Egyptian Informatics Journal 25 (2024) 100447

Contents lists available at ScienceDirect

Egyptian Informatics Journal

journal homepage: www.sciencedirect.com

A biometrics-generated private/public key cryptography for a blockchain-based e-voting system

Jide Kehinde Adeniyi [a,1], Sunday Adeola Ajagbe [b,c,*], Emmanuel Abidemi Adeniyi [d,1], Pragasen Mudali [b], Matthew Olusegun Adigun [b], Tunde Taiwo Adeniyi [e], Ojo Ajibola [a]

[a] Department of Computer Science, Landmark University, Omu-Aran, Nigeria
[b] Department of Computer Science, University of Zululand, Kwadlangezwa 3886, South Africa
[c] Department of Computer Engineering, First Technical University, Ibadan 200255, Nigeria
[d] College of Computing & Communication Studies, Bowen University Iwo, Nigeria
[e] Department of Computer Science, University of Ilorin, Ilorin, Nigeria

ARTICLE INFO

Keywords:
Biometrics
Cryptography
Blockchain
E-voting system
Private key

ABSTRACT

Voting aims to provide the best decision or select the most selected option for the largest group of voters. Malicious parties gaining access, and otherwise tampering with election results, or the votes make this effort counterproductive. To alleviate this, this study examined the introduction of blockchain. The transparent and immutable nature of the blockchain makes this data impossible to alter and allows the election results to be transparent. To further increase the transparency of the system while keeping voters anonymous, a biometric based cryptography was introduced. The biometric was introduced as the source for the private key for each voter while a public was generated to act as the identity of the voter. The biometric trait of each individual is unique and cannot be forged, hence the identity of the voter is secured. The public key available cannot be traced by to the private key, hence, identity of the voter is anonymous. The system showed an encouraging performance after testing.

1. Introduction

After conversations, political arguments, or campaigning, a gathering such as a meeting or an electorate can come to an agreement or make a statement through voting [1]. The goal of voting is to make the best decision or choose the most popular alternative for the greatest number of people. On a paper ballot, voters mark their votes by filling in a shape as required by the electoral committee. Paper ballots were screened and consequently recorded at the polling site or at a centralized location [2]. No electronic machine is used in this type of paper-based polling [3]. The paper-based polling method can be very costly, and it was prone to many malicious attackers at the point of voting. User identities could be stolen, papers could be swapped, ballots could be stolen, miscalculations could be made, and results could be altered. Overall, paper-based voting is prone to many forms of attack [3]. This led to the introduction of electronic voting.

Electronic voting refers to the use of Information and Telecommunication devices in the process of casting and collating votes. Electronic voting can take the form of freestanding electronic voting machines. It could also merely involve computers connected to the Internet. Some electronic voting could cover a wide range of Internet services, from the transfer of results to a more robust online voting platform that can be accessed using very easily accessible devices [4,5]. It usually entails a robust electronic system which supports vote casting, vote collation, encryption of the data, and movement of all the aforementioned information to servers, as well as election results accumulation and summarization. How electronic voting is used depends on the use-case required, and how it is implemented by the electoral body [6].

While the aforementioned electronic system reduces voting stress significantly, a "good" voting system as described by [7] is a system that must satisfy a variety of sometimes conflicting objectives, whether it is computerized, paper ballots, or mechanical devices. The secrecy of a voter's votes must be guarded, not just to help guarantee the voter's security while trying to vote against a malignant candidate, but also in

* Corresponding author at: Department of Computer Science, University of Zululand, Kwadlangezwa 3886, South Africa.
E-mail addresses: adeniyi.jide@lmu.edu.ng (J.K. Adeniyi), saajagbe@pgschool.lautech.edu.ng (S.A. Ajagbe), abidemi.adeniyi@bowen.edu.ng (E.A. Adeniyi), MudaliP@unizulu.ac.za (P. Mudali), adigunm@unizulu.ac.za (M.O. Adigun), taiwo.jide@unilorin.edu.ng (T.T. Adeniyi), ojo.ajibola@lmu.edu.ng (O. Ajibola).
[1] Landmark University SDG 4 (Quality Education).

https://doi.org/10.1016/j.eij.2024.100447
Received 18 May 2023; Received in revised form 20 December 2023; Accepted 20 January 2024
Available online 25 January 2024

order ensure that voters have no proof as to who they nominated or voted for [8]. This electronic voting system is still quite flawed, data integrity is more easily compromised, there is no transparency, the administrator of such a system could easily alter the results, and a lack of verifiable paper-trail makes it harder for voters to certify their votes [9]. To solve the problem of transparency, data compromise and verification, the introduction of blockchain and biometrics would of immense importance [10,11].

The term "blockchain" refers to a growing collection of records that are connected cryptographically. Each block includes some information about the transaction, which are: the transaction data, the timestamp, and a cryptographic hash of the block that precedes that block [12]. The timestamp helps to ensure that the transaction data was available at the moment the block was published in order to enter the hash [13]. They form a chain with each new block supporting the ones before it since each block provides information about the one before it. Blockchains are thus impervious to falsification since, once stored, the data in any one block cannot be changed subsequently without affecting all succeeding blocks [14]. In order to store such information on the blockchain, a program is deployed on the blockchain known as a smart contract, which enables updating and removal of voting information [15]. To automate the execution, control, and documentation of legally relevant events and actions in line with the terms of a contract or agreement, smart contracts are the computer programs or transaction protocols responsible for this [16].

Biometrics is the use of an individual's behavioural or physiological trait for recognition [16]. It primarily aims at recognizing an individual using how an individual does something (behavioural) or what an individual is born with (physiological). Examples of behavioural biometric include speech recognition, gait recognition and so on [17]. Face recognition, fingerprint recognition are examples of physiological recognition [18,19]. Major contributions of the proposed method in this study are as follows:

i. the study proposes the use of smart contracts for application logic, biometric-based cryptography and storing of voting information on the blockchain.
ii. introduces the fingerprint biometric identification layer to reduce voter fraud and increase the credibility and verifiability of an election.
iii. the initial stage involves scanning the authorized voters' fingerprints, collecting the data from them.
iv. data collected was used to generate secret and public keys unique to that voter. It is unique because it generated from the fingerprint which is a distinct feature of every authorized voter.

