International Journal of Scientific Research in Science, Engineering and Technology
Print ISSN: 2395-1990 | Online ISSN : 2394-4099 (www.ijsrset.com)
doi : https://doi.org/10.32628/IJSRSET

A Survey on Biometrics Based Secured E-Voting System

Tazaeen Ilyas Shaikh, Suyash Santosh Gugale, Hritika Kamalakar Ranadhir, Vrushali Prakash Patil, Omkaresh Kulkarni

School of Computer Science and Technology, MITWPU, Pune, Maharashtra, India

Article Info
Volume 9, Issue 3

Page Number : 63-72

Publication Issue :
May-June-2022

Article History
Accepted : 01 May 2022
Published: 07 May 2022

ABSTRACT

An election is a powerful tool of any democratic country, which allows every citizen to exercise their right to vote. Though in-person voting is the most widely used medium for a citizen to vote, circumstances like a pandemic, natural disasters, or other location-based issues could deter an individual from doing so. Electronic voting systems must be legitimate, accurate, safe, and convenient when used for elections. Nonetheless, adoption may be limited by potential problems associated with electronic voting systems. With the use of biometrics and encryption techniques the whole system can be made secured. The drive towards biometrics has been facilitated by its largely apolitical nature. The biometrics based secured e-voting system is a beautiful replacement for traditional electronic voting solutions with distributed, non-repudiation, and security protection characteristics. That's why in this paper we have performed a survey on e-voting system.

Keywords: e-voting system, fingerprint verification, face recognition, machine learning, deep learning.

I. INTRODUCTION

Electoral systems enable a country's inhabitants to elect parliament representatives of their choosing. A paper-based election system is a traditional way to fulfil the stated aim. This approach involves submitting printed ballots to numerous voting stations around the nation at least one day before the election. Following the election, sealed boxes holding votes are unsealed in front of all valid booth members and tallied. Along with bags of paper ballots, the information from counted votes is sent to a centralised station. The names of winners and losers are compiled and published by the central station through television and radio stations. This strategy is only beneficial if the whole procedure is done in a transparent manner. This approach, however, has several limitations. These include increased costs, a longer time to finish the voting process, fraudulent actions by election officials, and voter misconduct. As a consequence of these obstacles, election outcomes are influenced. Electronic voting systems offer an effective and dependable method for people of a nation or members of an organisation to choose a person of their choosing. These systems may be divided into three types: supervised, hybrid, and remote voting. Electoral organisations often offer supervised voting, also known as offline voting. Voting machines are positioned at polling places under this design. These devices, however, are not linked to a centralised system for cross-verification or any other reason.

Advertisements for electronic voting, particularly Internet voting, present a variety of reasons in support of its use. These are associated with technology, social issues, and election administration. For starters, electronic voting has the potential to make the voting process simpler and more accessible to voters. This is particularly true for unlikely Internet voting and telephone voting, since votes may be cast from any computer with an Internet connection or any functional telephone. These new technologies significantly reduce the cost of voting for many voters by increasing the number of entry points from which they may vote. There is the possibility of removing lengthy lines at voting places and better addressing accessibility issues for those with disabilities, those suffering from sickness, those serving in the military or living abroad, and those on personal trip. Single parents who may find it difficult to get to a typical voting place.

1. Eligibility: Only qualified citizens are eligible to vote.
2. Anonymity: Voters' votes cannot be traced to them.
3. Voter mobility: Voters may vote from any location.
4. Verifiability: Voters may check to see whether their votes were tallied or rejected in the final election results.
5. Fairness: The amount of votes cast for each candidate should not be known before the election.
6. Distinctiveness: Each voter may only vote once in each election session.

A. *Problems and Solutions of Developing Online Voting Systems*

Whether we are talking about classic paper-based voting, digital voting machines, or an internet voting system, many requirements must be met:

- Eligibility: Only genuine voters should be allowed to vote.
- Unreusability: Each voter can only vote once.
- Privacy: No one can acquire information about the voter's decision except the voter; • Fairness: No one can access intermediate voting results;
- Soundness: Invalid votes should be recognised and not counted during tallying; • Completeness: All legitimate ballots should be appropriately tallied.

