S. Venkateshwara Rao, 2026, 14:3
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science,
Engineering and Technology
An Open Access Journal

Secure Digital Voting System Using Blockchain And Web Technologies

[1]S. Venkateshwara Rao,[2]Kota Spandana

[1]Assistant Professor, [2]M.Tech Student, Department of CSE,

Megha Institute Of Engineering And Technology For Womens, Edulabad (Village),

Ghatkesar (Mandal), Medchal District, Telangana

Abstract—In order to solve the problems with conventional offline voting in India, which include expensive prices, staff needs, delayed results, and accessibility concerns, especially for NonResident Indians (NRIs) and users with technical knowledge, we need to create a safe and effective online voting system. First, there's the Authentication Phase, when users are checked using Face Recognition and OTP Verification. Then, to make sure everything is honest, there's Live Real-time Monitoring and Session Monitoring. If anything fishy is found, the vote won't go through. Problems arise for Non-Resident Indians (NRIs) because to the high expenses and substantial human effort needed by India's current voting system, which uses Electronic Voting Machines (EVMs) and conventional ballot papers. To guarantee the safety of online voting, the suggested system incorporates several security measures, such as Aadhaar-based authentication with OTP, MTCNN for face recognition, MobileNetV2 for face real-time monitoring, Blockchain-based smart contracts for secure verification, and end-to-end encryption. Due to logistical constraints, the participation of non-resident Indian voters in conventional elections has been low. Because of the increased accessibility and convenience offered by an online voting system, projections indicate that participation will increase by 5% in 2024, reaching 72%. A more inclusive voting process and more participation are outcomes of this digital transition, which removes geographical obstacles (p = 0.049). By using cutting-edge technology like as TensorFlow and MobileNetV2, the created system successfully overcomes the shortcomings of conventional offline voting. Aligning with the changing demands of future generations and offering an inclusive solution for all voters, it provides the groundwork for a democratic voting process that is entirely digital, safe, and efficient.

Keywords— Blockchain, MobileNetV2, Online Vote, NRI, Face recognition, Secure, Real-time Monitoring, Aadhaar number.

I. INTRODUCTION

By using cutting-edge technology, an electronic voting system may revolutionise the traditional voting process. This system will fix current problems with accessibility for non-resident Indians and operational inefficiencies, all while guaranteeing the privacy, authenticity, and openness of data [1]. Electronic voting machines (EVMs) and ballot papers form the backbone of India's conventional voting system, which is notoriously labor-intensive, expensive, and fraught with complicated processes [2]. Research has shown that online systems save costs and are more accessible [3], thus there is a need for a more efficient method to keep up with the rising usage of digital technology. Secure, transparent, and real-time monitoring of elections is integrated into the proposed online voting system, which is based on deep learning and blockchain technology. This will help prevent fraud and expedite results [4]. Because it streamlines the voting process and makes it easier for tech-savvy consumers to participate in digital elections, this approach is great for them [5].

II. RELATED WORKS

Several real-world situations, including medical settings, crime scenes, and pandemics, have increased the need for reliable face mask identification and face recognition systems. In order to efficiently extract features and classify masked images, researchers in this field often use pre-trained deep learning models like MobileNetV2. Notable work in this area is [6], which achieves a classification accuracy of up to

99.64% for mask detection by integrating MobileNetV2 with extra layers to boost accuracy.

Notable publications like [7] also bring attention to face recognition in complicated settings, which might be affected by mask use. Both the successes and failures of facial recognition technology were highlighted by the results of the facial Recognition Vendor Test (FRVT) in 2002. Mobile banking has seen a surge in popularity, which has led to an increase in security measures, most notably one-time password (OTP) systems. Graphical one-time passwords (OTPs) and other mobile security solutions provide superior defence against hacker efforts [8]. Machine learning and computer vision researchers compare MobileNetV2's performance on picture categorisation tasks to that of earlier models, such as MobileNetV1.

The role of activation functions like ReLU in enhancing classification results has been the subject of several studies, such as [9]. A number of approaches have been investigated in the field of face recognition and authentication systems, one of which is the use of deep learning architectures such as CNN and MobileNetV2. Particularly in settings with varying variables (as when people wear face masks), these models have shown promising accuracy. Improving classification accuracy has been the focus of recent research into enhancing these models via the addition of layers to pre-existing architectures. For example, by adding five more layers to the MobileNetV2 model, the accuracy of its face mask detection was much enhanced (as shown in reference [10]).