The remaining part of this research is organized as follows. Section 2 presents the review of the related studies. Section 3 presents the methodology for this study. Section 4 implementation results and discussion. Section 5 concludes the study and presents future works for the realization of effective e-voting.

2. Review of the related works

Several literatures have examined electronic voting with the aim of increasing credibility and verifiability in elections. Some of the literatures are examined in this session. Amongst the notable literatures in this area of study is the work of Hassan et al. [9]. Their study examined a liquid democracy enabled blockchain-based electronic voting system. In their study, they examined how electronic voting can be used in elections as a service. They examined the use of distributed ledgers in fine-tunning election collation. Their aim was to improve security and reduce the cost incurred in the election process. They noted in their study however that Scalability issues are exacerbated as the number of nodes in the blockchain network grows.

Verma [1] presented an e-voting framework in their study. The framework was designed to ensure security, confidentiality and reliability. In their system, a key is generated during registration. After which a hash is created. Each candidate block on the blockchain increases as votes are casted in their favour. A central database is kept on the cloud and this database manages the blockchain created. The fingerprint of the voter is also collected at registration and it is used to generate the hash. The hash is kept at the beginning of each blockchain. In their system, the fingerprint did not really play any major part in the voting system.

Al-maaitah et al. [20] presented a blockchain based e-voting system for Jordan election. In their system, hyper ledger fabric was used as a platform for the creation of blockchain. The main units of the system include stakeholders, frontend, backend, hyper ledger blockchain, database and the consensus algorithm. Votes are casted using the client-side application (front-end). The backend used the hyper ledger fabric SDK to interact with request from voters and candidates. This was sent to the server. Transactions are generated through smart contracts and these transactions are saved on the blockchain. The consensus algorithm unifies the work of the individual units.

Jumaa et al. [21] proposed smart contract-based e-voting system with the use of a decentralized private blockchain. The system was designed with existing Elliptic Curve Cryptography (ECC) cryptosystem for dependability, anonymity and security of the voting systems. A mobile application was proposed for voting, the QRcode is scanned for election registration. The fingerprint or face is used for authentication and then the user can cast a vote. The casted vote is encrypted using ECC algorithm.

Sherine et al. [22] proposed a mobile e-voting system using a 3-step security process before casting a vote. The system was designed for students to vote anywhere, at any time. The three security steps include a captcha, phone One Time Password (OTP) and fingerprint verification. The authentication steps are primarily aimed at authenticating the use of the voting application. The have less use when the actual voting is concerned.

Rao et al. [13] presented a voting system that is independent of the blockchain platform. In their system, voters interact with a front-end smart contract server, under the supervision of a Smart contract administrator. A voter administrator manages and collates the votes. The smart contract is then validates the vote and added to the blockchain. Voters are required to register, during which a secret and public key is assigned to the voter.

Yang et al., [15] suggested Deep Improving Commute Experience (DeepICE), a cutting-edge blockchain-enabled model, to enhance the commuter experience for private car owners by forecasting the best times to leave and arrive. In this model, privacy concerns raised by private car users are addressed by developing a blockchain with a consensus mechanism. The authors also suggested using a graph convolution network (GCN) method enabled by multitask learning to capture the intricate relationships and features between two tasks, such as the departure time and travel cost, and then build a model to predict these two tasks. The experimental findings show that the suggested model performs better than current methods.

3. Methodology

In this study, the initial stage involves scanning the authorized voters' fingerprints, collecting the data from them. After this data has been collected, it was used to generate secret and public keys unique to that voter. It is unique because it generated from the fingerprint which is a distinct feature of every authorized voter.

When the keys have been generated from the fingerprints, these keys can then be imported into a cryptocurrency wallet like Meta-mask for easy connection with Decentralized Applications (DAPPs) anytime (i.e., logging into DAPPs without using username and password, rather just by connecting your wallet to the application). These keys can then be used to interact with the voting DAPP which is the web 3.0 application that

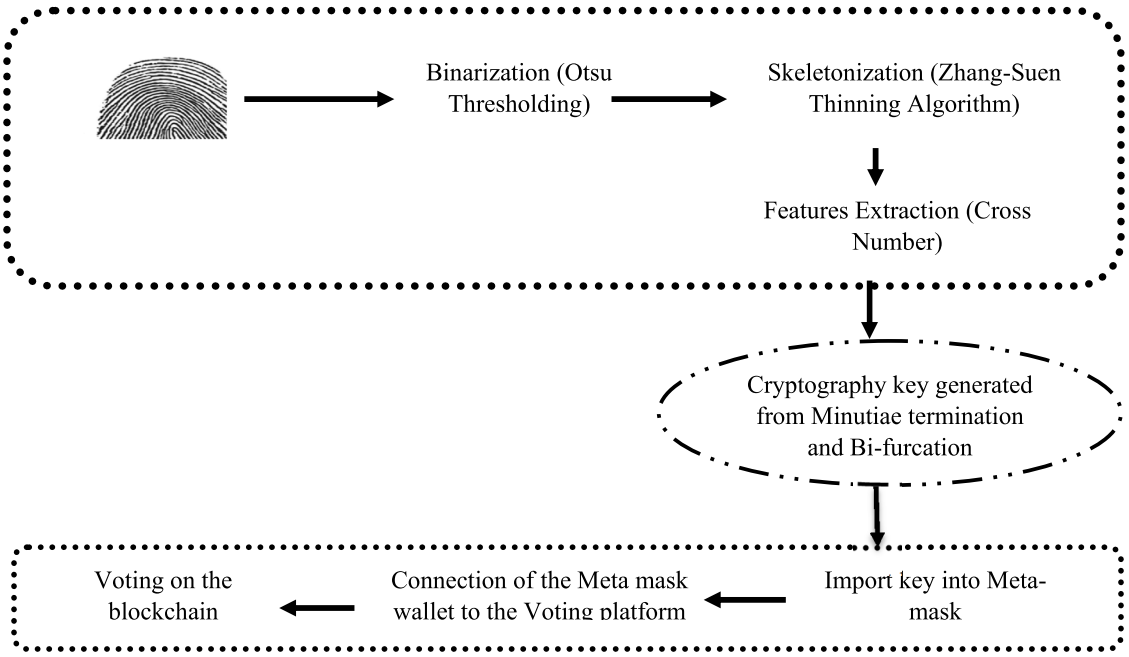

Fig. 1. Block diagram of the proposed e-voting system.

