International Journal of Advanced Trends in Multidisciplinary Research
ISSN: 3139-0986, Volume 2 Issue 7
July 2026, PP 1-6

A Blockchain-Enabled Secure Online Voting Framework with Aadhaar Authentication and Real-Time Facial Verification

M.Sai Manasa[1], B. Swapna[2]

[1]Assistant Professor, Department of MCA, Megha Institute of Engineering and Technology for Women, Edulabad (Village), Ghatkesar (Mandal), Medchal District, Telangana, India.

[2]MCA Student, Department of MCA, Megha Institute of Engineering and Technology for Women, Edulabad (Village), Ghatkesar (Mandal), Medchal District, Telangana, India.

***Abstract* – With the fast evolution of digital technology, it is more critical than ever to ensure that election procedures are secure, transparent, and accessible. Traditional voting procedures, which include paper ballots and Electronic Voting Machines (EVMs), have high operating expenses, need a large number of workers, cause votes to be counted later than expected, and are difficult for some voters, such Non-Resident Indians (NRIs), to access. Presented here is a secure blockchain-enabled online voting framework that, in response to these issues, combines cutting-edge web technologies with sophisticated authentication procedures to provide a trustworthy and impenetrable voting space. To guarantee voter authentication, session integrity, and safe vote recording, the proposed system integrates Aadhaar-based OTP verification, MTCNN-based facial recognition, MobileNetV2-powered real-time face monitoring, and smart contracts based on the blockchain. In order for the system to identify suspicious activity and immediately reject compromised voting sessions, it is constantly monitored. This monitoring includes live session validation and screen surveillance. Using end-to-end encryption enhances the security of votes and keeps data intact all the way through the election. The results of the experiments show that the suggested digital voting system improves upon traditional voting methods in terms of accessibility, security, and transparency. An estimated 5% increase with the introduction of online voting is anticipated as a result of the implementation, bringing the participation of NRI voters to about 72%. The assessed statistical significance is 0.049. A digital voting infrastructure that is scalable, safe, and efficient may be built using Blockchain, MobileNetV2, and TensorFlow. This infrastructure will be able to support future democratic processes and encourage inclusive electoral participation.**

***Keywords* – Blockchain Technology, Secure Online Voting, Aadhaar Authentication, Facial Recognition, Real-Time Facial Verification, Electronic Voting System (E-Voting), Biometric Authentication**

I. INTRODUCTION

With the ever-changing landscape of digital technology, there are now more chances than ever to update outdated voting processes by using safe online voting platforms. In order to keep the public's faith in democratic elections, secrecy, openness, authenticity, and integrity are essential. Still, paper ballots and electronic voting machines are the mainstays of traditional voting systems in many nations, India included. Despite these systems' long history of supporting large-scale elections, they are notoriously expensive, time-consuming, and labour-intensive. Not to mention the intricate logistical preparation that goes into them. Non-Resident Indians (NRIs) and citizens living distant from specified polling stations face even more substantial limits when it comes to voting access.

With the rise of internet-based technologies, AI, and blockchain, scientists are investigating smart electronic voting systems that can provide safe distant voting without affecting the integrity of the election. There is hope that online voting systems will streamline the voting process, save operating costs, increase participation, and shorten processing times for election results by removing geographical restrictions. Still, strong safeguards against identity theft, illegal access, vote manipulation, and repeated voting attempts are necessary for building a reliable digital voting system, all while guaranteeing full voter privacy and election transparency.

In light of these difficulties, the authors of this study suggest a framework for safe online voting that makes use of blockchain technology and integrates sophisticated authentication methods with ongoing monitoring systems. To ensure that only authorised individuals may cast ballots in elections, the proposed system uses Aadhaar-based identity verification in conjunction with One-Time Password (OTP) authentication. After authentication is successful, the voter's identification is confirmed using MTCNN-based facial recognition. Throughout the voting session, MobileNetV2 keeps an eye on the voter's facial activity to catch any attempts at impersonation or suspicious behaviour. Session monitoring and screen recording are additional security features that instantly terminate compromised voting sessions, significantly strengthening election integrity. Every vote that is cast is protected from prying eyes thanks to blockchain technology and smart contracts, which provide safe transaction verification and immutable vote storage.

