ISSN: 2454-9940

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

E-Mail :
editor.ijasem@gmail.com
editor@ijasem.org

www.ijasem.org

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

ISSN 2454-9940

www.ijasem.org

Vol 16, Issue 3, 2025

Secured Digital Voting System using Web + Blockchain

[1]SHAIK MUSTAFA HUSSAIN, [2]J A PAULSON

[1]Student, Department of CSE, Varaprasad Reddy Institute of Technology, Sattenapalli, Kantepudi (Village), India

2Associate Professor, Department of CSE, Varaprasad Reddy Institute of Technology, Sattenapalli, Kantepudi (Village), India

Abstract

We look forward to the day when our safe online voting technology may replace India's costly and dated paper ballots. The system need to avoid delaying results and be easy to use for both tech-savvy users and Non-Resident Indians (NRIs). As part of the secure digital voting system's Authentication Phase, individuals may be verified using face recognition and one-time password verification. To ensure integrity, the system moves on to Live Real-time Monitoring and Session Monitoring. Upon discovery of any negative behavior, the vote is rescinded. The current voting system in India relies on expensive and labor-intensive electronic voting machines (EVMs) and conventional ballot papers, which causes problems for all Indian voters, including those outside of the nation. We provide a simple and secure method to cast an online vote in the proposed method. Various safeguards are used, such as end-to-end encryption, blockchain-based smart contracts for authentication, MTCNN for facial recognition, and MobileNetV2 for continuous feature tracking. Voting by non-resident Indians in conventional elections has been low owing to practical constraints. Because online voting is easy and convenient, participation rates are expected to reach 72% in 2024, a 5% increase over 2023. There is greater involvement and a more inclusive voting process as a result of this digital transition that removes geographical boundaries (p = 0.049). Developed using state-of-the-art technology like TensorFlow and MobileNetV2, the system successfully gets around the problems with regular offline voting. All voters will have their questions answered, and the framework for a digitized, safe, and efficient democratic voting process will be laid. It also takes into account the changing demands of future generations.

Keywords:

Some of the subjects covered are Aadhaar numbers, blockchain technology, mobile netv2, online voting, security, face recognition, non-resident Indians, and real-time monitoring.

INTRODUCTION

By using cutting-edge technology, increasing accessibility for non-resident Indians, and improving operational efficiency, an electronic voting system has the ability to drastically change the traditional voting process [1]. Furthermore, this approach guarantees the confidentiality, integrity, and accessibility of all collected data. Voting in India has traditionally been done using paper ballots and electronic voting machines (EVMs), however this process is notoriously time-consuming, expensive, and prone to confusing processes [2]. Research has shown that online systems are more accessible and cost-effective, thus there has to be a better strategy to accommodate this trend [3]. The suggested online voting method is based on blockchain and deep learning and has the dual goals of reducing the likelihood of fraud and increasing the speed of the results [4]. Users with a good understanding of technology will find this approach especially useful since it streamlines the voting process and makes it easier to participate in digital elections [5]. affirm that transparent and thorough oversight of the elections is being maintained, avoiding.

RELATED WORK

There have been forty articles written on this subject in the previous five years in publications such as Applied Science, Sensors Journal, and IEEE Xplore, among others. Hospitals, crime scenes, and pandemic warning systems are just a few of the real-world settings where accurate face mask identification and recognition systems are in great demand. Feature extraction and masked image classification using pre-trained deep learning models such as MobileNetV2 are typical methods used by researchers in this area. In particular, by augmenting MobileNetV2 with additional layers, the accuracy of mask recognition may be increased to 99.64% in [6]. Facial recognition in complex scenarios, which may be impacted by mask wearing, is also emphasized in notable