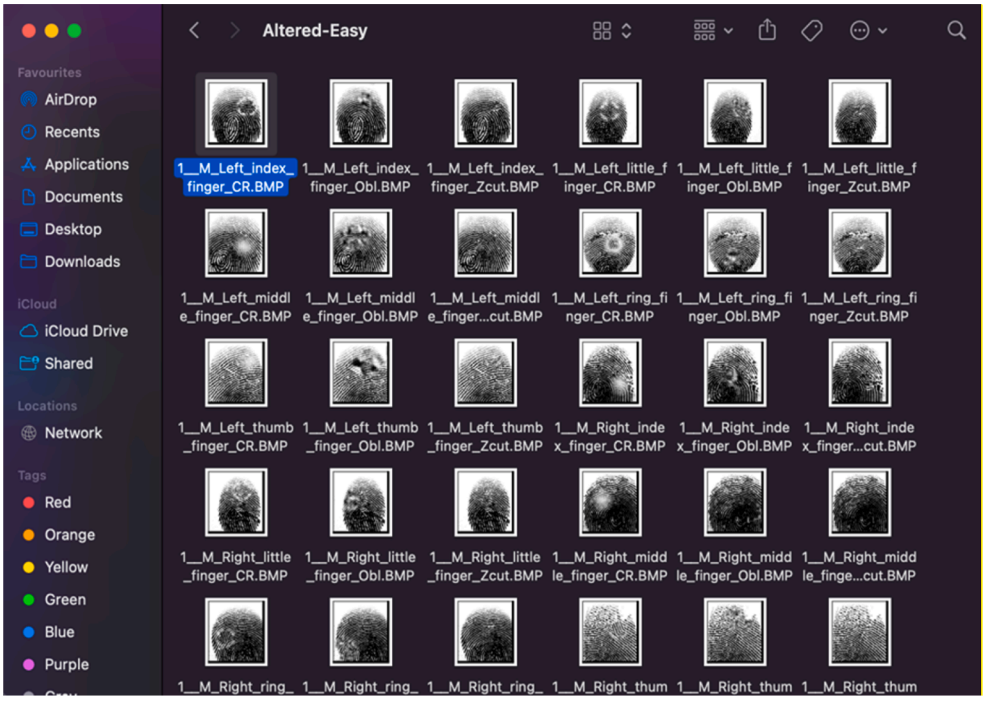

Fig. 2. Sample SOCOFing Images.

the voters will interact with to cast their votes [23]. Once their votes have been casted, the votes cannot be altered, and everyone would be able to see that a particular person has voted since they know the public key of the voter. However, since the public is just a sequence of random strings, no one can tell who it is exactly, and by that, voter was granted anonymity and his/her vote, immutability. This is enforced by the smart contracts provided by blockchain technology. The block diagram of the system is depicted in Fig. 1.

3.1. *Fingerprint data source*

The Sokoto Coventry fingerprint dataset obtained from Kaggle repository (https://www.kaggle.com/datasets/ruizgara/socofing) was used for this study. The Sokoto Coventry Fingerprint Dataset (SOCOFing), a biometric fingerprint database was designed for academic research purposes. SOCOFing is made up of 6,000 fingerprint images from 600 African subjects. Fig. 2 shows some images of fingerprints in the dataset [24]. The cv2 library was used to load the image into the program and also used to display the image. Fig. 3 below shows a sample of a fingerprint image loaded into the system.

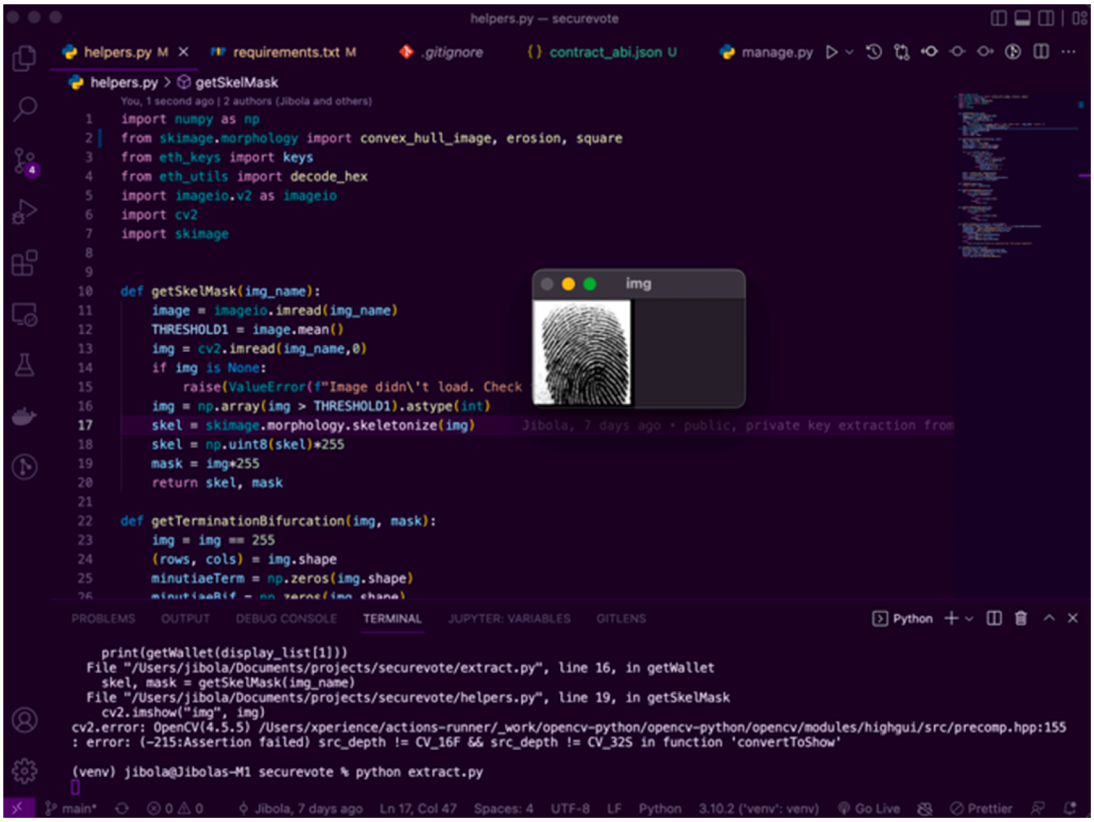

Fig. 3. Loading a fingerprint image.