Improvements in object identification and face recognition have been made possible by developments in activation functions (e.g., ReLU) and machine learning methods like TensorFlow [11]. Ongoing research has focused on how to incorporate blockchain technology into voting systems, particularly for elections. Immutable records and data integrity are two ways in which blockchain technology improves openness and safety. Blockchain technology has many potential uses, but it is not without its problems when it comes to protecting data storage [12], particularly in edge computing settings (as pointed out by [13]). A complete, secure, and user-friendly voting system for NRIs (Non-Resident Indians) is still lacking, despite the fact that prior research has improved facial recognition systems and integrated blockchain into safe platforms.

Making a foolproof voting system that integrates Aadhaar-based identification [14], real-time face recognition, and blockchain is no easy task. There aren't enough answers in the current literature that handle all these needs at once. The suggested system utilises many technologies, including as Aadhaar-based verification, face recognition, and blockchain, to provide a safe online voting platform for Indian citizens and non-residents (NRIs). By verifying the authenticity of every vote in real-time via validation and monitoring methods, this technology aims to improve election security and transparency. Using the MobileNetV2 model for continuous face identification during the session is a crucial part of this solution.

Based on the results thus far, it can be inferred that the proposed technique comprises improved security measures for online voting and integrates many layers to increase the accuracy of face mask identification in real-time. Concerns about the accessibility and integrity of elections are on the rise; this technology offers a solution by seamlessly integrating face recognition, OTP-based Aadhaar authentication, and blockchain security. When compared to other face recognition systems, the accuracy is much higher when using MobileNetV2 for face identification in conjunction with continuous session monitoring. There is a great deal of infrastructure, security, and human resources required for the very complicated voting system that uses electronic voting machines and traditional vote papers.

While EVMs have a modest computing cost for counting votes, conventional ballots have a low computational cost but a significant logistical expense. Adding sophisticated features like blockchain or authentication based on AI increases the processing

cost. The inefficiency of the system is worsened since it is still out of reach for non-resident Indians. The overall complexity of counting votes is O(n), however the operational and logistical overhead is low.

III. MATERIALS AND METHODS

This project aims to develop a safe and effective online voting infrastructure by using modern computational algorithms and blockchain technology. To improve voter verification and avoid fraud, MobileNetV2-based face recognition and Aadhaar authentication were used. To maintain security and system resilience, real-time session monitoring was included. People who aren't citizens of India but are proficient with technology are the target audience for this site.

In order to make voting easier, increase participation, and provide a reliable democratic voting process, important elements were session monitoring, live voter analytics, and blockchain-based vote security [15]. Group 1 makes use of the current voting system in India, which is still dependent on paper ballots and electronic voting machines (EVMs), which are labor-intensive, expensive, and time-consuming [16]. The inaccessibility of these systems makes it difficult, if not impossible, for Non-Resident Indians (NRIs) to participate un elections. Group 2 presents a solution for a safe online voting system that incorporates Aadhaar-based identification with one-time passwords, MTCNN for face recognition, and smart contracts built on the blockchain for trustworthy verification. With MobileNetV2's real-time face monitoring capabilities and blockchain's smart contracts and end-to-end encryption, voters may cast their ballots with peace of mind.

User authentication is the first step in an online voting system's workflow, which also includes session monitoring and finally, vote submission. With a 98.5% success rate and a 1.5% false positive rate, it checks the session integrity and either records the vote or rejects it if it finds out that the session is hacked. The procedure of a safe electronic voting system is shown in Figure 1.

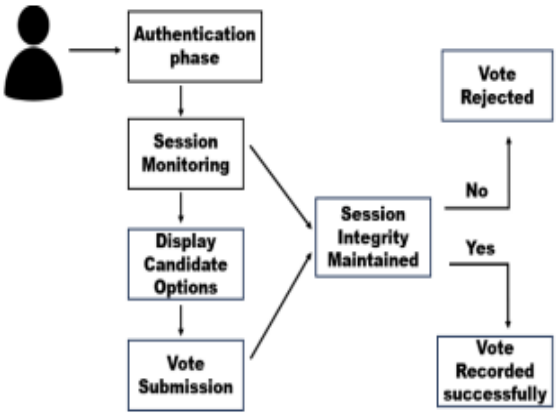


Fig. 1. Block diagram for Proposed System.