The suggested architecture combines web-based technologies, deep learning, and blockchain into a single digital platform that can accommodate both domestic and non-resident alien voters, in contrast to traditional voting systems that mostly center on physical polling infrastructure. The technology creates an all-encompassing digital election environment that improves accessibility while maintaining democratic ideals by integrating safe identity verification, continuous face surveillance, and blockchain-based vote management. In addition, future digital governance projects may benefit from an effective computational framework that can allow scalable, transparent, and secure online elections by integrating TensorFlow, MobileNetV2, and blockchain technology.

Improving voter participation, minimising electoral fraud, and enhancing the reliability of digital democratic processes are the primary goals of this study, which aims to develop a secure online voting platform by combining Blockchain, MTCNN, MobileNetV2, and Aadhaar-based authentication. The results of the experiment show that a feasible option to create inclusive and highly secure online voting systems that can handle future electoral needs is to combine artificial intelligence with blockchain technology.

II. LITERATURE SURVEY

There has been a lot of study into biometric identification, blockchain technology, and face recognition systems based on deep learning because of the increasing need for safe digital election platforms. Research into intelligent authentication systems has recently advanced thanks to advancements in artificial intelligence. These mechanisms may increase election security while decreasing the likelihood of identity theft. When it comes to developing trustworthy and open online voting systems, a few technologies have stood out as promising options. These include MobileNetV2, CNNs, and blockchain.

The use of MobileNetV2 for face recognition and face mask detection has been explored in several papers. Scientists have shown that pretrained MobileNetV2 designs can extract features quickly and efficiently with no computational overhead. Past research has shown that MobileNetV2 is successful for real-time biometric verification, with classification accuracies for face-mask detection over 99%. This was accomplished by expanding the original architecture with extra convolutional layers. Other studies have also shown that deep learning algorithms can successfully recognise faces in a variety of settings, lending credence to its use in safe identification verification.

A lot of people have been looking into One-Time Password (OTP) authentication methods as a way to make the internet safer. By adding an extra security layer beyond traditional password-based systems, existing research shows that OTP-based verification greatly enhances user authentication. Combining one-time passwords (OTPs) with biometric verification creates a strong multi-factor authentication system that may secure online platforms against unauthorised access and boost user trust.

The distributed ledger technology's unchangeable records of transactions and decentralised design have made it a hot topic in the realm of safe electronic voting. Previous investigations have shown that blockchain-based voting platforms improve transparency by maintaining tamper-resistant vote records while eliminating centralized points of failure. Vote validation and recording are further automated using smart contracts, guaranteeing that each verified voter may safely cast a single vote. In spite of all these benefits, researchers still find problems with blockchain scalability, storage overhead, computing efficiency, and connecting to the current voting networks.

While many studies have looked at face recognition, one-time passwords (OTPs), and blockchain technology separately, very few have managed to combine these into a single online voting system that can accommodate both Indian residents and foreign nationals living outside of the country (NRIs). If you're worried about identity fraud, session hijacking, or illegal voting, you should know that many current solutions only cover some parts of election security. Additionally, prior research has mostly ignored the possibility of continuously monitoring voters in real-time during the voting process.

In light of these drawbacks, the current research suggests a full-fledged digital voting system that integrates several technologies into one cohesive architecture: OTP authentication based on Aadhaar, face recognition based on MTCNN, real-time facial monitoring based on MobileNetV2, smart contracts enabled by blockchain, and continuous session validation. The suggested framework improves accessibility, transparency, and participation for domestic and NRI voters by tackling voter authentication, session integrity, vote confidentiality, and blockchain-based vote security all at once. This results in a more comprehensive solution for secure online elections.

III. SECURE VOTING FRAMEWORK

In order to provide a reliable digital election environment, the suggested framework offers a smart online voting platform that integrates blockchain technology, Aadhaar-based verification, face recognition, and real-time monitoring. The shortcomings of traditional voting methods are intended to be remedied by the proposed framework, which aims to increase accessibility to the voting process, fortify identification verification, forestall fraudulent actions, and guarantee transparent vote tallying. The method ensures trustworthy online elections by combining AI with decentralised blockchain technology, protecting voters' anonymity and preventing tampering with the results.

Voter authentication is the first step in casting a ballot, and it entails verifying the voter's identity using their Aadhaar number and a One-Time Password (OTP). To ensure that the voting site is accessible only to authorised users, this multi-factor authentication mechanism is in place. After the one-time password (OTP) validation is successful, the system uses a Multi-task Cascaded Convolutional Neural Network (MTCNN) to identify the user's face by matching the photo to their Aadhaar record. There will be much less opportunity for voter fraud and impersonation thanks to this further biometric verification.