3.2. Fingerprint image pre-processing

Image preprocessing is a step carried out on images before features are extracted. It is mostly targeted at one or more of the following: noise removal, grey scale conversion, binarization, thinning, amongst others. The aim is to get the image ready for features to be extracted. In the proposed system, the preprocessing stages followed are binarization and skeletonization [14].

3.2.1. Binarization

Binarization converts images from digital to binary format based on the threshold value of the original image's pixel intensity [25]. The image intensity threshold is either chosen by the user or generated automatically by the application. Pixels are transformed to 0 or 255 depending on whether they are above or below the threshold value. Thresholding divides the foreground (black) from the background of an image (white). For this study, Otsu thresholding was used. Binarization was chosen because there is need to extract minutae and it must be a thin and compact line.

3.2.2. OTSU thresholding

The propose of introducing Otsu thresholding is to obtain a binary representation of the fingerprint image. This implies that the ridges and valleys of the fingerprint will be properly separated. The key principle of Otsu's method is to separate the image into the background and foreground. This is achieved by maximizing the variance between-class. Otsu's method uses the histogram of an image, which is a dimensional array. The term optimal threshold is used for the corresponding threshold grey value for classification [26,27]. Otsu uses double thresholding instead of a single like its peers. This makes it produce a more compact output than its counterparts.

An image with pixel total of N, the probability P_i of each pixel in the grey image in given in (1).

$$P_i = \frac{n_i}{N}, i = 0, 1, 2, \cdots, L-1 \tag{1}$$

where the number of pixels with grey value i is n_i and the payert pray value is $L-1$. Suppose k is the initial value of the threshold [28]. This threshold is used to separate all the image's pixels into two such that each grey value belongs to 0 to $k-1$. Eq. (2) is used to obtain the between-class variance (σ_B^2). The initial value of k is usually set 1, and the maximum variance between- class when $k = 1, 2, 3, \cdots, L-2$ is computed. The segmentation threshold k that maximizes σ_B^2 is finally calculated, noting that $w_0, w_1, \mu_0, \mu_1, \mu_r$ are given in (3), (4), (5), (6), (7) respectively:

$$\sigma_B^2 = w_0(\mu_0 - \mu_r)^2 + w_1(\mu_0 - \mu_r)^2 \tag{2}$$

$$w_0 = \sum_{i=0}^{k-1} P_i \tag{3}$$

$$w_1 = \sum_{i=k}^{L-1} P_1 = 1 - w_0 \tag{4}$$

$$\mu_0 = \sum_{i=0}^{k-1} iP_i/w_0 \tag{5}$$

$$\mu_1 = \sum_{i=k}^{L-1} P_i/w_1 \tag{6}$$

$$\mu_r = \sum_{i=0}^{L-1} P_i \tag{7}$$

3.2.3. Skeletonization

In this study, Zhang-Suen skeletonization algorithm was proposed. Zhang-Suen fast parallel Skeletonization algorithm is aimed at producing a compact representation of pixels. If the target point is marked 1 and the background is 0. Taking the point at the boundary as 1, the 8 neighbouring pixels has at least a pixel marked 0. Following the algorithm, the neighbouring pixels need to undergo the following steps

Table 1
A central pixel B1 and 8 neighbouring pixels.

B9	B2	B3
B8	B1	B4
B7	B6	B5

Table 2
Pixel P and surrounding eight pixels.

P_4	P_3	P_2
P_5	P	P_1
P_6	P_7	P_8

Table 3
CN values and their corresponding meaning.

CN	Pixel
0	Isolated point
1	Ending point
2	Connective point
3	Bifurcation point
4	Crossing point

[29,30]. Suppose the central point was $B1$ and the 8 neighbouring pixels are labelled $B2, B3, \cdots, B8$ in a clockwise manner. Suppose $B2$ was above the central point $B1$ as shown in Table 1. Then all points that meet the following requirements are selected:

$$2 \leq N(B1) \leq 6$$

$$S(B1) = 1$$

$$B2 \times B4 \times B6 = 0$$

$$B4 \times B6 \times B8 = 0$$

Where N(B1) is the number of non-zero neighbouring points. S(B1) is the number of 0 to 1 change(s) in the sequence of B1, B2, …, B9. After this inspection, all marked points are eliminated. Following the first step, the requirements (c) and (d) are changed to $B2 \times B3 \times B4 = 0$ and $B2 \times B6 \times B8 = 0$ respectively. The marked points after the analysis are also eliminated. The two steps above are repeated until no points fulfil the requirement; hence, producing a skeleton representation of the pixels.

3.3. Extracting minutiae features

Features extracted in this study are the fingerprint's termination and bifurcation. To extract these features, cross number was used. Bifurcation and Ridge-ending detection was done using Cross Number (CN). The number can be calculated using (8) and Table 2. Cross number values and their associated CN value are shown in Table 3. Fig. 4 shows the minutiae features extracted from a typical fingerprint [31,32].

$$CN = \frac{1}{2}\sum_{i=1}^{8} |P_i - P_{i+1}| \tag{8}$$

3.4. Generating private key from minutiae features

The private key proposed in this paper is a 256-bit integer. To generate the private key from minutiae features, a fixed length binary string is generated from a combination of the matrix generated by the terminations and bifurcations. The program generating the private key and the public address from fingerprint images from minutiae feature were implemented.

