability of the voting systems.**

***Index Terms*—Authentication, Biometrics, Blockchain, Ethereum, E-Voting, Fingerprint, Smart-Contracts, Voice Recognition.**

I. Introduction

Due to the importance of decision-making in democratic countries, there is a need to implement transparent and accurate election systems that enable all citizens to cast their votes, regardless of their situations, whether they are without disabilities or facing challenges. In traditional electoral processes, vulnerabilities to various kinds of fraud and tampering exist; moreover, these processes can be time-consuming. For example, results stored on electronic devices are susceptible to hacking, allowing data to be altered. Additionally, individuals with physical challenges or older adults may find it difficult to access voting stations or centers, potentially compromising the fairness and accuracy of elections. To enhance the electoral process and keep it aligned with rapid technological advancements, integrating a secure blockchain system is essential. Such a system would significantly increase the security and reliability of these critical infrastructures, ensuring a more robust electoral process [1], [2].

Single-Factor Authentication (SFA) represents a moderate approach in e-voting systems, where users can enter only one piece of information, such as usernames and passwords, and will directly gain access or become authorized [3]. These systems have a very low level of security and are vulnerable to any kind of tampering. Considering the limitations of such configurations, relying solely on passwords or electronic signatures is insufficient [4]. On the other hand, Two-Factor Authentication (2FA), also known as Multi-Factor Authentication (MFA), introduces an additional layer of authorization and verification. It requires users to go through multiple steps of authentication before they can gain access. These mechanisms can be categorized as knowledge factors (something a user knows, such as usernames and passwords), possession factors (such as verification pins or OTPs (One-Time Passwords or Pins) that may be linked to their owned devices), or biometric factors (for example, face recognition, fingerprints, and voice recognition) [3].

Considering the critical importance of implementing secure systems and verification models in our e-voting process, we focus in this paper on comparing alternative authentication methods, including their strengths and weaknesses. This exploration serves as the foundation for presenting our proposal of fingerprint verification, supplemented by voice recognition integration. This approach aims to ensure users can securely cast their votes before applying this robust 2FA methodology. Thus, this paper is organized as follows: in Section II, we present the principle of e-voting integrated with blockchain technology and biometric techniques. In Section III, we provide a brief analysis and comparison between previous approaches in this field. In Section IV, we present our proposed model. In Section V, we conclude this paper.

II. Principle of Blockchain-Based E-Voting Systems

A. Traditional Voting Systems and the Need for Blockchain

In every democratic country and since the dawn of history, governmental authorities have tried to maintain accurate and fair elections by ensuring secure and accurate voting processes. These voting methodologies relied only on pens and papers, and occurred in specified centers in every region, where people from these regions gather and vote. This procedure can be very risky on several levels, including security concerns as

well as people's ability to reach voting centers. For example, during the voting process, many issues can arise, starting from these items being destroyed when people use them to write or select their preferred candidate, to result counting that can be vulnerable to numerous human errors and loss of any paper that represents a vote. Additionally, these results are susceptible to many kinds of tampering and manipulation by any party [5].

During this era of technological progress, we can benefit from technological achievements to enhance the voting process. Electronic voting (e-voting) can be the best approach that adds more value to the whole system, in addition to being up-to-date with technology standards and flows. E-voting systems are mainly characterized by:

- Their ease and availability: voting online can be easier to access. Once the user is allowed to vote, he will directly enter the system, vote, and then wait for the results. Moreover, people are no longer required to leave their houses to reach the voting centers, keeping in mind the difficulty in doing so, especially for physically disabled people.
- Time saving: people can vote from their own houses with just a few clicks, regardless of any obstacle. In this scenario, the government is only responsible for the preparation of this electronic setup with specialized people. In traditional voting processes, preparations include setting up voting centers, tools to be used, specified people to manage the procedures, and specified people for result validation and counting.
- Reliability: instead of relying on people to count the results and later validate them, with possibilities of data loss or mistakes, electronic counting of votes and results validation is more accurate and reliable.

Although e-voting systems represent a more resilient procedure for elections and voting, these systems can still be vulnerable to manipulation because of the data storage and results validation by third parties or central entities. For these concerns, blockchain-based e-voting systems will be the most reliable solution to the presented issues [6].