publications such as [7]. It was in 2002 when the Faux Recognition Vendor Test (FRVT) revealed the pros and cons of face recognition algorithms.
Security measures, such as one-time password (OTP) systems, have been strengthened in response to the meteoric rise of mobile banking. Graphical one-time passwords and other mobile security measures make smartphones harder to exploit [8].Machine learning and computer vision specialists compare MobileNetV2 against its predecessors, including MobileNetV1, to see how well it performs on image classification tasks. There has been prior research on the topic of how activation functions, such as ReLU, improve classification outcomes [9]. Several methods, including deep learning, have been investigated for application in face recognition and authentication systems.Our tools include CNN and MobileNetV2. When it comes to producing very precise outcomes, this device has really proved its mettle, especiallyrisky situations without the necessary safety gear, including a face mask.Recent attempts to enhance these models and their classification accuracy have focused on adding layers to pre-existing architectures. For instance, [10] added five more layers to the MobileNetV2 model to greatly improve its ability to detect face masks. Machine learning techniques, such as TensorFlow, and activation functions, such as ReLU, have improved object identification and facial recognition accuracy [11].Researchers have been investigating the potential of blockchain technology for use in voting systems, especially in relation to elections, for a while now. Blockchain technology ensures data integrity and immutable records, which boosts security and transparency. Although blockchain data security can be difficult, especially in edge computing environments, the technology shows promise in general (as stated in [13]). A comprehensive and user-friendly voting system for NRIs (Non-Resident Indians) is still required, even if previous studies have enhanced face recognition technology and incorporated blockchain into safe systems. Strong and private voting procedures must be provided using Aadhaar-based identification [14], real-time facial recognition, and blockchain technology. To meet all of these demands simultaneously, the existing literature does not provide sufficient solutions.

To provide a secure online voting platform for citizens and NRIs (Non-Resident Indians), the proposed technique makes use of many technologies, such as blockchain, Aadhaar-based authentication, and facial recognition. This method is designed to increase election security and transparency by using validation processes and real-time monitoring to ensure that every vote is legitimate. Importantly, the system uses the MobileNetV2 model for face detection throughout the session. Results show that the proposed technique achieves higher accuracy for real-time face mask detection than prior methods. The reason for this is its comprehensive approach to ensuring the security of online voting. With this system's flawless integration of blockchain security, facial recognition, and OTP-based Aadhaar identification, voters may feel more at ease about the accessibility and integrity of the election. Compared to other facial recognition systems, MobileNetV2's accuracy is much higher when combined with continuous session monitoring.
It takes a lot of time and money to print ballots and program voting equipment. Traditional ballots are expensive, despite their cheap cost, because to the large logistical cost of tallying votes, in contrast to EVMs' relatively modest computational cost. Complex features, like blockchain or authentication based on artificial intelligence, raise processing costs. No amount of inefficiency will allow non-resident Indians to use it. The operational and logistical complexity of vote counting is low, and it is an O(n) procedure.

MATERIALS AND METHODS

Using state-of-the-art computational methods and blockchain technology, this project aims to provide a safe and efficient platform for online voting. Improved voter verification and fraud prevention were outcomes of integrating Aadhaar with MobileNetV2-based face recognition. To ensure the system's reliability and security, real-time session monitoring was included. The site's target audience consisted of technically savvy individuals and Non-Resident Indians (NRIs). Vote security based on blockchain technology, real-time voter analytics, and session tracking all contributed to a more trustworthy democratic voting process, more participation, and easier access [15].

Group 1 in India's voting system still uses both paper ballots and computerized voting machines. Quite a few people and a lot of money are required for these methods to be implemented [16]. These processes are unavailable to non-resident Indians (NRIs), who encounter many obstacles while trying to participate in elections.Group 2 encompasses our method, which makes use of Aadhaar-based OTPs, MTCNN for face recognition, and blockchain-based smart contracts for secure verification. An online voting system that is both safe and easy to use is within reach with these settings. Blockchain technology, which incorporates

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

ISSN 2454-9940

www.ijasem.org

Vol 16, Issue 3, 2025

features like smart contracts and end-to-end encryption, together with MobileNetV2, has made the possibility of secure, real-time vote submissions a reality.