The shown procedure starts with the Authentication Phase, which involves verifying the user's identity using Face Recognition and One-Time Password (OTP) technology. The individual's Aadhaar number, name, and facial traits have been successfully verified. The accuracy of the person's identity authentication is guaranteed by this multi-layered verification procedure. In order to guarantee the authenticity of the session, the system will record the screen, monitor in real-time, and perform session monitoring if authentication is successful. Vote rejection occurs upon detection of Unwanted Activity.

If not, the user is prompted to browse Candidate Options, where they may choose a candidate and then confirm their selection. When the vote is about to be recorded, the system verifies if the session is secure. After a successful vote, the user is able to log out. In such case, the vote is not accepted. Validation and submission of votes guarantee that only qualified voters may safely cast their ballots. Methods such as ID authentication or face recognition are used to verify voters. After verification, their vote is sent in a secure manner, guaranteeing that it is both private and accurate.

IV. STATISTICAL ANALYSIS

To analyse the performance parameters of the MobileNetV2 and Blockchain models, including accuracy, recall, F1-score, and detection time, statistical analysis was carried out using SPSS version 26. This study included an independent samples t-test and group statistics [17]. The dependent variables included things like recall, accuracy, F1-score, and detection time, whereas the independent variable was the kind of model (NetV2 or Blochian). P-values less than 0.05 indicate uneven variances, according to Levene's test, which evaluated the equality of variances.

Precision, recall, and F1-score were supposed to have unequal variances, but detection time was considered to have equal variances. Results from the t-test showed that there were statistically significant variations in all parameters (Sig. 2-tailed < 0.05). Although MobileNetV2 had a longer detection time of 0.45100, Blockchain did better in terms of accuracy (-1.39200), recall (-5.40600), and F1-score (-3.35900). The results were further supported by the 95% confidence intervals, which showed that Blokhin was more efficient and performed better overall, especially when it came to detecting things quicker.

V. RESULT

The secure digital voting system's operation starts with voter authentication through face recognition and one-time password confirmation. It then moves on to features like real-time monitoring to guarantee integrity, session monitoring, and screen recording of transaction flows to prevent violence.

TABLE 2. From 2014 to 2024, there was a steady 26% increase in the number of votes cast by non-resident Indians. The number of registered voters increased from 12,000 to 118,000, and the number of estimated votes increased from 60 to about 30,680.

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)

For 2014, 2019, and 2024, the maximum participation of registered NRI voters is shown in Table I, which also includes other relevant voter statistics. There were 12,000 non-resident Indians (NRIs) who were eligible to vote in 2014, and their voting percentage was 0.5 percent, or 60 votes. With 71,735 eligible voters, turnout was 18,651—a 26% increase from the previous year. An estimated 30,680 ballots were cast out of 118,000 registered voters this year, according to the same 26% turnout projections.

Table 2: In the midst of ever-changing schemes and problems, some additional thought was given to testing and evaluating the frameworks in order to choose the best performance option. Two systems, MobileNetV2 and Blockchain, were subjected to a thorough evaluation.

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	user 009	96.4	97.1	91.75	96.4	94.02	96.75	1.3	0.76
10	user 100	95.8	97.85	90.5	96.8	93.08	97.32	1.5	0.75

Table 2. A Performance Evaluation Was Conducted On Mobilenetv2 And Blockchain To Determine The Best Option Amidst Evolving Schemes And Challenges.

Table 3. Blockchain Outperformed Mobilenetv2 In Precision (97.49% Vs. 96.1%) And Detection Time (0.76s Vs. 1.21s)

	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

Table 3.shows the results of the evaluations of recall, accuracy, F1-score, and detection time. Blochian outperformed MobileNetV2 across the board, outperforming it by a wide margin in accuracy (mean: 97.49% vs. 96.1%), detection time (mean: 0.76 s vs. 1.21 s), and all other measures.

Table Iv. The T-Test Confirms Blockchain Outperforms Mobilenetv2 In Precision, While Mobilenetv2 Has A Longer Detection Time, With Significant Differences (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	-0.71177
	Equal variances not assumed			-4.299	13.824	0.001	-1.39200	0.32378	-2.08726	-0.69674

Table 4: The results of the independent samples t-test reveal that, while MobileNetV2 has a longer detection time, Blockchain performs better in terms of accuracy. All measurements showed statistically significant differences (p = 0.049), and confidence intervals corroborated these findings.