A quick review of the methods for achieving these requirements in online voting systems is provided below.

B. *Strengths associated with e-voting*

- Better vote tally and tabulation
- Less human error means better outcomes.
- Handling complex election systems requiring tedious counting techniques.
- Better display of complex ballots.
- Convenience for voters
- Increased engagement and turnout, especially with online voting.
- More responsive to a mobile society's requirements.
- Lessening human interference at polling stations and during transmission and tabulation of results.
- Improved accessibility, such as audio ballots for blind voters, Internet voting for housebound people, and overseas voters.
- Multilingual user interfaces may be better than paper ballots for multilingual voters.
- Voting systems may alert voters to invalid votes, reducing spoilt ballots (although consideration should be given to ensuring that voters are able to cast a blank vote should they so choose).
- Potential long-term cost reductions through decreased poll worker time and ballot paper manufacture and delivery.
- Why Internet voting saves money by allowing global access with little overhead. No shipping expenses, no delays in returning stuff.
- Compared to postal voting, Internet voting reduces e-selling and family voting by permitting repeated

voting where only the latest vote counts and controlling voting timeframes.

Researchers work incorporated artificial intelligence (AI) pattern recognition, Machine Learning, Deep Learning, as well as cyber security techniques for data encryption and decryption, as well as fingering, facial biometrics.

II. LITERATURE SURVEY

A. Use of Encryption Techniques for Secure E-voting

Prof. S.M. Jambhulkar et al. developed a web-based internet voting system [2], in which the author defends the right to vote. The majority of the time, security is essential while transferring votes from a casting ballot client to a casting ballot server. Solid apparatuses are the concept of a number of encryption and decryption. Patil et al [6] proposed system based on smartphone availability, a smart voting application offers voters with several kinds of verification. If the user has a smartphone and may vote from anywhere, an OTP is issued. The cast vote is encrypted using cryptography. It uses the Mix net technique to permute inputs and creates an encrypted message. Only those who have been granted access to the decryption key may decode it and count the casting vote. Dyta et al [12] proposed new EVS, it employs the RSA-based Paillier cryptosystem and blind signature. It is made up of CTF, which connects with several servers of the local committee located among polling stations. RFID is employed to maintain voter individuality. Hussien at el in [18] creates a new voting mechanism based on the Pallier cryptosystem and a blind signature technique based on RSA. Their module includes a central tabulating facility for collecting and distributing all secret votes from local servers that connect between polling stations. Each server at the local polling station is linked to a number of embedded devices known as voting terminals or machines, which are used to construct the voter's ballot. They also used RFID approach which fulfils eligibility and uniqueness of system.

Pomares et al in [14] examines Salta's experience as the first Argentine district to implement e-voting for all voters in 2013. Based on a survey of 1,000 voters in the 2013 provincial election, it assesses voters' knowledge and experience with the electoral process. He discovered that an elector's ability to operate the voting machine without assistance has a considerable effect on overall support for e-voting and positive views of integrity in the election process.

Agarwal at el [17] suggests an online voting system for India, allowing citizens to vote for any candidate and from any location. The Adhaar card is used for unique voter identification in order to prevent repeated votes and to offer high-security measures throughout the election process. The usage of the central database built by the Indian electoral commission helped the counting of votes and the calculation of results.