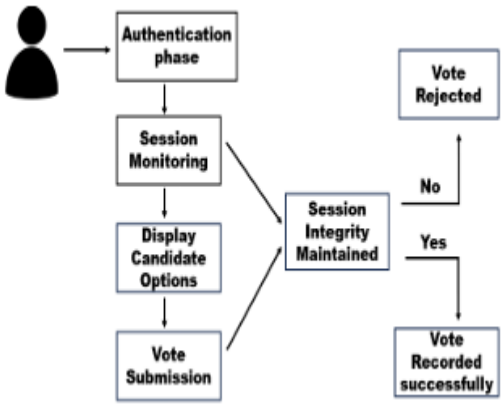


Figure 1 shows the block diagram of the proposed system.

The process flow of an online voting system starts with authenticating users, then moves on to monitoring their sessions, and finally finishes with the submission of votes. There is a 98.5% success rate and a 1.5% false positive rate; if it determines that the integrity of the session has been compromised, it rejects the vote.

The steps of a safe online voting system are shown in Figure 1.

Using Face Recognition and One-Time Password Verification, the user's identity is authenticated during the Authentication Phase, the first step. A successful match was made between the individual's name, Aadhaar number, and facial traits, validating their identify. To guarantee the accuracy of the person's identity, this multi-step authentication procedure is used. In order to guarantee the security of the session, the system will record the user's screen, watch their session, and monitor real-time data, supposing they have been authenticated. Votes are discarded in the event that Unwanted Activity is identified. On the other hand, they may go to the Candidate Options page, choose a candidate, and then confirm their selection.

Prior to the vote being recorded, the system verifies the Session Integrity. After their vote has been correctly recorded, the user has the option to log out. In such case, the vote has no validity. We verify that only qualified voters are able to cast ballots by submitting and authenticating their votes. Face recognition and ID authentication are two ways that voters' identities may be confirmed. By secretly recording and transmitting their vote only after verification, we guarantee its confidentiality and correctness.

STATISTICAL ANALYSIS

A statistical analysis was performed on the data using SPSS version 26. Using group statistics and an independent samples t-test, the Blockchain and MobileNetV2 models were evaluated for recall, accuracy, F1 score, and detection time [17]. One of the independent factors was the kind of model (NetV2 or Blochian), while the dependent variables were accuracy, recall, F1-score, and detection time. According to Levene's test, the variances are not equal if the p-values are less than 0.05. For detection time, it was assumed that the variances of F1-score, accuracy, and recall were uneven; however, the converse was also true. All parameters showed statistically significant changes, according to the t-test results (Sig. 2-tailed < 0.05). Accuracy(-1.39200), recall(5.40600), and F1-score (-3.35900) were all better obtained by Blockchain, even though MobileNetV2 had a longer detection time (0.45100). These findings were much more clear with 95% confidence intervals, proving that Blokhin was efficient and successful, particularly with regard to the shorter detection times.

RESULTS

Using face recognition technology and a one-time password confirmation, voters must first verify themselves before they can begin operating the secure digital voting system. Session monitoring, screen recording of transaction flows to prevent violence, and real-time monitoring to assure integrity are capabilities that follow closely after this.

Table 1 shows that between 2014 and 2024, there was a 26% rise in the number of votes cast by non-resident Indians. With an anticipated increase in votes from 60 to about 30,680, the number of registered voters increased from 12,000 in 2014 to 118,000 in 2024.

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

ISSN 2454-9940

www.ijasem.org

Vol 16, Issue 3, 2025

Year	Total Register NRI Voters	NRI Voter Turnout (%)	Total NRI Voter Cast	Overall Turnout (%)	NRI Contribution to Overall Turnout (%)
2014	12,000	<1% (~0.5%)	60	66.44%	~0.00001%
2019	71,735	26%	18,651	67.40%	~0.003%
2024	118,000	Not Yet Released (~26% estimated)	~30,680	66.33%	~0.005% (tentative)

To see how many registered non-resident Indian voters there were in 2014, 2019, and 2024, look at Table I. In 2014, 12,000 non-resident Indians cast 60 ballots, which is 0.5 percent of the total electorate. There was a 26% rise to 18,651 voters out of 71,735 registered voters in 2019. Compared to previous years, the turnout was 26%, with 11,8,000 registered voters casting 30,680 ballots.