3.4.1. Generating public key from minutiae features

The public key is generated through elliptic curve digital signature algorithm (ECDSA). ECDSA uses elliptic curve obtained in a finite field to get and confirm signatures. The security and efficiency of the process of signing is increased because of the elliptic curve, as it relies on how complex elliptic-curve discrete logarithm problem is. It can also be viewed as elliptic curve analogues of older discrete algorithm crypto-

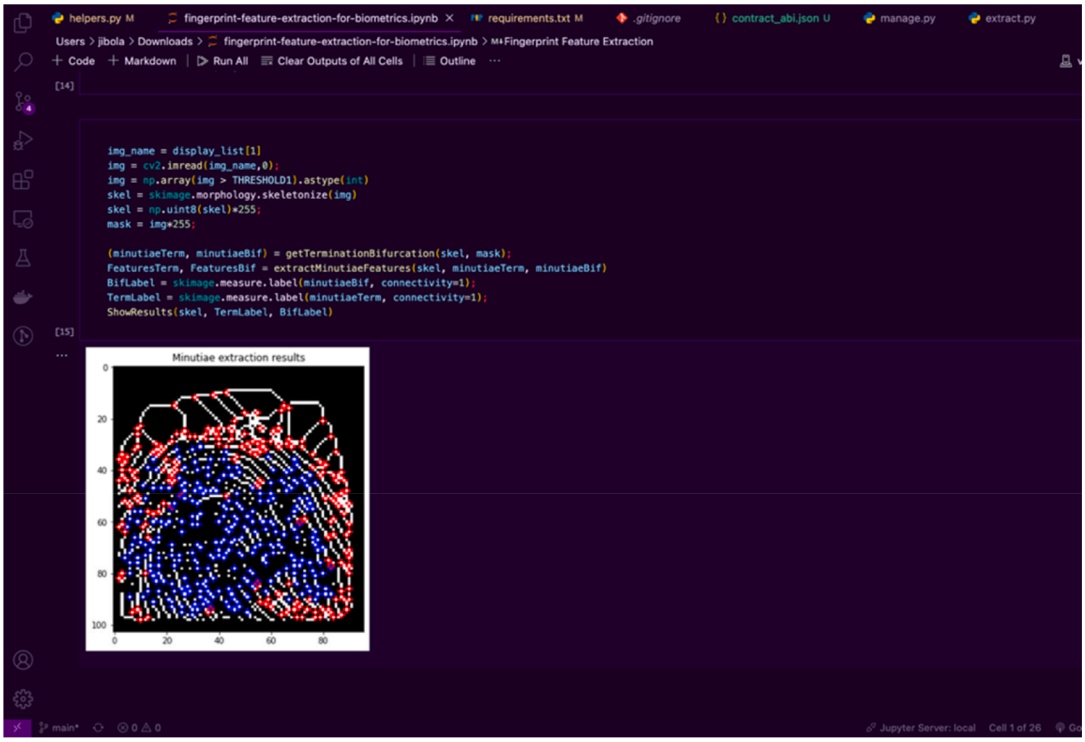

Fig. 4. Minutiae Features Extracted.

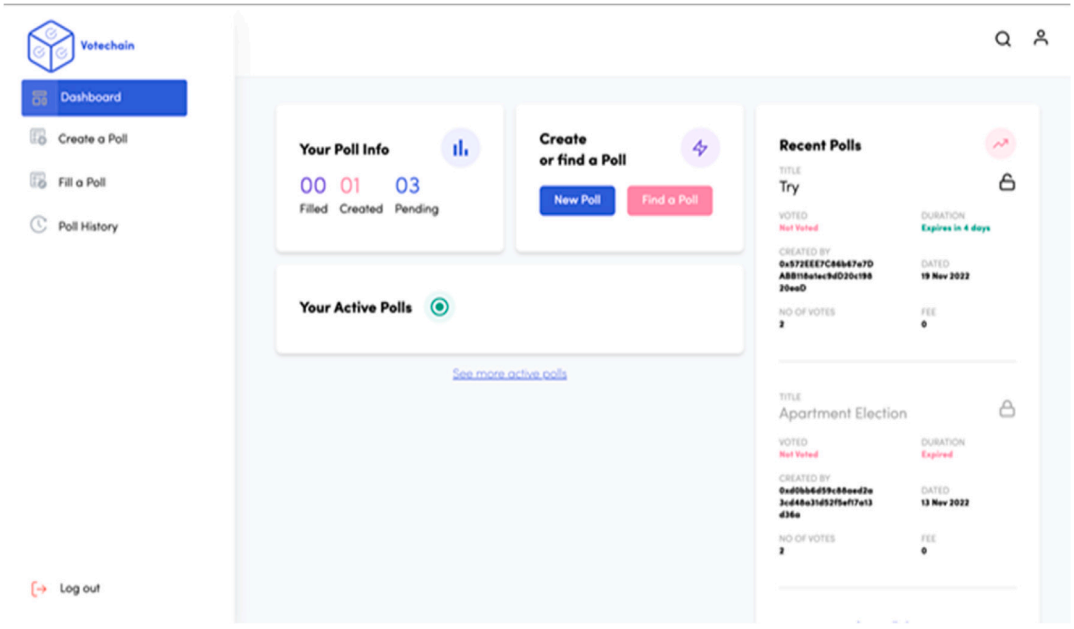

Fig. 5. The general dashboard of the Vote-chain application.