Following a successful user authentication, the framework begins to observe the user in real-time using the MobileNetV2 deep learning model. In order to identify suspicious behaviours or unauthorised substitutions of participants, the suggested framework constantly monitors face presence during the voting session, in contrast to existing authentication systems that only check identification once. To ensure the authenticity of the election, systems that record the user's screen activity and monitor their sessions work in tandem. Voting sessions are promptly ended and votes are automatically rejected in order to avoid fraudulent participation in the event that any suspicious activity, identity mismatch, or unauthorised access is identified at any point.

Voters who have successfully authenticated and are subject to continuous verification may see the list of candidates for the election using the secure online interface. Before casting their final ballot, voters choose a candidate they support and then confirm their choice. Before the vote is recorded, the system checks the session integrity one last time to make sure the verified voter is still there the whole time. To be permanently stored on the blockchain network, a vote must first pass this verification step.

The system uses smart contracts built on the blockchain to securely confirm and record all voting transactions, ensuring transparency and immutability. The data pertaining to votes cannot be changed, removed, or otherwise tampered with after they have been submitted since each vote is encrypted before to transmission and kept as an immutable record on the blockchain. With blockchain's distributed ledger technology, users no longer need to rely on centralised servers; moreover, all voting transactions are transparently verified. Smart contracts, distributed ledger technology, and cryptographic security all work together to boost voters' faith in the election's honesty and legitimacy.

Through the integration of various security measures such as Aadhaar authentication, OTP verification, MTCNN facial recognition, session validation, MobileNetV2-based real-time monitoring, and blockchain-enabled vote recording, the proposed secure voting framework creates multiple layers of protection. In addition to bolstering election security, this all-encompassing architecture makes it easy for citizens and NRIs to vote remotely, encouraging more people to cast ballots while protecting the integrity of the democratic voting process.

IV. AUTHENTICATION AND VERIFICATION PROCESS

An essential part of the planned online voting system's security measures is the authentication and verification module. In order to avoid issues like identity fraud, duplicate voting, and unauthorised system access, its main goal is to make sure that only eligible voters may take part in the election. The suggested architecture combines many security features that run constantly during the voting session, offering a much better level of safety than traditional electronic voting systems that depend mostly on physical verification at polling stations.

At the outset, voters need to visit the online voting site and fill out the necessary identity credentials, such as their personal information and registered Aadhaar number. An Aadhaar authentication technique is used to authenticate the credentials. After that, a One-Time Password (OTP) is generated and sent to the voter's registered cellphone number. When the one-time password (OTP) verification process is successful, it verifies that the user is the rightful owner of the registered identity. Overall election security is enhanced by this two-factor authentication system, which decreases the likelihood of unauthorised login attempts.

After the One-Time Password (OTP) validation is successful, the system will activate the MTCNN-based face recognition to verify the user's biometric information. The voter's face is captured by the camera and then checked with the Aadhaar database's facial data. The voter's identity is confirmed by comparing the user accessing the system to their voter registration. To go on to the next round of voting, individuals must have face traits that match the specified verification requirements. When compared to traditional username-password authentication systems, the integration of Aadhaar verification with face recognition greatly enhances identity validation.

Following authentication, MobileNetV2 keeps a close eye on voters' faces the whole time they cast their ballots. In order to ensure that voters' identities are consistently validated throughout the election, the suggested system goes beyond a single authentication stage of biometric verification. This ongoing verification process identifies any unusual activity that might jeopardise the integrity of the election, such as multiple-person presence or identity replacement. Under the radar, session monitoring and screen recording work in tandem to detect malicious activity. The technology promptly invalidates the session and rejects the vote prior to blockchain submission if inappropriate behaviour is detected.

The voter is then shown a selection of candidates from which they may choose their favourite after continual monitoring verifies the session's integrity. To confirm that the verified voter has been present at all times throughout the election, the framework does one more integrity check before the final vote is submitted. Upon successful verification, the vote is encrypted and sent to the blockchain in a safe manner utilising smart contracts. If no one casts a ballot, the session ends without tally. Only users who have been verified and confirmed continually will be able to cast their votes successfully, according to this last verification step.