B. Use of ML/ DL Algorithms in the field of biometrics identification

The Komatineni at el. [3] has introduced a new voting system that focuses on potential face detection and identification as well as biometric authentication features such as biometric scanning, as well as an execution plan that improves protection and prevents duplicate and voting fraud to make the system more efficient and cost effective. Face identification using Eigen's face-based recognition algorithm and Minutiae-based algorithm strengthens and secures the traditional voting system by using a two-factor bio-metric authentication technique with a full-fledged database as input. Bindia at el [9] also uses face recognition, one-time password approaches, and fingerprint recognition techniques are being investigated for use in implementing the new e-voting system. In Voting, this enables authentication, secrecy, and data integrity by using the required electronic signature, encryption algorithms, and hash functions. Gentles et al [20] also uses fingerprint to register vote from anywhere via mobile internet, and they can vote for any candidate from anywhere. Even if the procedure of authenticating and registering fingerprints requires a visit to the election office.

The biometric voting system (BVS) was proposed by Chakraborty et al [10]. It uses information recorded in the Aadhaar Card database for Indian citizens. Iris and fingerprint pictures are saved in order to identify unique individuals based on Aadhaar card data. This BVS is coupled to a biometric fingerprint system that recognises verified voters based on data stored in a database. To avoid discrepancies in elections, the Madan Mohan at el in [11] presented a way for a safe and trustworthy biometric voting system based on Aadhaar. When an alcoholic approaches a voting station, a buzzer alerts authorised persons or constables on duty. It also sounds a buzzer when an un-authorised user enters to participate or when the same individual enters with valid RFID many times, allowing the officer at the booth to take necessary action.

Three various sizes of 3-D facial recognition technology modules are utilised for voting by Ujir et al [16]. The design included at least six basic face expressions as well as 3D landmarks from the Bosphorus database. To calculate the recognition rate for 3D face recognition, the concept of face decomposition is applied. The modular testing was carried out using two kinds of voting schemes: Majority Voting System (MVS) and Weighted Voting Scheme (WVS) (WVS). Furthermore, regardless of the recognition rate, the MVS algorithm calculates the greatest number of subjects voted.

Sudhakar at el in [13] proposed the new technology employs fingerprint-based identification to boost security by prohibiting tampering with voting machines and voting multiple times. As an added security step, picture and voter information are presented from a distant server on the ARM9 LCD, and results are seen on the central server by an authorised individual. In the WINCE6 development environment, software code is written to interface the ARM processor with the fingerprint module. The technology offers the greatest answer for reducing the amount of time required for voter identification.

Shahram Najam Syed at el [21] propose, and assess a new hybrid electronic voting system. Compared to single identification methods, their suggested approach employs two voter verification mechanisms. They used fingerprint and face recognition to identify voters. Their face recognition system employs the Viola-Jones algorithm and rectangular Haar feature selection technique to identify and extract characteristics for a biometric template and voting. GPCA (Generalized Principle Component Analysis) and K-NN (K-Nearest Neighbor) are used to compare characteristics for identity verification.

Cheema at el in [22] propose a blockchain based and machine learning-based e-voting system. They employ blockchain to secure votes and machine learning to identify hacking in voting data centres and e-voting booths. The suggested paradigm combines personal and public blockchain. They used personal blockchain is to register and vote. As the public blockchain protects the privacy of voters by recording the root hash of the Merkle hash tree and publishing the results of the polling stations after the voting process. The suggested blockchain-based e-voting system delivers openness, security, and trust while preventing network interference.

Electoral fraud is an unlawful involvement in the election process when people vote repeatedly for a preferred party to increase vote share. This electoral fraud should be abolished to conduct elections legitimately. So, Convolutional Neural Network (CNN) automated voting mechanism was suggested. Using a convolutional neural network, all label pictures are trained to predict the output [23]. Salama AbdELminaam D at el in [24] develop a complete Face recognition system using transfer learning in fog computing and cloud computing. Their developed system uses deep convolutional neural networks (DCNN) because of the dominant representation; there are some conditions including occlusions, expressions, illuminations, and pose, which can affect the deep FR performance. DCNN is used to extract relevant facial features. These features allow us to compare faces between them in an efficient way. The system can be trained to recognize a set of people and to learn via an online method, by integrating the new people it processes and improving its predictions on the ones it already has. For result comparison they used different ML and DL algorithms. They achieved 99.0 % accuracy for face recognition using DCNN algorithm.