In order to use the National Online Voting Portal, users are required to provide their complete name and Aadhaar number, as seen in Figure 2.

Figure 2 depicts the National Online Voting Portal, an official Indian government website that allows citizens to cast ballots online. To verify their identification, individuals are asked to provide their complete name and Aadhaar number in a straightforward form.

Figure 3 shows that after a user has authenticated using their Aadhaar data, the National Online Voting Portal validates the OTP verification.

An online voting system user called "Jerry" inputs their Aadhaar number and one-time password (OTP) for verification in Figure 3. A notification stating "Invalid OTP" appears. There was an issue with the OTP validation, and a popup message saying "Please try again" was shown. The layout has input areas and transparent submit and verify buttons.

Secure authentication with real-time monitoring to identify unauthorised access is achieved using the camera capturing a selfie for Aadhaar-based face recognition (Fig. 4).

To access the camera, one must take a selfie using a face-recognition camera (Fig. 4). This picture will subsequently be utilised for Aadhaar-based verification, which guarantees safe identity identification. By constantly checking identities and identifying unauthorised access, real-time monitoring further improves security.

Fig. 5. A verification success page displaying Aadhaar details with confirmation.

With the successful matching of the individual's name, Aadhaar number, and facial characteristics, the Aadhaar verification process is shown in Figure 5. The accuracy of the person's identity authentication is guaranteed by this multi-layered verification procedure. Validation and submission of votes guarantee that only qualified voters may safely cast their ballots. Methods such as ID authentication or face recognition are used to verify voters. After verification, their vote is sent in a secure manner, guaranteeing that it is both private and accurate.

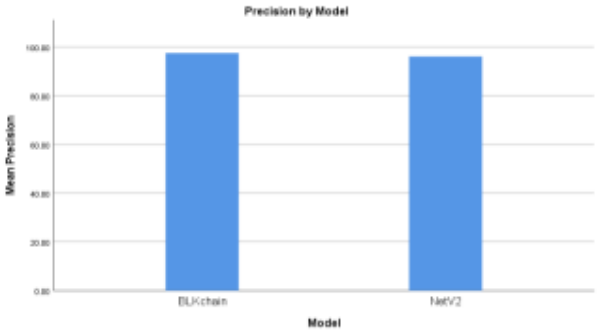
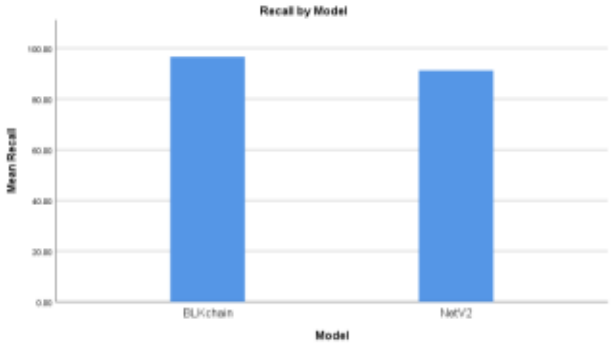


Figure 6 shows that Blockchain and MobileNetV2 are equally effective and reliable in achieving high accuracy with few false positives.

There are no statistically significant false positives in either the Blockchain or MobileNetV2 models, as seen in Fig. 6. This proves that all versions are equally good at what they do and very dependable, guaranteeing top-notch accuracy and performance.



While MobileNetV2's performance is somewhat lower than that of Blockchain (Fig.7), it is still quite effective and ensures that there are little missed positives.

In Figure 7, we can see that Blockchain achieved a recall of 100% and that NetV2 was somewhat lower but still very close to perfect when comparing their mean recall performance with MobileNetV2. This proves that Blockchain finds all important positives without omission, and that MobilNetV2 does the same with very few missing positives, demonstrating the efficacy of both models.