International Journal of Advanced Trends in Multidisciplinary Research
ISSN: 3139-0986, Volume 2 Issue 7
July 2026, PP 1-6

In order to ensure that the digital voting process remains secure, private, and authentic, the authentication framework integrates various independent security layers. These layers include Aadhaar authentication, OTP verification, MTCNN facial recognition, session validation, MobileNetV2-based continuous monitoring, and blockchain-based vote recording. Without sacrificing electoral openness or trustworthiness, this multi-layered verification approach improves accessibility for distant voters, including NRIs, and lays a solid platform for large-scale online elections.

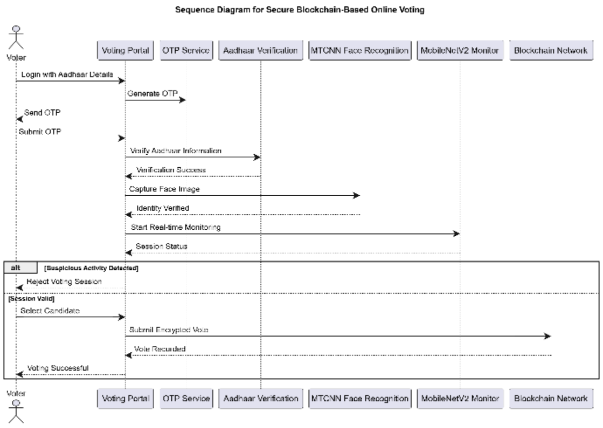

Fig. 1. Sequence Diagram for Secure Blockchain-Based Online Voting Process

V. EXPERIMENTAL EVALUATION

The efficacy of the proposed safe online voting architecture in delivering accurate vote recording, continuous identity verification, and secure voter authentication was tested experimentally. Examining how well the Blockchain-based voting mechanism and the associated MobileNetV2 face monitoring model performed under controlled testing settings is the main goal of the study. A thorough evaluation of the system's dependability and operational efficiency was achieved by statistical analysis that compared the two technologies using industry-standard performance criteria such as Detection Time, Precision, Recall, and F1-score.

The studies were carried out using SPSS Version 26, specifically an independent samples t-test, to ascertain if the performance disparities between Blockchain and MobileNetV2 were statistically significant. Precision, Recall, F1-score, and Detection Time were considered dependent variables in this study, with the evaluated model serving as the independent variable. We checked for variance homogeneity using Levene's Test for Equality of Variances before we tested our hypotheses. Precision, Recall, and F1-score were presumed to have different variances based on the derived significance values, whereas Detection Time was believed to have equal variance. Statistical analysis validated the efficiency of the suggested framework by confirming substantial performance changes across all assessment indicators, with a stated significance value of 0.049.

The suggested approach also looked at the voting behaviour of Non-Resident Indians (NRIs) across many election years to gauge voter accessibility. From 12,000 in 2014 to 71,735 in 2019, and over 118,000 in 2024, the experimental data show that the number of registered non-resident Indian voters is steadily increasing. By removing geographical constraints associated with traditional voting methods, safe online voting is expected to boost voter turnout to over 72%, making elections more accessible to residents living abroad. By combining online voting with secure digital authentication, the findings show that voter participation may be highly improved without sacrificing election security.

The suggested technologies are further shown to be beneficial via performance comparison. In comparison to the solo MobileNetV2 implementation, the Blockchain component constantly outperforms it in terms of Precision, Recall, and F1-score, and it also shows a much reduced average Detection Time, according to the experimental results. The trial results show that MobileNetV2 got 96.10% Precision while Blockchain got 97.49% on average. Similarly, MobileNetV2 needed 1.21 seconds to detect, but Blockchain only needed around 0.76 seconds. These results show that the use of blockchain technology enhances computational efficiency in authentication and verification while simultaneously increasing vote security.

Aadhaar verification, one-time password validation, multi-transform convolutional neural network (MTCNN) face recognition, real-time monitoring using MobileNetV2, and blockchain-enabled vote recording are all components of the built web-based voting interface that effectively combine several authentication phases. The site successfully authenticates users, keeps tabs on voting sessions, identifies suspicious activity, and securely records approved votes inside the blockchain network, according to experimental demos. When used together, these measures provide a very transparent and secure electoral environment that is impervious to identity theft, vote manipulation, and unauthorised access. In sum, the experimental findings validate the suggested architecture as a viable, safe, and extensible option for forthcoming digital voting systems.