III. E-voting System

This section introduces system architecture of electronic voting system. Electronic voting is a voting method that uses electronic technology to record or count votes. Electronic voting is backed by electronic hardware and software. E-voting system is capable of supporting/implementing functions from election preparation to vote storage. System include election kiosks, PCs, mobile devices, fingerprint devices and camera. Electronic voting systems must include voter registration, authentication, voting, and tallying. Secure voting, on the other hand, will be an encrypted piece of data saved on a dispersed network rather than a single server. Each encrypted vote is validated by consensus, and the public records of each vote is stored on a distributed system. The e-voting method is decentralised and open, yet also protects voters and votes. With the use of double biometric verification (fingerprint and face) in voting system improves the number of voters as voter can vote from anywhere and with encrypted electronic voting, everyone can count the votes, but no one knows who voted for whom. Following figure 1 shows the overall system architecture of secure e-voting system.

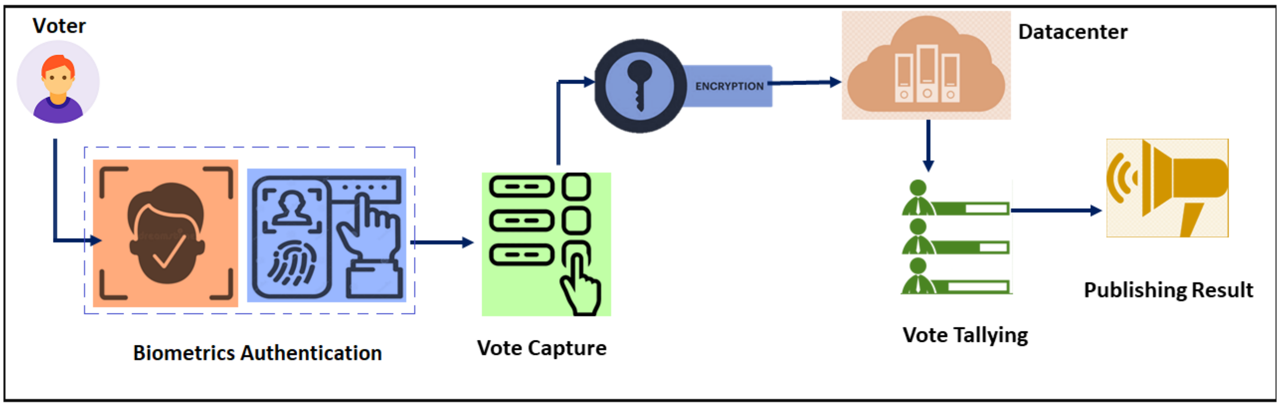

Fig .1 Secure e-voting system architecture.

IV. Result and Discussion

A. Comparative Results (Existing System)

Table 1 shows the existing researchers comparison based on techniques, methodology and tools that they have used for secure e-voting system.

Table 1: List of contributions of researchers on Voting systems.