The second table is here. In order to determine the best course of action amid emerging schemes and challenges, a performance study was conducted using mobilenetv2 and blockchain.

S.NO	Image IDs	Precision		Recall (%)		F1-Scores (%)		Detection Time	
		MobileNet V2	*Blockchain*	*MobileNet V2*	*Blockchain*	*MobileNet V2*	*Blockchain*	*MobileNet V2*	*Blockchain*
1	user001	96	97.44	90.57	96.94	93.2	97.19	1.2	0.8
2	User002	96..84	97.87	92	96.34	94.36	97.1	1	0.75
3	user003	95.5	96.9	89	95.85	92.15	96.37	1.1	0.85
4	user004	97.2	98.2	91.5	97.1	94.28	96.65	1.3	0.7
5	user005	96.75	97.3	93	96.5	94.83	96.9	1	0.78
6	user006	95	96.75	91	95.9	92.97	96.32	1.2	0.8
7	user007	94.5	97.5	90	96.75	92.2	97.12	1.4	0.72
8	Uer008	97	98	92.5	97.3	94.69	97.65	1.1	0.68
9	user009	96.4	97.1	91.75	96.4	94.02	96.75	1.3	0.76
10	user100	95.8	97.85	90.5	96.8	93.08	97.32	1.5	0.75

Double-Tabbed Desk We evaluated and tested the frameworks in response to ever-changing schemes and problems in an effort to identify the best performance option. We thoroughly compared MobileNetV2 and Blockchain to find out which one was better.

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

ISSN 2454-9940

www.ijasem.org

Vol 16, Issue 3, 2025

Table III shows that blockchain outperformed MobileNetV2 in terms of detection time (0.76 s) and accuracy rate (97.49 vs. 96.1%).

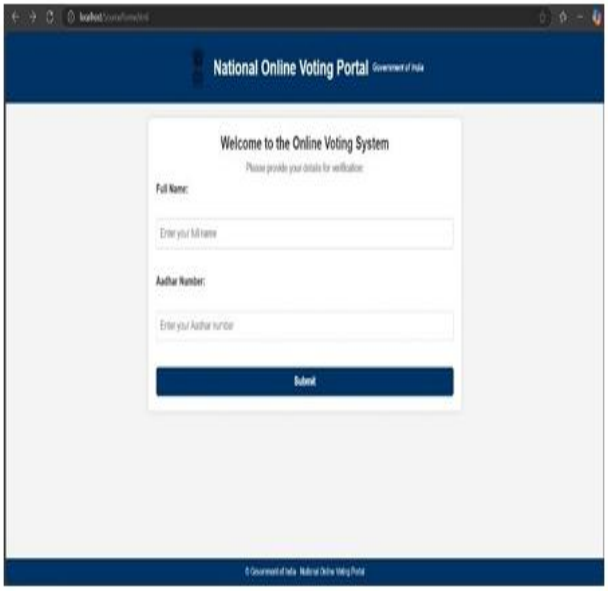
	Model	N	Mean	std.Deviation	std.Error Mean
Precision	MobileNetV2	10	96.0990	0.90124	0.28500
	Blockchain	10	97.4910	0.48588	0.15365

Accuracy, recall, F1-score, and detection time are shown in Table III. Blochian outperformed MobileNetV2 in every single category. In comparison, its processing time was 0.76 s and its accuracy was 97.49%, whereas the latter required 1.21 s.

Table IV shows that there are notable differences between the two networks. While MobileNetV2 has a longer detection time, Blockchain offers greater accuracy (P = 0.049).

		Levene's Test for Equality of Variances		T-test for Equality of Means				95% confidence Interval of the Difference	
		F	*sig*	*t*	*df*	*Sig. (2-tailed)*	*Mean Difference*	*std..Error Difference*	*Lower*	*Upper*
Precision	Equal variances assumed	4.436	0.049	-4.299	18	0.000	-1.39200	0.32378	-2.07223	-0.711 77
	Equal variances not assumed			-4.299	13.824	0.001	-1.39200	0.32378	-2.08726	-0.696 74

Part Four Despite MobileNetV2's longer detection time, Blockchain outperforms it in terms of accuracy, according to the findings of an independent samples t-test. The confidence intervals corroborated the findings, and there were statistically significant differences everywhere (p = 0.049).