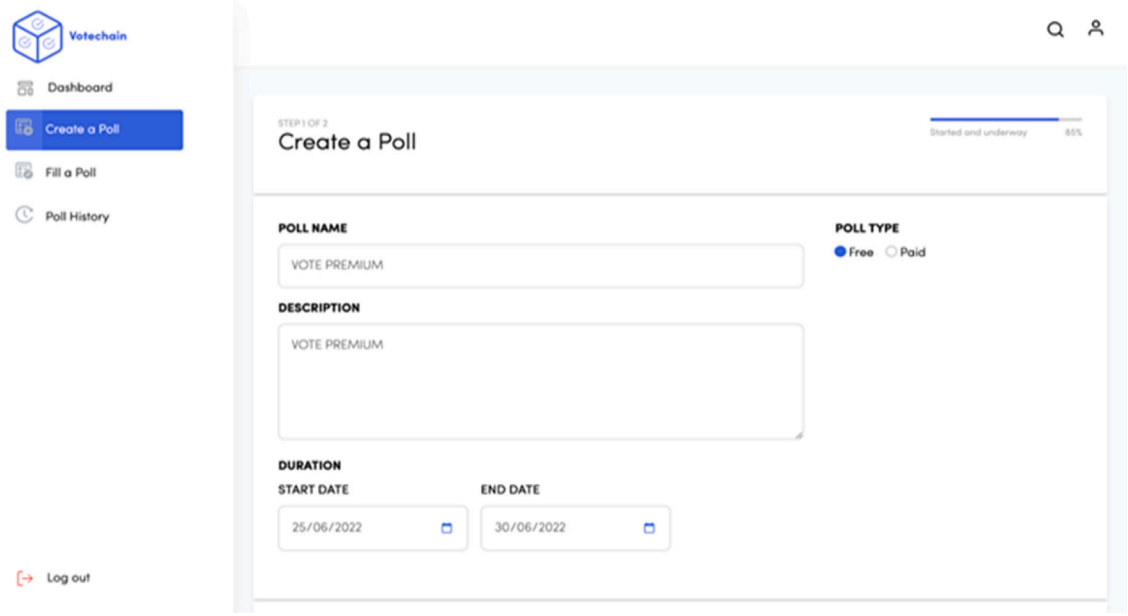

Fig. 6. User Interface to create a poll.

system such that the subgroup Z_p^* is substituted by the group of points on an elliptical curve over a finite field. An elliptic curve E over Z_p is defined by the cartesian coordinate system in (9).

$$y^2 = x^3 + ax + b \tag{9}$$

Where $a, b \varepsilon Z_p$, and $4a^3 + 27b^2 \neq 0\,(mod\,p)$, include special point O (termed point at infinity). The set $E(Z_p)$ is made up of all points (x, y), $x\varepsilon Z_p$, $y\varepsilon Z_p$, which satisfy the defining equation and O. A different elliptic curve is obtained from each value of a and b. The private key is a random number (obtained from the fingerprint) and the public key is the result of the multiplication of the private key with a generator point G in the curve [33–35].

4. Results of the implementation and discussion

After creating a poll, the voting options are entered into the system. In the interface, there are three options from which the voter can only cast for one. The details of the duration of the voting period are stated on the interface and the public key of the poll creator is also included. Each interaction with the smart contract sends a request to the user on the Meta-mask browser wallet. The general interface of the vote-chain application is shown in Fig. 5. The details used to create a poll using the decentralized voting application is shown in Fig. 6. Fig. 7 shows voting option entering interface and how a poll is created, it is the interface for the second step involved in creating a poll, which is adding the options. Fig. 8 shows an interface of a poll with options for users to vote for.

The voting system allowed voters to vote on the block chain

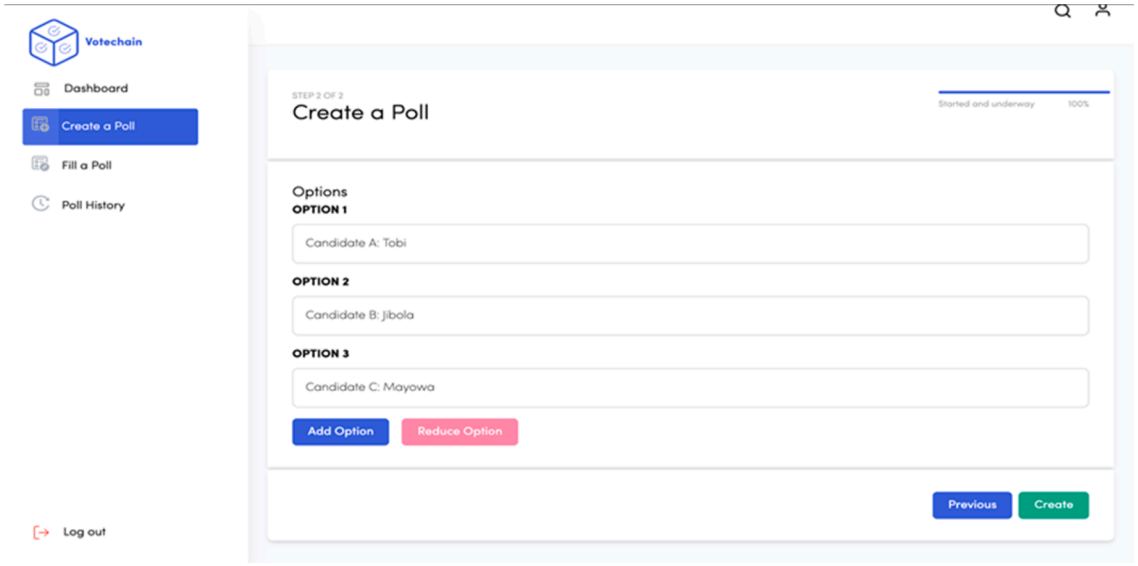

Fig. 7. Interface for the second step involved in creating a poll.