B. Blockchain in E-voting Systems

Blockchain technology has become widely spread and used on many platforms thanks to its high security and reliability. Considering its distributed ledger, transactions on blockchain are stored on all the nodes or computers that are connected to the same network, and these transactions can never be modified once approved by the nodes and deployed on the chain. This ensures that transacting via blockchain is tamper-proof and can never be manipulated. Also, any transaction on the blockchain is never lost due to the absence of centralized parties that store the data. The procedures of transacting via blockchain are transparent and well recorded, which gives users full access and knowledge of how their data is being processed, without the fear of being attacked or having any data tampered with [7].

Blockchain smart contracts can help in enhancing e-voting systems with conditions that are predefined and predetermined. Each smart contract will automatically execute all the flows and conditions that are set by the government, and this saves a lot of time for the voting process to be completed. The traditional election process that relies on paper ballots is very time and resource consuming if we consider the preparations of voting centers that need to be done, the people that are required to monitor the whole election procedure, and the people and equipment needed for results counting and validation. This started to improve when governments began relying on e-voting instead of traditional voting methods. E-voting methods are a lot better than traditional methods, take less time, rely mostly on computers and software rather than human work, and do not need any centers or places to vote or review results. But even these election methods need third parties to be involved, and this subjects the systems to many kinds of manipulation or data loss. Thus, we can say that blockchain-based systems that rely on smart contracts are the best approach.

Moreover, to add more privacy and security to blockchain-based systems, we can benefit from 2FA instead of SFA systems that will require users to undergo double security checks or verification after login or registration, in order to grant proper access to vote. These methods can be user-traits related, or biometric, to give a more scientific orientation [8]. By relying on fingerprint and voice recognition authentications, we first enable the eligible users to access the system in order to cast their votes. Then, upon registration and information filling, we allow users to acknowledge their second verification method. Therefore, we should first implement fingerprints to grant access for the allowed users. Then, as credentials, we can rely on a specific sentence that the user chooses, and then it will be verified by the specified smart contracts to allow authorization. The user shall be able to cast his vote and later get the results once they are done.

C. Biometrics

Biometrics can be defined as the fastest and most accurate and reliable authentication method that relies on unique biological characteristics [9]. These characteristics are used to identify a unique trait in each person, and these characteristics are analyzed by biometric systems and transformed into digital data that are stored later in databases. Once there is a need to authenticate someone, the programmed authentication system (with biometrics) takes the newly entered inputs or biological traits or behaviors, transforms them into digital units, and then compares the new data with the expected or saved one. Once the data is compatible, the user is granted proper access. Biometrics are mostly used in computer science as a form of access control, and in surveillance and statistical applications.

We can classify biometrics into two categories: physiological biometrics and behavioral biometrics.

- **Physiological Biometrics**: these measurements include physical traits that are unique for each human and can rarely change over time, so they are fixed measures that

can be taken into consideration. Examples of physiological biometrics:
  - Fingerprint: capturing the lines and spaces in fingertips.
  - Face Recognition: relies on the distance between facial elements such as the distance between the eyes, nose, mouth, and jawline.
  - Iris Scanning: scans the colored part of the eyes, and details of the blood vessels in the white part.
  - DNA: includes genetic unique traits of humans.
- **Behavioral Biometrics**: these are behavioral traits that specify an action, movement, or any behavior of humans. These traits can be unique to any person and can be fixed as well, but they may also change over long periods of time or under external circumstances. Examples of behavioral biometrics:
  - Voice Recognition: includes the analysis of vocal traits (related to the sound waves and their characteristics).
  - Typing Rhythm: calculates speed, error rates, and most used typing patterns.

Property	Iris	Retina	Fingerprint	Palm Print	Hand Geometry	Face	Ear	DNA	Voice
Uniqueness	High	High	High	High	Medium	Medium	Medium	High	Low
Permanence	High	High	High	High	Low	Medium	Medium	High	Low
Universality	High	High	Medium	Medium	High	High	High	High	Medium
Measurability	Medium	Low	High	High	High	Medium	Medium	Low	Medium
Collectability	High	Medium	Medium	Medium	High	High	Medium	Low	Medium
Performance	High	High	Medium	Medium	Medium	Low	Low	High	Low
Acceptability	Medium	Low	High	High	Medium	High	Medium	High	High

Fig. 1. Comparison of Biometric Data

Some authors, like [10], [11], and [12], mentioned a comparison between multiple biometric methods. This comparison is based on the following metrics:

- Measurability: the biometric parameters should be measured easily.
- Universality: the biometric trait that the system is working on should be common to all individuals involved.
- Permanence: biometric systems should be able to generate the same results for each individual and over time.
- Uniqueness: the biometric trait should be unique to every individual, and relatively stable over periods of time.
- Acceptability: biometric systems should be affirmed by the users for ease of use.
- Performance: biometric systems should be fast, accurate, and reliable when used for authentication.
- Collectability: biometric systems should be efficient in terms of data and trait capturing or collecting.