According to Figure 2, users must verify their identity by entering their complete name and Aadhaar number on the National Online Voting Portal login screen.

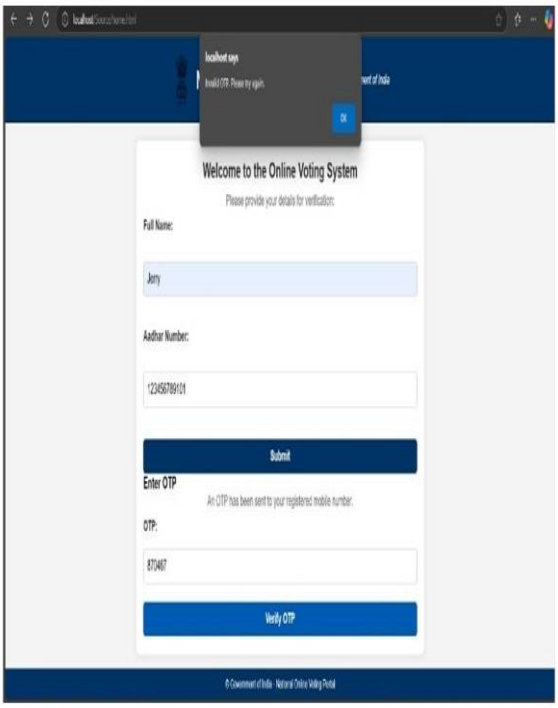
Figure 2 shows the confirmation. For the purpose of conducting elections online, the government of India has created the National Online Voting Portal. For security reasons, it includes a user-friendly form that asks for users' full names and Aadhaar numbers.

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

ISSN 2454-9940

www.ijasem.org

Vol 16, Issue 3, 2025



At the end of the Aadhaar verification process, the National Online Voting Portal verifies the OTP (as shown in Figure 3).

Figure 3 shows the user interface of the online voting system. A user identifying as "Jerry" confirms their identification by entering their Aadhaar number and an OTP. An notice stating "Invalid OTP" appears. Due to an unsuccessful OTP validation, a "Please try again" message is shown in the popup. There are input fields all throughout the design with obvious submit and verify buttons.

As seen in Figure 4, the camera capturing a selfie for Aadhaar-based face recognition enables secure authentication and continuous surveillance to identify breaches.

As shown in Figure 4, the only method to access the camera is via shooting a selfie. In order to validate identities securely, this selfie will be used for face recognition, more especially Aadhaar-based verification. Regular ID checks and the detection of unwanted access are two ways in which real-time monitoring further improves security.

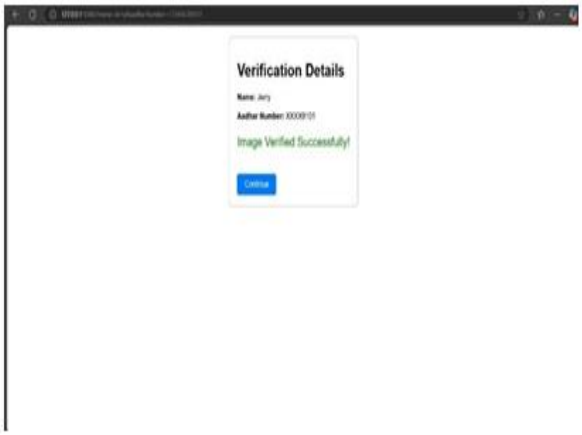


Figure 5 shows the confirmation screen that occurs after verification,

which displays the Aadhaar data. Your name, Aadhaar number, and facial characteristics were a perfect match, allowing us to successfully validate your Aadhaar information (Figure 5). The goal of this multi-stage authentication process is to guarantee that the person's identity is accurate.