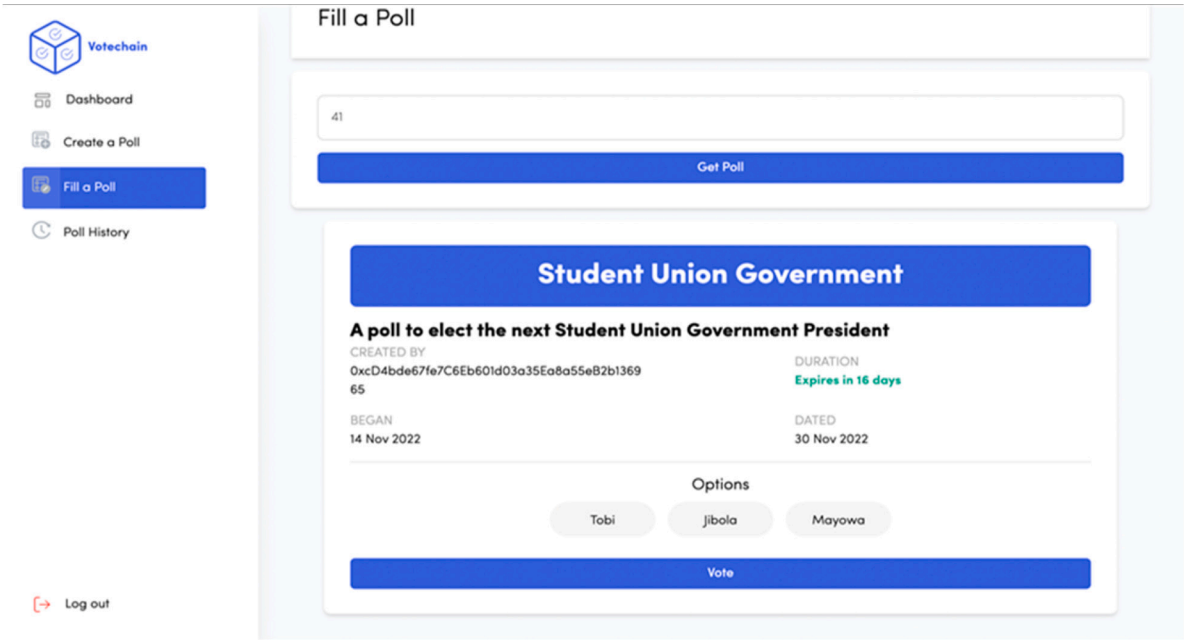

Fig. 8. Interface of a poll with possible options a user can vote for.

platform. The voting was simulated with users using the fingerprint database. It may be easy or difficult to ensure that election results are more trustworthy depending on the number of parties involved in the voting process. It might be feasible to use paper ballots and manual counting in elections with a small number of voters. However, because counting is done by hand, the traditional ballot voting system tends to be inaccurate as the population of people who can vote grows. The introduction of electronic means is a result of technological advancement. On a large scale, this has been found to be more cost-effective and efficient when there is no interference. Nevertheless, the election results are unreliable due to interference. Thus, a transparent block chain voting system based on fingerprints was created to guarantee greater legitimacy and confidence in elections [36]. The electronic voting system was constructed using blockchain technology, and fingerprint features were used to generate the public/private key pair that allowed users to sign transactions and vote on the blockchain.

5. Conclusion

The goal of voting is to make the best decision or choose the most popular alternative for the greatest number of people. Any part of the process that impedes the credibility of the results of such an election defeats the purpose of the voting. Depending on the number of parties involved in voting, ensuring that election results are more trustworthy may be deemed easy or difficult. In elections involving a small number of voters, using paper ballots and manually counting may be possible. However, as the population of the voting individuals increase, the traditional ballot voting system tends to be erroneous as counting is manually done. The advancement of technology has led to the introduction of electronic means. Without interference, this have been found to be more efficient and cost effective on a large scale. However, in the case of interference, the results from this election cannot be trusted. Hence, a fingerprint based transparent block chain voting system that

ensures more credibility and trust in elections was developed. Blockchain technology was used to build the electronic voting system, and the public/private key pair used that was used to allow users sign transactions (thereby voting on the blockchain) was generated using fingerprint features. An image of the fingerprint is first capture and preprocessed. Features were then extracted from the preprocessed image. From the extracted features, a 256-bit private key is generated and used with an elliptic curve digital signature algorithm generated public key for voting. The public key identifies a vote without exposing the voter and the private key is used to verify if an individual has voted before. The private key is hidden; hence it is difficult for impersonators to intrude into the block of votes. Both key pairs are linked in the wallet as at the time of enrolment of the fingerprint by the user. The system was tested on a population of 400 voters with each assigned a fingerprint set of an individual in the socoprint database and the result showed that each voter was able to vote without his/her identity being compromised. Likewise, the introduced biometrics made login and voting process seamless. We hope to introduce an hybrid encryption system in our future study.

CRediT authorship contribution statement

Jide Kehinde Adeniyi: Conceptualization, Methodology, Writing – original draft, Data curation, Visualization, Software. **Sunday Adeola Ajagbe:** Conceptualization, Methodology, Writing – original draft, Data curation, Project administration, Validation, Resources, Visualization, Software. **Abidemi Emmanuel Adeniyi:** Conceptualization, Methodology, Writing – original draft, Data curation, Project administration, Methodology, Validation. **Pragasen Mudali:** Software, Resources, Writing – review & editing, Supervision. **Matthew O. Adigun:** Software, Resources, Writing – review & editing, Supervision. **Tunde Taiwo Adeniyi:** Project administration, Methodology, Validation. **Ojo Ajibola:** Writing – original draft, Data curation, Resources, Visualization, Software.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data Availability Statement.

The data used to support the findings of this study are available from the corresponding author upon request.

References

[1] Verma G. A Secure Framework for E-Voting Using Blockchain. 2022 Second International Conference on Computer Science, Engneering and Applications (ICCSEA). 2022.

[2] S.S. Gandhi, A.W. Kiwelekar, L.D. Netak, H.S. Wankhede, Security requirement analysis of blockchain-based e-voting systems, in: Intelligent Communication Technologies and Virtual Mobile Networks. Lecture Notes on Data Engineering and Communications Technologies, vol. 131, G. Rajakumar, K. L. Du, C. Vuppalapati and G. N. (. Beligiannis, Eds., Springer, Singapore, 2023, pp. 73-85.

[3] Jafar U, Aziz MJA, Shukur Z. Blockchain for electronic voting system—review and open research challenges. Sensors 2021;21:584.

[4] Benabdallah ALI, Audras A, Coudert L, Madhoun NEL, Badra M. Analysis of blockchain solutions for e-voting: a systematic literature review. IEEE Access 2022; 10:70746–59.

[5] Y. Kho and S. Heng, "A Review of Cryptographic Electronic Voting," Symmetry (Basel), 2022, pp. 1-3, 14.

[6] Baudier P, Kondrateva G. Peace engineering: The contribution of blockchain systems to the e-voting process. Technol Forecast Soc Chang 2020;162:120397.

[7] Kohno T, Stubblefield A, Rubin AD, Wallach DS. Analysis of an Electronic Voting System. Proceedings of the 2004 IEEE Symposium on Security and Privacy (S&P'04). 2004.