The metrics are classified across different biometric systems and are summarized in Fig. 1.

III. Literature Review

This section is divided into two categories: e-voting approaches with SFA and approaches with MFA methods, including biometrics. Each approach will be highlighted with its advantages and disadvantages.

A. E-Voting with SFA Approach

Because of the increased reliability of electronic systems in many fields, and especially in voting systems, the paper [13] suggested going further and implementing complex systems using this platform. They presented a new concept of a decentralized e-voting system based on a two-level architecture model that provides security without the redundancy of the previous systems. This proposal consists of performing six steps to ensure all requirements of the protocol are met, and it focuses on the transparency and anonymity of the voting system. This proposal is considered one of the best approaches for securing e-voting systems, but the absence of biometrics, which are essential in security approaches nowadays, can be a real threat that puts the voter or user at real risk of identity theft.

Depending on the structure of the blockchain network, the paper [14] designed a model that is implemented in a private blockchain network, and it doesn't require any platform to be installed; instead, it is reachable using the system devices, and not via the internet. The resulting votes and criteria are handled when directly requesting this data from the database that consists of two unrelated databases. The first one contains information about the people that are authorized to vote, the other one contains the blockchain and its related databases. The data is then processed and presented when needed. This voting model helps in reducing the hardware and software requirements and equipment, and thus reducing costs. But, at the same time, this system is vulnerable to malware due to the mining computers that are interconnected to the network.

Addressing biometric authentication systems and their accuracy and reliability in ensuring security, the paper [15] presented an e-voting system that relies on fingerprint authentication. This proposal consists of a fingerprint biometric sensor programmed using Python, and a web page developed using HTML and CSS, with the voting system handled using PHP. The system handles user and admin roles and actions, starting with user registration with their biometrics, casting their votes, and then publishing the results. This system showed improvements and enhancements over traditional voting systems (balloting) in terms of mobility, transparency, and efficiency.

B. Multi-Factor Authenticated Voting Systems Based on Blockchain

When it comes to two-factor authentication, or multi-factor authentication, which represent several layers of security checks to ensure systems are free from any kind of attacks, combined with biometric authentication, the paper [16] presented a multi-modal biometric authentication system, encrypted by firewalls that are installed on the servers, with fingerprint, iris scanning, and facial recognition authentication

methods. This proposal indicates high levels of security, but the implementation was not mentioned in the paper.

During this era of rising technology and the huge usage of mobile phones, many authors or researchers such as [17] focused on this field. The paper [17] proposed an m-voting (mobile voting) framework that works on MFA to authorize the voters before casting their votes, and then after they vote, this framework ensures that these votes are stored in a secure environment. This approach is easy to access and use, which helps elderly people or people with difficulties. In addition, this system covers the whole process, starting with user authentication, receiving the first OTP, choosing the preferred candidate and receiving the second OTP, and finally reaching the results counting and publication. The main concern in such mobile systems is that they can be a bit hard for some people to use, especially with this kind of technology, in addition to possible issues with mobile compatibility with these mobile systems (especially in the case of elderly people).

Similarly, the paper [18] presented a multi-modal system with fingerprint authentication and a cryptographically secured smart card. The technique requires the combination of an enhanced Feistel block cipher and first moment feature extraction technique for securing both confidential data on voters' smart cards and voters' fingerprint templates. This is done to avoid any failures upon registering fingerprints of the user. The paper [19] also proposed a multi-modal e-voting system, and relied on combining a facial recognition algorithm and RFID (Radio Frequency IDentification), and developing a smart contract that provides the required measures of integrity and verifiability for secure e-voting. This approach solves the problems of vote-rigging, voter impersonation, and vote falsification, thus providing a credible voting process.

IV. Proposed Model

In the interest of biometric authentication systems in securing software, and adding to the role of blockchain as well in this industry, our model is presented as a combination of these two security methods. Our proposed system relies on two biometrics: the first is fingerprint, and the other is the voice recognition system.