Authors [ref]	Year	Tools / Techniques	Methodology
Komatineni, & Lingala [3]	2020	Face recognition with Eigen face based recognition algorithm and Minutiae based algorithm	The two-factor Bio-metric authentication process with a full-pledged database as an input turns the regular voting system hooked on a robust and safer one.
Mohan, et al [4]	2020	Arduino Uno	Improve protection by resolving bogus voting and fingerprint-based authentication.
Jamkar, et al. [5]	2019	Arduino and Fingerprint module	An advanced framework, using the Arduino and Fingerprint module to eliminate abuse and defraud voting methods
Patil, et al. [6]	2018	Smartphone with cryptography	Next-generation online highly secure voting system.
Kavitha, et al [7]	2018	Fingerprint, face and iris recognition	the voting system based on the Fingerprints and Iris verification is used
Rezwan, et al. [8]	2017	Arduino and Finger Print Scanner	Arduino and Finger Print Scanner, capable of identifying every voter, counting votes, and preventing fake votes in Bangladesh
Bindia, & Aggarwal [9]	2016	An electronic signature, encryption	E-voting techniques like one-time password techniques, face recognition, and fingerprint recognition techniques.
Chakraborty, et al. [10]	2016	Fingerprint and Iris recognition	BVS is linked to a biometric fingerprint system that uses data stored in the database to recognize authenticated voters
Madan Mohan & Srihari [11]	2015	RFID	A biometric voting method based on Aadhar card to prevent misconceptions.
Data, et al. [12]	2015	Paillier cryptosystem and blind signature method	RSA-based Pailier cryptosystem and blind signature scheme for EVS is designed
Sudhakar & Sai [13]	2015	Fingerprint-based electronic voting machine using ARM9 microcontroller	Fingerprint-based authentication to improve security by preventing fake voting and voting repetition
Pomares, et al. [14]	2014	Online voting	A voting machine without the assistance of the user in the election process
Mythili, et al. [15]	2014	Biometric devices	Voting is conducted using the SMS voting method
Djir, et al. [16]	2014	3-D face recognition technology	For voting, modular approach human 3D faces recognition through neutral and 6 simple facial image expressions tests were conducted
Agarwal, & Pandey [17]	2013	Web-based and Fingerprint recognizer software	A person can vote from anywhere from their allotted constituency or their preferred location
Hussien, & Aboelnaga [18]	2013	Homomorphic System and Blind signature scheme with RFID	For security tools, a new voting system is implemented with Pallier cryptosystem and a blind signature scheme created on RSA
Kumar et al [19]	2012	Biometric devices	Various types of EVM, issues, biometric used are studied.

Gentles, et al. [20]	2011	Android 3.0 (Honeycomb)	Biometric secured voting using mobile is developed

Figure 3 shows the researches accuracy comparison graph, from graph we can clearly say that deep learning algorithms outperforms the other traditional machine learning algorithms.

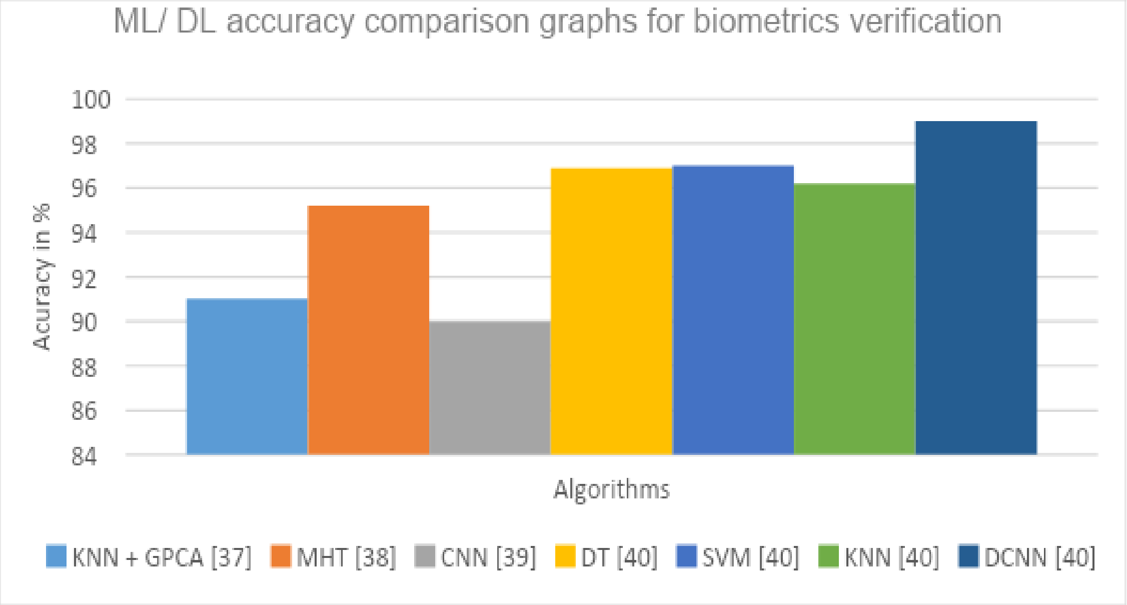

Fig. 3 Accuracy comparison graph.