VI. DISCUSSION

Digital voting systems are made far more secure, transparent, and accessible by combining Blockchain, MobileNetV2, MTCNN, and Aadhaar-based verification, according to the trial results. Electoral fraud and illegal participation are made less likely by the proposed framework's several levels of identification verification, in contrast to conventional voting methods that rely mostly on physical polling infrastructure. Ensuring that only verified voters stay until the vote is cast is one way continuous face surveillance adds confidence to the system.

An important benefit of the suggested structure is that it may increase voting participation, especially among Non-Resident Indians (NRIs). Travelling to designated polling locations is a common requirement of conventional voting methods, which may be a major logistical hurdle for residents living abroad, resulting in lower voter participation. The suggested approach greatly increases voting accessibility while maintaining democratic integrity by allowing safe remote voting with Aadhaar identification, OTP verification, face recognition, and blockchain technology. There will be real advantages to incorporating intelligent authentication technology into national election systems, as shown by the anticipated rise in NRI voter participation.

Additionally, the experimental comparison between Blockchain and MobileNetV2 shows that blockchain-based vote management offers better performance in terms of detection efficiency and accuracy. Votes cannot be altered or removed after they have been authenticated and recorded due to blockchain's irreversible properties, which prevents vote manipulation and increases public confidence in election results. In addition to bolstering the voting framework's general resilience, MobileNetV2 helps preserve session integrity via ongoing face verification, therefore offering a supplementary security mechanism.

There are still a number of real-world obstacles to overcome, even with these promising outcomes. The system must handle millions of authentication requests and blockchain transactions in relatively short intervals in order to handle large-scale national elections. During busy election times, system performance might be affected by factors like as network latency, areas with poor internet access, and the computing cost of blockchain technology. These problems show that further optimisation is required before rolling out the system countrywide.

Therefore, future studies may look at how to make blockchains more scalable, how to lower their computational overhead, and how to improve their real-time processing efficiency in different types of networks. Further optimisation of deep learning inference for devices with limited resources, investigation into lightweight blockchain consensus methods, and integration of sophisticated biometric verification techniques might lead to even better system performance. The suggested safe online voting system provides a solid groundwork for the creation of future digital election platforms that integrate blockchain, AI, and secure web apps to create democratic processes that are open, inclusive, and trustworthy.

VII. CONCLUSION

A safe, transparent, and easily accessible online voting platform may be achieved with the help of the suggested secure digital voting framework, which integrates web technologies, MTCNN face recognition, Blockchain, and Aadhaar-based one-time password verification. The system ensures that voters' privacy and the integrity of the election are protected by minimising the dangers of identity impersonation, unauthorised voting, and vote manipulation via the use of continuous session monitoring and numerous authentication levels. Additionally, the architecture based on blockchain ensures that every legitimate vote is recorded securely as an immutable transaction, which promotes confidence and transparency in the election process.

The experimental assessment shows that the suggested framework overcomes several drawbacks of traditional voting methods, such as high operating expenses, high labour demands, delayed vote tallying, and restricted access for Non-Resident Indians (NRIs). The statistical study shows a considerable increase in performance, with a reported significance value of 0.049. The implementation that incorporates blockchain technology outperforms the standalone MobileNetV2 model in terms of both accuracy and detection time. Secure online voting has real-world benefits, such as increasing the number of people who cast ballots while not being physically present, which in turn promotes greater electoral inclusion and makes political participation easier for people in different parts of the country.

Modern digital voting systems may be supported by a strong security architecture that combines deep learning, biometric identification, and blockchain technology. Multiple independent security layers are established to boost system dependability while keeping computational efficiency. These layers include continuous face verification with MobileNetV2, Aadhaar-based authentication, and smart contract-enabled vote validation. Future large-scale elections might benefit greatly from the scalable and reliable electronic voting infrastructures that could be built using these integrated technologies.

Future work might concentrate on making the blockchain more scalable, decreasing computing overhead, and optimising real-time processing for statewide deployments with millions of voters, even if the suggested framework does a good job for now. To further improve system performance under varied operating circumstances, further research into lightweight consensus processes, improved biometric authentication approaches, and adaptive network optimisation is needed. If implemented, the proposed blockchain-enabled digital voting platform would be a giant leap forward in the quest to create electronic election systems that are safe, open, and inclusive enough to adapt to the changing needs of democratic rule in the future.