First, the user will register his fingerprint using a fingerprint machine, which will be later saved in our database. Upon login, he will be authorized. These user's data will be stored in our blockchain, in a distributed manner, to make sure there are no failures or any data loss. The blockchain-related functions are developed using Solidity language. After fingerprint registration, the system will ask the user to enter a preferred sentence of a specified number of characters. Then the user is redirected to a page to record this chosen sentence. After this step, the voice of the user, as well as his fingerprint data, will be stored digitally on our blockchain, to be used for comparison every time the user tries to login using new data to make sure the data complies with the actual correct data. When the user has registered his fingerprint and voice, and logs in, first the system will ask for the fingerprint. After this fingerprint is verified by the system, the user will need to say his preferred and registered sentence. Then, a comparison occurs and the user will, in case of acceptance of entered data, be authorized to log in and will have access to enter the application to cast his vote. Later, he is also able to view the results after the elections end. In Fig. 2, Fig. 3 and Fig. 4, we illustrate the steps of the whole process.

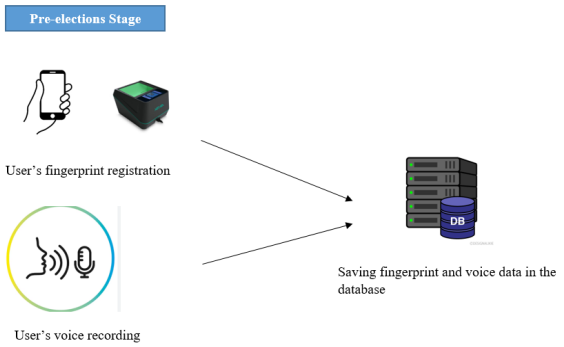

Fig. 2. Biometrics Registration and Storage in the Blockchain

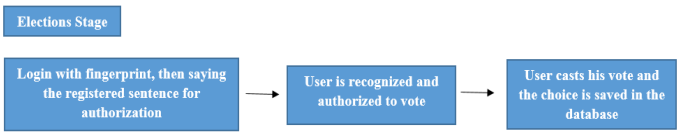

Fig. 3. Users Authorization, Voting, and Data Storage Stage

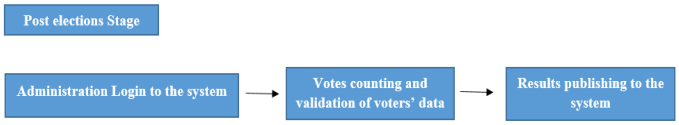

Fig. 4. Obtaining Votes, Auditing Results, and Publishing Stage

For user fingerprint registration, we used a fingerprint sensor machine, and Python for integration to detect allowed users' data and store it on the blockchain. The functionality of the system is developed with Python as well, and the user interface is coded with HTML and CSS to ensure ease in development and use. For integrating the machine (Raspberry Pi 3B+), we first checked the most suitable one with our OS, then we installed the needed libraries from the machine manufacturer that already contain the SDK for Python libraries, and then started our Python coding.

For voice registration, using Raspberry Pi 3B+, we connected a microphone to the Raspberry Pi's audio input. By

using Python as well, we captured audio input, processed it, and recognized speech patterns. By doing so, we recorded the user saying his preferred sentence with his own voice, and the sentence, in addition to his voice pattern, was saved in our databases (blockchain) for comparison when the user logs in to authenticate his data and is allowed to vote via our system. For both authentication systems to interact with users, we implemented the app on a web page to be accessible on computers and mobile phones. In Fig. 5, we illustrate our overall system.

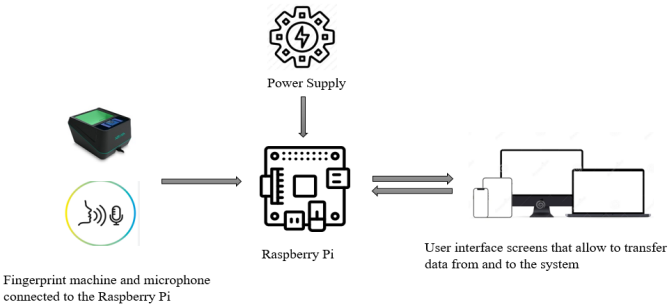

Fig. 5. Summary: Input Data, Implementation, and User Experience Model

V. Conclusion

In this paper, we proposed a blockchain-based e-voting system that relies on fingerprint and voice recognition methods for user authentication. When the allowed users register their fingerprint and use their preferred phrase for logging in later, their voting system can never be hacked, and their data stored on the blockchain can never be tampered with or manipulated. By using blockchain technology and multi-factor authentication methods, systems will acquire more privacy and security, and will be less vulnerable to threats and attacks, or data altering and tampering. We relied on previous studies to build our system and presented some of them in our sections. Our future work will include the implementation of this presented system in terms of functionality and user accessibility.