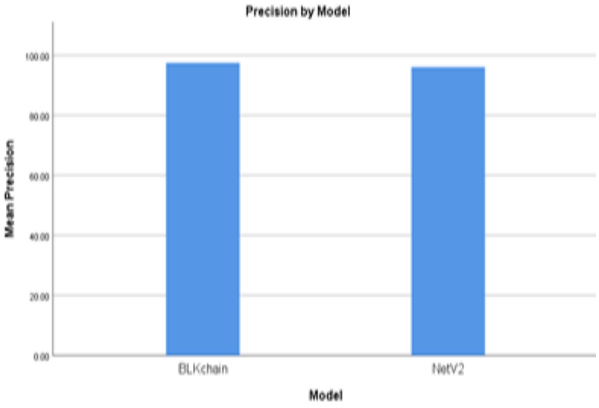
Ensuring that only qualified voters are able to cast their votes safely is the job of vote validation and submission. Voter ID authentication and face recognition are two examples of the technologies used to verify voter identification. By secretly recording and transmitting their vote only after verification, we guarantee its confidentiality and correctness.

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

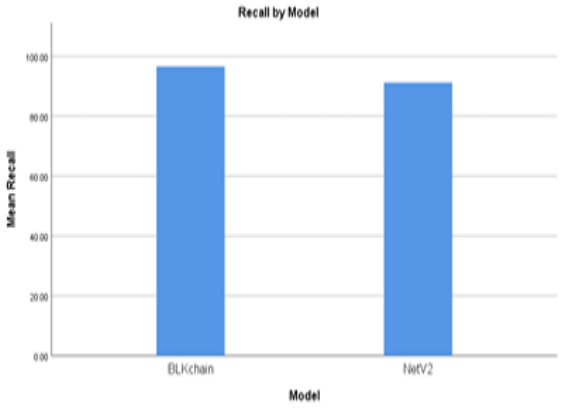
ISSN 2454-9940

www.ijasem.org

Vol 16, Issue 3, 2025



Blockchain and MobileNetV2 are equally effective and reliable, as seen in Fig. 6, as they both attain high accuracy with little false positives. Figure 6 shows that both Blockchain and MobileNetV2 achieve positive mean accuracy ratings without any notable false positives. It is evident that both models perform wonderfully and consistently, as anticipated, ensuring exceptional precision and efficiency.



Even while MobileNetV2 isn't quite as effective as Blockchain, it nevertheless ensures very few false positives (Fig. 7).

Blockchain achieved a recall of 100% and NetV2 somewhat lower but still near flawless, as shown in Fig. 7, which compares Blockchain with MobileNetV2. This proves that Blockchain finds all relevant positives without omission, and that MobilNetV2 does the same with very few missing positives; hence, both models are quite successful.

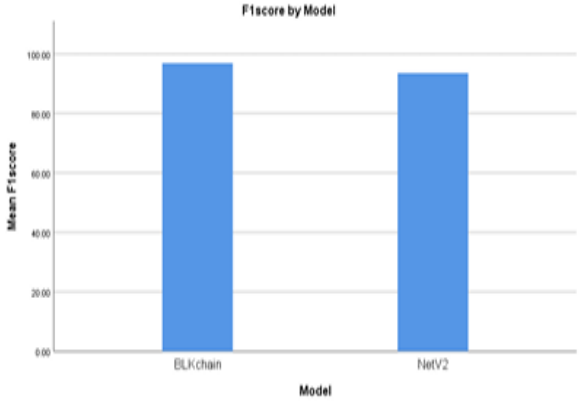


Fig.8: Blockchain and MobileNetV2 both have a perfect F1 score, s

howing that their recall and accuracy are well-balanced, guaranteeing that they work very well.

The findings are shown in Figure 8, which compares Blockchain with MobileNetV2 F1 scores. Both models are deemed to have outstanding accuracy and recall with a flawless score of 100. These models achieve outstanding overall performance in their respective tasks by reliably detecting true positives while reducing false negatives and false positives.