[8] Li C, Dong M, Xin X, Li J, Chen X, Ota K. Efficient Privacy Preserving in IoMT With Blockchain and Lightweight Secret Sharing. IEEE Internet Things J 2023;10(24): 22051–64.

[9] Hassan CA, Hammad M, Iqbal J, Hussain S, Ullah SS, AlSalman H, et al. A Liquid Democracy Enabled Blockchain-Based Electronic Voting System. Sci Program 2022;2022:1–10.

[10] Goyal J, Ahmed M, Gopalani D. A Privacy Preserving E-Voting System with Two-Phase Veri cation based on Ethereum Blockchain. Res Sq 2022:1–33.

[11] Blanchard E, Gallais A, Leblond E, Sidhoum-Rahal D, Walter J. "an Analysis of the Security and Privacy Issues of the Neovote Online Voting System", in Electronic Voting (lecture Notes in Computer Science) 2022;vol. 13553:1–18.

[12] Yaqoob I, Salah K, Jayaraman Rea. Blockchain for healthcare data management: opportunities, challenges, and future recommendations. Neural Comput Application 2022;34:11475–90.

[13] Rao KV, Panda SK. Secure electronic voting (e-voting) system based on blockchain on various platforms. Comput Commun Netw IoT 2022.

[14] Guo Y, Zhang C, Wang C, Jia X. Towards public verifiable and forward-privacy encrypted search by using blockchain. IEEE Trans Dependable Secure Comput 2023;20(3):2111–26.

[15] Yang J, Yang K, Xiao Z, Jiang H, Xu SDS. Improving commute experience for private car users via blockchain-enabled multitask learning. IEEE Internet Things J 2023;10(24):21656–69.

[16] Malhotra M, Kumar A, Kumar S, Yadav V. Untangling E-Voting Platform for Secure and Enhanced Voting Using Blockchain Technology. In: Al-turjman F, Yadav SP, Kumar M, Yadav V, Stephan T, editors. Transforming Management with AI, Big-Data, and IoT. Cham.: Springer; 2022. p. 51–72.

[17] Arora S, Bhatia MPS. Challenges and opportunities in biometric security: a survey. Inf Secur J A Glob Perspect 2021:1–21.

[18] Ipeayeda FW, Oyediran MO, Ajagbe SA, Jooda JO, Adigun MO. Optimized gravitational search algorithm for feature fusion in a multimodal biometric system. Results Eng 2023;20(4):101572.

[19] Singh K, Kaur K, Sardana A. Fingerprint feature extraction 1 2. Int J Comput Sci Technol 2011;2(3):237–41.

[20] Al-maaitah S, Quzmar A, Qatawneh M. Blockchain-based E-Voting System for Election in Jordan. J Theor Appl Inf Technol 2022;100(5):1584–93.

[21] Jumaa MH, Shakir AC. Iraqi E-Voting System Based on Smart Contract Using Private Blockchain Technology. Informatica 2022;46(2):87–94.

[22] Sherine A, Peter G, Stonier AA, Ping DWL, Praghash K, Ganji V. Development of an Efficient and Secured E-Voting Mobile Application Using Android. Mob Inf Syst 2022;2022:1–10.

[23] Liu X, Zhou G, Kong M, Yin Z, Li X, Yin L, et al. Developing multi-labelled corpus of twitter short texts: a semi-automatic method. Systems 2023;11(3):390.

[24] Shehu YI, Ruiz-garcia A, Palade V, James A. Sokoto coventry fingerprint dataset. arXiv 2018;2018:5–7.

[25] K. Cao, H. Ding, W. Li, L. Lv, M. Gao, F. Gong and B. ... Wang, "On the Ergodic Secrecy Capacity of Intelligent Reflecting Surface Aided Wireless Powered Communication Systems," IEEE Wireless Communications Letters, p. 1.

[26] Han H, Deng H, Dong Q, Gu X, Zhang T, Wang Y. An Advanced Otsu Method Integrated with Edge Detection and Decision Tree for Crack Detection in Highway Transportation Infrastructure. Adv Mater Sci Eng 2021;2021.

[27] Tang W, Zhao C, Lin J, Jiao C, Zheng G, Zhu J, et al. Improved Spectral Water Index Combined with Otsu Algorithm to Extract Muddy Coastline Data. Water 2022;14: 855.

[28] Zhao X, Yang M, Qu Q, Xu R, Li J. Exploring Privileged Features for Relation Extraction With Contrastive Student-Teacher Learning. IEEE Trans Knowl Data Eng 2023;35(8):7953–65.

[29] Haseena F, Clara R. Performance Analysis of Iterative Thinning Methods using Zhang Suen and Stentiford Algorithm. International Conference on Advancements in Computing Technologies. 2018.

[30] W. Chen and L. Sui, "Improved Zhang-Suen Thinning Algorithm in Binary Line Drawing Applications," in 2012 Int. Conf. Syst. Informatics (ICSAI 2012), 2012.

[31] M. M. Abu, Z. A. Alqadi and K. Aldebei, "Comparative Analysis of Fingerprint Features Extraction Methods 2. Features Extraction Methods," J Hunan Univ (Nat Sci), 48(12) (2021).

[32] Khalique A. Implementation of elliptic curve digital signature algorithm. Int J Comput Appl 2010;2(2):21–7.

[33] S. Kazmirchuk, A. Ilyenko, S. P. O. Ilyenko, Y. Mazur, The Improvement of Digital Signature Algorithm Based on Elliptic Curve Cryptography," Adv Comput Sci Eng Educ III, 2020;327–37.

[34] Li H, Huang Q, Huang J, Susilo W. Public-Key Authenticated Encryption With Keyword Search Supporting Constant Trapdoor Generation and Fast Search. IEEE Trans Inf Forensics Secur 2023;18:396–410.

[35] Ajagbe SA, Florez H, Awotunde JB. AESRSA: A New Cryptography Key for Electronic Health Record Security. Peru: Computer and Information Science; 2022.

[36] Li W, Bu J, Li X, Peng H, Niu Y, Zhang Y. A survey of DeFi security: Challenges and opportunities. Journal of King Saud University - Computer and Information Sciences 2022;34(10, Part B):10378–404.