V. CONCLUSION

The purpose of this work is to examine and assess existing research on biometrics-based electronic voting systems. The work addresses contemporary electronic voting research that makes use of ML / DL technologies. As we see that existing voting system has many defects such as lengthy process, time taking, not secure, bogus voting, no security level but now we can say that there is need to developed system which is more useful and secure from the existing system. The facial authentication technique is very much useful in identifying the fraud voters, so we can avoid the bogus votes during election commission. The voters can cast their voting from anywhere by login to our proposed smart voting system through internet. As data is stored in centralized repository so, data is accessible at any time as well as backup of the data is possible. Smart voting system provides updated result at each and every minute. Also requires less man power and resources. With use of fingerprint device, face recognition and encryption technique the proposed system becomes very robust and secure which can be used for e-voting. We highlighted the details of word done by researchers in table 1 and in figure 3; rom that we can say that the deep learning algorithm performs better in terms of accuracy.

VI. REFERENCES

[1]. X. Yang, X. Yi, S. Nepal, A. Kelarev and F. Han, "A Secure Verifiable Ranked Choice Online Voting System Based on Homomorphic Encryption," in IEEE Access, vol. 6, pp. 20506-20519, 2018. doi: 10.1109/ACCESS.2018.2817518

[2]. Prof. S.M. Jambhulkar, Prof. Jagdish B. Chakole, Prof. Praful. R. Pardhi," A Secure Approach for Web Based Internet Voting System using Multiple Encryption", 2014 International

Conference on Electronic Systems, Signal Processing and Computing Technologies.

[3]. Komatineni, S., & Lingala, G. (2020). Secured E-voting System Using Two-factor Biometric Authentication. In 2020 Fourth International Conference on Computing Methodologies and Communication (ICCMC) (pp. 245-248). IEEE. ISBN: 978-1-7281-4889-2.

[4]. Mohan, M. Madhu, M. Prakash, M. Madhuseelan, and A. Kishore Kumar (2020). Design of Secured Biometric Voting Machine. International Journal of Research in Engineering, Science and Management, 3(3),199-201.

[5]. Jamkar, A., Kulkarni, O., Salunke, A., & Pljonkin, A. (2019). Biometric Voting Machine Based on Fingerprint Scanner and Arduino. In 2019 2nd International Conference on Intelligent Communication and Computational Techniques (ICCT), 322-326. IEEE. ISBN: 978-1- 7281-1711-9.

[6]. Patil, S., Bansal, A., Raina, U., Pujari, V., & Kumar, R. (2018). E-Smart Voting System with Secure Data Identification Using Cryptography.In 2018 3rd International Conference for Convergence in Technology (I2CT).

[7]. Kavitha, S. N., Shahila, K., & Kumar, S. P. (2018). Biometrics Secured Voting System with Finger Print, Face and Iris Verification. In 2018 Second International Conference on Computing Methodologies and Communication (ICCMC) (pp. 743-746). IEEE. ISBN: 978-1-5386-3452-3.

[8]. Rezwan, R., Ahmed, H., Biplob, M. R. N., Shuvo, S. M., & Rahman, M. A. (2017). Biometrically secured electronic voting machine. In 2017 IEEE Region 10 Humanitarian Technology Conference (R10-HTC) (pp. 510- 512). IEEE.

[9]. Bindia, & Aggarwal, N. (2016). NEXT GENERATION HI-TECH E-VOTING TECHNIQUES IN INDIA. International Journal of Science, Engineering and Technology Research (IJSETR), 5(1), 228–233.