References

[1] A. Benabdallah, A. Audras, L. Coudert, N. El Madhoun, and M. Badra, "Analysis of blockchain solutions for e-voting: A systematic literature review," *IEEE Access*, vol. 10, pp. 70 746–70 759, 2022.

[2] S. Tanwar, N. Gupta, P. Kumar, and Y.-C. Hu, "Implementation of blockchain-based e-voting system," *Multimedia Tools and Applications*, vol. 83, no. 1, pp. 1449–1480, 2024.

[3] PrivacySense, "Single-factor authentication," *privacysense*, January 2023.

[4] O. Olaniyi, E. Dogo, B. Nuhu, H. Treiblmaier, Y. Abdulsalam, and Z. Folawiyo, "A secure electronic voting system using multifactor authentication and blockchain technologies," *Blockchain Applications in the Smart Era. EAI/Springer Innovations in Communication and Computing. Springer, Cham.*, 2022.

[5] F. P. Hjalmarsson and G. K. Hreioarsson, "Blockchain-based e-voting system," *2018 IEEE 11th International Conference on Cloud Computing (CLOUD)*, July 2018.

[6] U. C. Çabuk, E. Adıgüzel, and E. Karaarslan, "A survey on feasibility and suitability of blockchain techniques for the e-voting systems," *International Journal of Advanced Research in Computer and Communication Engineering*, March 2018.

[7] E. Ahmadieh and N. El Madhoun, "Artwork nfts for online trading and transaction cancellation," *2023 Fifth International Conference on Blockchain Computing and Applications (BCCA)*, October 2023.

[8] J. K. Adeniyi, S. A. Ajagbe, E. A. Adeniyi, P. Mudali, M. O. Adigun, T. T. Adeniyi, and O. Ajibola, "A biometrics-generated private/public key cryptography for a blockchain-based e-voting system," *Egyptian Informatics Journal*, January 2024.

[9] "Biometrics: definition, use cases, latest news," *Identity and Biometric Solutions*, 2023.

[10] N. Singh, A. Agrawal, and R. Khan, "Voice biometric: A technology for voice based authentication," *American Scientific Publishers*, 2018.

[11] H. Srivastava, "A comparison based study on biometrics for human recognition," *IOSR Journal of Computer Engineering 15(1):22-29*, 2013.

[12] O. M. Olaniyi, J. A. Bala, S. Ganiyu, Y. S. Abdulsalam, and C. E. Eke, "Voice recognition systems for the disabled electorate: Critical review on architectures and authentication strategies," *Computer Engineering and Applications (ComEngApp) Journal*, 2023.

[13] K. Isirova, A. Kiian, M. Rodinko, and A. Kuznetsov, "Decentralized electronic voting system based on blockchain technology developing principals," *CEUR-WS.org/Vol-2608/paper17.pdf*, 2020.

[14] C. Ribon, J. Leon, and O. Corredor, "Design of an electronic voting system using a blockchain network," *Cooperative University of Colombia, Faculty of Engineering, Telecommunications Engineering, Bogotá*, 2019.

[15] B. U. Umar, O. M. Olaniyi, L. Ajao, D. Maliki, and C. Okeke, "Development of a fingerprint biometric authentication system for secure electronic voting machines," *School of Electrical and Engineering Technology (SEET)*, 2019.

[16] J. Bhatti, S. Chachra, A. Walia, and A. Vishal, "Secure electronic voting machine using multi-modal biometric authentication system, data encryption, and firewall," *International Journal of Performability Engineering*, 2019.

[17] T. P. Abayomi-Zannu, I. Odun-Ayo, and T. Barka, "A proposed mobile voting framework utilizing blockchain technology and multi-factor authentication," *International Conference on Engineering for Sustainable World*, 2019.

[18] B. Oke, O. Olaniyi, A. Aboaba, and A. O.T, "Developing multifactor authentication technique for secure electronic voting system," *IEEE International Conference on Computing, Networking and Informatics (ICCNI 2017)*, 2017.

[19] O. Olaniyi, E. Dogo, N. B.K, H. Treiblmaier, Y. Abdulsalam, and Z. Folawiyo, "A secure electronic voting system using multifactor authentication and blockchain technologies," *Blockchain Applications in the Smart Era (pp.41-63)*, 2022.