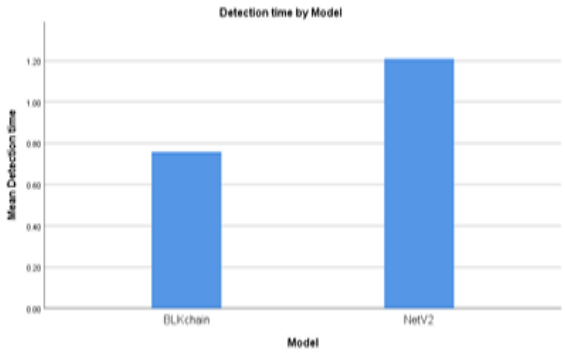


Figure 9: The graph contrasts the detection times of Blockchain (~0.76s) with MobileNetV2 (~1.21s), demonstrating the efficiency advantage of Blockchain.

Figure 9 shows See how the Blockchain and MobileNetV2 models stack up in terms of average detection time in the graph. With an average detection time of about 0.76 seconds, the Blockchain

model outperforms MobileNetV2's 1.21 seconds. This proves that the Blockchain paradigm is more efficient.

DISCUSSION

By using cutting-edge face recognition and blockchain technology to improve the safety and accessibility of online voting, the proposed technique increases the number of voters, especially Non-Resident Indians (NRIs). Using MobileNetV2 for continuous face validation will make the voting process more secure and less susceptible to hackers. Results from studies like [18] demonstrate that these technologies can improve facial recognition in real-time and secure vote inputs. Also, as revealed in [19], previous research has proved that blockchain prevents any manipulation or alterations, which guarantees vote integrity. Despite these improvements, issues about the system's scalability and its capacity to effectively manage large-scale elections have not been resolved. Unstable networks in certain areas could cause inaccurate real-time processing, which might impact system performance in unserved areas [20]. And that's before we even get into the rollout of

IN THE END

Since there are less logistical hurdles for Non-Resident Indians (NRIs) to use an online voting system, their electoral participation might be significantly increased. The ease of casting an online ballot has led many to speculate that as many as 72% of eligible non-resident Indians (NRIs) would cast ballots in the 2024 election. This strategy facilitates the participation of all eligible voters by doing away with the need that non-resident Indians physically visit the polls.
To make the polls more transparent and safe, technologies like face recognition and Aadhaar-based verification might be used. More people, no matter where they live, will have their voices heard in politics because of this invention. More individuals are able to access and participate in elections because to online voting, which is a huge boon to democracy.

REFERENCES

[1]. Louise Tillin wrote the piece titled "Indian elections 2014: explaining the landslide." Published in 2015, volume 23, issue 2, Section 2, pages 117–122, Modern South Asia "Smart Online Voting System," presented in 2021 in Coimbatore, India, by Ganesh Prabhu, Prabu, R.R. Thirrunavukkarasu, Nizarahammed, Raghul, and P. Jayarajan at the 7th International Conference on Advanced Computing and Communication Systems (ICACCS).

[2]. Hong-Ning Dai, Huaimin Wang, Xiangping Chen, Zibin, and Shaoan Xie [3]. "Blockchain challenges and opportunities: A survey."

[3]. International Journal of Web and Grid Services, Volume 14, Pages 352-375, 2018. Abdul Aziz, Mohd Juzaiddin, and Zarina Shukur. "Blockchain for electronic voting system—review and open research challenges."

[4]. Published in Sensors 21, issue 17, 2021, pages 5874/5875.
This is a list of writers that includes Safa Alsafari, Ashfaq, Tehreem, Sheraz Aslam, Rabiya Khalid, and Ibrahim A. Hameed (5). "A machine learning and blockchain based efficient fraud detection mechanism." On page 7166 of Issue 19, Sensors 22, 2022 takes place.
B. Anil Kumar, Mohan Bansal, and others cited in

[5]. "Face mask detection on photo and real-time video images using Caffe-MobileNetV2 transfer learning." The paper's number is 935 and it appears in volume 13, issue 2 (13/02/2023). Tolba, El-Sayyid, and El-Harby authored the report referred to as "Face recognition: A literature review." Volume 2, issue 2, pages 88-103, International Journal of Signal Processing, published in 2006.