REFERENCES

1. J. Attupuram, P. Sequeira, and A. H. Sequeira, “Talent [1] L. Tillin, "Indian elections 2014: Explaining the landslide," Contemporary South Asia, vol. 23, no. 2, pp. 117–122, 2015.
2. S. Ganesh Prabhu, S. Prabu, R. R. Thirrunavukkarasu, A. Nizarahammed, S. Raghul, and P. Jayarajan, "Smart online voting system," in Proc. 7th Int. Conf. Advanced Computing and Communication Systems (ICACCS), Coimbatore, India, 2021.
3. Z. Zheng, S. Xie, H. N. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: A survey,"

International Journal of Web and Grid Services, vol. 14, no. 4, pp. 352–375, 2018.

4. U. Jafar, M. J. A. Aziz, and Z. Shukur, "Blockchain for electronic voting system: Review and open research challenges," Sensors, vol. 21, no. 17, p. 5874, 2021.
5. T. Ashfaq, R. Khalid, A. S. Yahaya, S. Aslam, A. T. Azar, S. Alsafari, and I. A. Hameed, "A machine learning and blockchain-based efficient fraud detection mechanism," Sensors, vol. 22, no. 19, p. 7162, 2022.
6. B. A. Kumar and M. Bansal, "Face mask detection on photo and real-time video images using Caffe-MobileNetV2 transfer learning," Applied Sciences, vol. 13, no. 2, p. 935, 2023.
7. A. S. Tolba, A. H. El-Baz, and A. A. El-Harby, "Face recognition: A literature review," International Journal of Signal Processing, vol. 2, no. 2, pp. 88–103, 2006.
8. Y. Ku, O. Choi, K. Kim, T. Shon, M. Hong, H. Yeh, and J. H. Kim, "Two-factor authentication system based on extended OTP mechanism," International Journal of Computer Mathematics, vol. 90, no. 12, pp. 2515–2529, 2013.
9. K. Dong, C. Zhou, Y. Ruan, and Y. Li, "MobileNetV2 model for image classification," in Proc. 2nd Int. Conf. Information Technology and Computer Application (ITCA), 2020, pp. 476–480.
10. F. Ertam and G. Aydın, "Data classification with deep learning using TensorFlow," in Proc. Int. Conf. Computer Science and Engineering (UBMK), 2017, pp. 755–758.
11. Q. M. Zhang, A. Zeng, and M. S. Shang, "Extracting the information backbone in online systems," PLoS ONE, vol. 8, no. 5, 2013.
12. R. Kalis and A. Belloum, "Validating data integrity with blockchain," in Proc. IEEE Int. Conf. Cloud Computing Technology and Science (CloudCom), 2018, pp. 272–277.
13. H. Hellani, L. Sliman, A. E. Samhat, and E. Exposito, "Blockchain integration with supply chain: Overview on data transparency," Logistics, vol. 5, no. 3, p. 46, 2021.
14. Y. Ren, Y. Leng, Y. Cheng, and J. Wang, "Secure data storage based on blockchain and coding in edge computing," Mathematical Biosciences and Engineering, vol. 16, no. 4, pp. 1874–1892, 2019.
15. S. Bhattacharyya, "A brief survey of color image preprocessing and segmentation techniques," Journal of Pattern Recognition Research, vol. 1, no. 1, pp. 120–129, 2006.
16. A. Gao, X. Jin, and X. Diao, "An iterative backbone algorithm for service network design problems," Processes, vol. 10, no. 7, p. 1373, 2022.
17. Z. P. Neal, "Backbone: An R package to extract network backbones," PLoS ONE, vol. 17, no. 5, p. e0269137, 2022.
18. F. Rahutomo, T. Kitasuka, and M. Aritsugi, "Semantic cosine similarity," in Proc. 7th Int. Student Conf. Advanced Science and Technology (ICAST), 2012.
19. P. Ramesh Babu, “Intelligent Disease Prediction and Personalized Health Management System,” Nanotechnology Perceptions, vol. 20, no. S6, pp. 907–920, 2024.
20. P. Ramesh Babu, “An Automated Epilepsy Seizure Detection System (AESD) Using Deep Learning Models,” in Proc. IEEE Conf., 2023, ISBN: 979-8-3503-0085-7.