[10]. Chakraborty, S., Mukherjee, S., Sadhukhan, B., & Yasmin, K. T. (2016). Biometric voting system using Aadhaar card in India. International journal of Innovative research in Computer and Communication Engineering, 4(4). 5284- 5291.

[11]. Madan Mohan Reddy, B., & Srihari, D. (2015). RFID Based Biometric Voting Machine Linked to Aadhaar For Safe and Secure Voting. International Journal of Science, Engineering and Technology Research (IJSETR), 4(4), 995–1001.

[12]. Dyta, P., Junjare, S., Pandita, A., & Ingle, D. R. (2015). E-Voting – Secured NFC Voting. IJSRD - International Journal for Scientific Research & Development, 3(1), 1032–1036.

[13]. Sudhakar, M., & Sai, B. D. S. (2015). Biometric system based electronic voting machine using arm9 microcontroller. IOSR Journal of Electronics and Communication Engineering (IOSR-JECE), 10(1), 57-65.

[14]. Pomares, J., Levin, I., Alvarez, R. M., Mirau, G. L., & Ovejero, T. (2014). From piloting to roll-out: voting experience and trust in the first full e-election in argentina. In 2014 6th International Conference on Electronic Voting: Verifying the Vote (EVOTE). 1-10. IEEE.

[15]. Mythili, K., Kanagavalli, K., & Shibi, B. (2014). An efficient method to avoid false voting using sms voting approach. International Journal of Computer Science and Mobile Computing, 3(2), 804-810.

[16]. Ujir, H., Sing, L. C., & Hipiny, I. (2014). A modular approach and voting scheme on 3D face recognition. In 2014 International Symposium on Intelligent Signal Processing and Communication Systems (ISPACS). 196-199. IEEE.

[17]. Agarwal, H., & Pandey, G. N. (2013). Online voting system for India based on AADHAAR ID. In 2013 Eleventh International Conference on ICT and Knowledge Engineering.1- 4. IEEE.

[18]. Hussien, H., & Aboelnaga, H. (2013). Design of a secured e-voting system. In 2013 International

Conference on Computer Applications Technology (ICCAT). 1-5. IEEE.

[19]. Kumar, D. A., & Begum, T. U. S. (2012). Electronic voting machine—A review. In International Conference on Pattern Recognition, Informatics and Medical Engineering (PRIME-2012) (pp. 41-48). IEEE. DOI:

[20]. Gentles, D., & Sankaranarayanan, S. (2011). Biometric secured mobile voting. In 2011 Second Asian Himalayas International Conference on Internet (AH-ICI) (pp. 1-6). IEEE.

[21]. Shahram Najam Syed and Aamir Zeb Shaikh and Shabbar Naqvi, A Novel Hybrid Biometric Electronic Voting System: Integrating Finger Print and Face Recognition, Mehran University Research Journal of Engineering and Technology, 2018, 37 (1), pp.59-68

[22]. Cheema, Muhammad & Ashraf, Nouman & Aftab, Asad & Qureshi, Hassaan & Kazim, Muhammad & Azar, Ahmad. (2020). Machine Learning with Blockchain for Secure E-voting System. 177-182. 10.1109/SMART-TECH49988.2020.00050.

[23]. Sruthi, M. and K Shanjai. "Automatic Voting System Using Convolutional Neural Network." Journal of Physics: Conference Series 1916 (2021)

[24]. Salama AbdELminaam D, Almansori AM, Taha M, Badr E (2020) A deep facial recognition system using computational intelligent algorithms. PLOS ONE 15(12): e0242269.

Cite this article as :

Khantharaju. V, Dhanalakshmi M. V, Nidhi, Deepa B, Almas A, "Secure Digital Voting System Based on Blockchain Technology - A Survey", International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Online ISSN : 2394-4099, Print ISSN : 2395-1990, Volume 9 Issue 3, pp. 58-62, May-June 2022. Available at doi : https://doi.org/10.32628/IJSRSET22938
Journal URL : https://ijsrset.com/IJSRSET22938