[6]. Article writers include Manpyo Hong, Yunlim Ku, Okkyung Choi, Kangseok Kim, Taeshik Shon, Hongjin Yeh, and Jai-Hoon Kim. "Two-factor authentication system based on extended OTP mechanism." Published in 2013, pages 2515–2529, the International Journal of Computer Mathematics is volume 90, issue 12.

[7]. The authors of the "MobileNetV2 model for image classification" [9] were Dong, Ke, Chengjie Zhou, Yihan Ruan, and Yuzhi Li. These findings may be found in the 2020 IEEE Second International Conference on

Computer Applications (ITCA), specifically on pages 476-480. With the IEEE in 2020.

[8]. “Ertam, Fatih, Galip Aydın” printed. "Data classification with deep learning using Tensorflow." Here are the included pages: Pages 755-758 of the proceedings of the 2017 UBMK International Conference on Computer Science and Engineering. It was published by IEEE last year. Ming-Sheng Shang, An Zeng, and Quian-Ming Zhang are named in Reference 11. "Extracting the information backbone in online system." Publication: Vol. 8, No. 5, 2013: e62624.

[9]. Those who wrote "Checking data integrity using "blockchain." "CloudCom 2018: Proceedings of the IEEE International Conference on Cloud Computing Technology and Science," 272-277 pages of material. IEEE,Here we are in 2018.

[10]. Abed Ellatif Samhat, Layth Sliman, Hellani, Houssein, and Ernesto Exposito [13]. "On blockchain integration with supply chain: Overview on data transparency." Volume 46, Issue 5, March 5, 2021, Journal of Logistics.

[11]. Members of the Ren, Jin, Leng, Cheng, and Yongjun Ren groups [14]. "Secure data storage based on blockchain and coding in edge computing." Mathematical and Biosciences Engineering, 16th ed., issue 4, 2019, pages 1874–1892.

[12]. [15] This is Siddhartha Bhattacharyya. "A brief survey of color image preprocessing and segmentation techniques." Research paper included in the first issue of the Journal of Pattern Recognition

[13]. Ai, Gao, Xudong Diao, and Xin Jin were all listed in reference 16. "An Iterative Backbone Algorithm for Service Network Design Problems." Vol. 10, page 1373, published in 2022. Zachary P. Neal's R package "backbone" makes it possible to extract network backbones. The paper with the DOI: e0269137 was published in 2022 in the Open Science magazine. The four researchers that were a part of the study were Rahutomo, Faisal, Teruaki Kitasuka, and Masayoshi Aritsugi [18].

[14]. "Semantic cosine similarity." Volume 4, Issue 1, Page 1 of the Proceedings of the Seventh International Student Conference on Advanced Science and Technology (ICAST). South Korean publication from 2012 by Seoul National University.

[15]. Xing Ji, Yitong Wang, Zheng Zhou, Dihong Gong, Jingchao Zhou, Zhifeng Li, and Wei Liu were the authors of the cited study [19]. "Cosface: Large margin cosine loss for deep face recognition." The 2018 IEEE Computer Vision and Pattern Recognition Conference Proceedings, pages 5265–5274, are included here.

[16]. The authors of the work are Xu Yong, Zhang Zheng, Yang Jian, and Lu Guangming. "Approximately symmetrical face images for image preprocessing in face recognition and sparse representation based classification." Pattern Recognition, volume 54, 2016, pages 68–82.

[17]. Sowmitha and Mr. V. Senthilkumar are mentioned in the 21st reference. "A Cluster Based Weighted Rendezvous Planning for Efficient Mobile-Sink Path Selection in WSN." Volume 2, Issue 11, 2015, International Journal of Scientific Research and Development. The writers of the aforementioned work are V. Prakasham, M. Vimaladevi, and V. Sowmitha [22]. "A Secured and Authorized SEEN Protocol for Mobile Multimedia Data Collection Scheme in WMSNs."