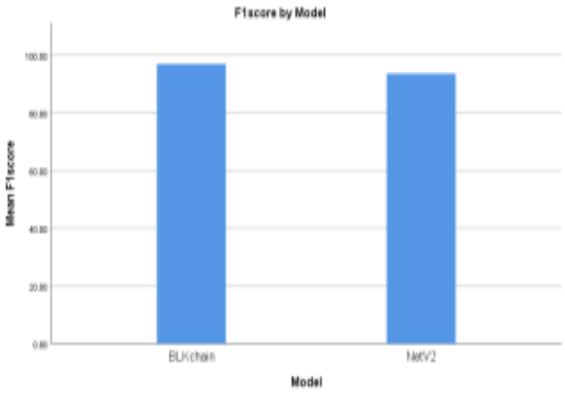
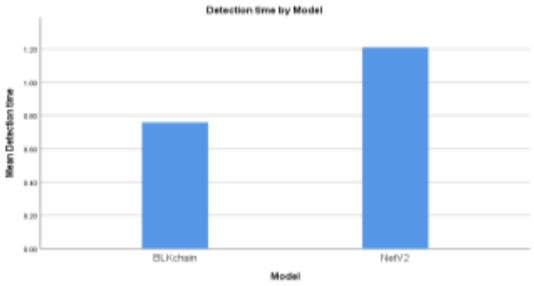


Figure 8 shows that both Blockchain and MobileNetV2 get a perfect score on the F1 test, which means that their recall and accuracy are well-balanced.

Figure 8 shows that when comparing Blockchain and MobileNetV2 on the F1 score, both models have a perfect score of 100, which means that their recall and accuracy are equally good. This outcome proves that both models perform admirably in their respective tasks by precisely detecting genuine positives and minimising false positives and false negatives.



In Figure 9, we can see that Blockchain has a much quicker detection time (~0.76s) than MobileNetV2 (~1.21s), demonstrating its higher efficiency.

You can see a comparison of the Blockchain and MobileNetV2 models' mean detection times in Figure 9. The mean detection time for the Blockchain model is around 0.76 seconds, which is quicker than MobileNetV2's 1.21 seconds. This proves that the Blockchain paradigm is more efficient.

VI. DISCUSSION

Higher voter participation, especially among Non-Resident Indians (NRIs), is a direct result of the proposed system's integration of cutting-edge face recognition and blockchain technology, which greatly improves the safety and accessibility of online voting. Enhancing the overall accuracy of the election system, the integration of MobileNetV2 for continuous face validation decreases the possibility for fraud or unauthorised access throughout the voting session. Research has shown that these technologies can improve face real-time recognition and make vote submissions more secure (e.g., [18]). Other research

applications, such as those by [19], have shown that blockchain can guarantee vote integrity by prohibiting any manipulation or modifications.Despite these improvements, questions remain about how well the system can scale to manage large-scale elections. Problems with real-time processing, especially in places with unpredictable network circumstances, could impact system performance in areas with inadequate internet infrastructure [20]. Furthermore, worries about energy consumption and the difficulty of integrating it with current voting systems make the deployment of blockchain in elections a divisive topic [21].

Although there have been notable advancements in security and inclusiveness, there is always need for development when it comes to making the system work better in low-resource settings and making sure it integrates smoothly with current voting infrastructures. The suggested system's capacity to process millions of votes in a massive election is also now being assessed. Improving system scalability, especially for large-scale elections, and investigating energy-efficient blockchain methods should be the focus of future study. Additionally, the system might be made more accessible in rural locations by improving its performance under different network situations, such intermittent connections or limited bandwidth.

VII. CONCLUSION

By eliminating the physical obstacles that have kept Non-Resident Indians (NRIs) from voting in the past, an online voting system might greatly increase NRI participation in elections. Estimates put the number of non-resident Indians voting in the 2024 election at 66.5%, but with the ease of casting a ballot online, that number might rise to 72 or even 72 percent. With this approach, qualified voters may cast their ballots remotely, making the process more accessible and removing the need for non-resident Indians to visit. The security and openness of the elections are further enhanced by integrating technology like face recognition and Aadhaar-based verification. This new development guarantees that all residents, no matter where they live, will have a say in the political process. By increasing the accessibility and participation in elections, the shift towards online voting signifies a revolutionary step in fortifying democracy.

REFERENCES

1. Tillin, Louise. "Indian elections 2014: explaining the landslide." Contemporary South Asia 23, no. 2 ,2015,pp.117-122.
2. Ganesh Prabhu S, Prabu S, R.R. Thirrunavukkarasu, Nizarahammed A, Raghul S, and P. Jayarajan, "Smart Online Voting System," in 2021 7th International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, India, 2021.
3. Zheng, Zibin, Shaoan Xie, Hong-Ning Dai, Xiangping Chen, and Huaimin Wang. "Blockchain challenges and opportunities: A survey." International journal of web and grid services 14, no. 4, 2018, pp: 352- 375.
4. Jafar, Uzma, Mohd Juzaiddin Ab Aziz, and Zarina Shukur. "Blockchain for electronic voting system—review and open research challenges." Sensors 21, no. 17, 2021, pp: 5874.
5. Ashfaq, Tehreem, Rabiya Khalid, Adamu Sani Yahaya, Sheraz Aslam, Ahmad Taher Azar, Safa Alsafari, and Ibrahim A. Hameed. "A machine learning and blockchain based efficient fraud detection mechanism." Sensors 22, no. 19, 2022, pp: 7162.
6. Kumar, B. Anil, and Mohan Bansal. "Face mask detection on photo and real-time video images using Caffe-MobileNetV2 transfer learning." Applied Sciences 13, no. 2, 2023, pp: 935.
7. Tolba, A. S., A. H. El-Baz, and A. A. El-Harby. "Face recognition: A literature review." International Journal of Signal Processing 2, no. 2 , 2006, pp: 88-103.
8. Ku, Yunlim, Okkyung Choi, Kangseok Kim, Taeshik Shon, Manpyo Hong, Hongjin Yeh, and Jai-Hoon Kim. "Two-factor authentication system based on

extended OTP mechanism." International Journal of Computer Mathematics 90, no. 12 , 2013: 2515-2529.

9. Dong, Ke, Chengjie Zhou, Yihan Ruan, and Yuzhi Li. "MobileNetV2 model for image classification." In 2020 2nd International Conference on Information Technology and Computer Application (ITCA), pp. 476-480. IEEE, 2020.
10. Ertam, Fatih, and Galip Aydın. "Data classification with deep learning using Tensorflow." In 2017 international conference on computer science and engineering (UBMK), pp. 755-758. IEEE, 2017.
11. Zhang, Qian-Ming, An Zeng, and Ming-Sheng Shang. "Extracting the information backbone in online system." PloS one 8, no. 5 (2013): e62624.
12. Kalis, Rosco, and Adam Belloum. "Validating data integrity with blockchain." In 2018 IEEE International Conference on Cloud Computing Technology and Science (CloudCom), pp. 272-277. IEEE, 2018.
13. Hellani, Houssein, Layth Sliman, Abed Ellatif Samhat, and Ernesto Exposito. "On blockchain integration with supply chain: Overview on data transparency." Logistics 5, no. 3 , 2021, pp: 46.
14. Ren, Yongjun, Yan Leng, Yaping Cheng, and Jin Wang. "Secure data storage based on blockchain and coding in edge computing." Math. Biosci. Eng 16, no. 4 , 2019, pp: 1874-1892.
15. Bhattacharyya, Siddhartha. "A brief survey of color image preprocessing and segmentation techniques." Journal of Pattern Recognition Research 1, no. 1
16. Gao, Ai, Xin Jin, and Xudong Diao. "An Iterative Backbone Algorithm for Service Network Design Problems." Processes 10, no. 7 , 2022, pp : 1373.
17. Neal, Zachary P. "backbone: An R package to extract network backbones." PloS one 17, no. 5, 2022, pp: e0269137.
18. Rahutomo, Faisal, Teruaki Kitasuka, and Masayoshi Aritsugi. "Semantic cosine similarity." In The 7th international student conference on advanced science and technology ICAST, vol. 4, no. 1, p. 1. South Korea: University of Seoul, 2012.
19. Wang, Hao, Yitong Wang, Zheng Zhou, Xing Ji, Dihong Gong, Jingchao Zhou, Zhifeng Li, and Wei Liu. "Cosface: Large margin cosine loss for deep face recognition." In Proceedings of the IEEE conference on computer vision and pattern recognition, pp. 5265-5274. 2018.
20. Xu, Yong, Zheng Zhang, Guangming Lu, and Jian Yang. "Approximately symmetrical face images for image preprocessing in face recognition and sparse representation based classification." Pattern Recognition 54, 2016, pp: 68-82.
21. S. Venkateswara Rao, S. Pushpalatha, "An Online Tool for Identifying and Classifying Apple Leaf Diseases Using Deep Learning in Real Time" In International journal of application or innovation in engineering and management, Vol. 14, 2025.
22. S. Venkateswara Rao, "The Use of Convolutional Neural Networks for the Monitoring of Driver Drowsiness" In IJARR,Vol.10, 2025.