Optimizing Electoral Integrity: A Blockchain and Machine Learning-Enhanced Voting App with an Advanced Ensemble Model

Ajmeet kour
CSE
Chandigarh university
Mohali, Punjab
ajmeetkour33@gmail.com

Nishchay sorout
CSE
Chandigarh university
Mohali, Punjab
nishchaysorout@gmail.com

Muskan
CSE
Chandigarh university
Mohali, Punjab
muskan5972sharma@gmail.com

Avneet kaur
CSE
Chandigarh university
Mohali, Punjab
Avneett.e14476@cumail.in

***Abstract*—The combination of Blockchain and Machine Learning (ML) technologies has opened new avenues for creative solutions in several fields, including the crucial area of voting systems, in the modern era of technological growth. To improve voting processes' security and accuracy, this study presents a unique voting application that makes use of machine learning's predictive capabilities in conjunction with the immutable and transparent nature of blockchain technology. Through the use of an ensemble model that incorporates the Gradient Boosting, Decision Tree, and Logistic Regression techniques, the programmed attains an astounding accuracy of 0.97. The ensemble model's capacity to maximize the benefits of each individual algorithm while minimizing its drawbacks is responsible for this outstanding performance, which produces a strong and dependable prediction mechanism. The use of Blockchain technology guarantees the safe recording and verifiability of every vote, therefore mitigating the long-standing issues of vote manipulation and fraud. In addition to demonstrating the possibilities of fusing blockchain technology with machine learning.**

Keywords—Machine Learning, Ensemble Model, Blockchain, Voter, App

I. Introduction

A democracy's fundamental element is its voting system, which supports the authority of the government and the laws it enacts. With the potential of improving accessibility, efficiency, and convenience in electoral processes, electronic voting systems have attracted a lot of attention since the emergence of digital technology. These systems do, however, also present difficult security, voter privacy, and reliability issues. Blockchain technology presents a strong answer to these problems because of its intrinsic decentralisation, immutability, and transparency properties [1].

Voter coercion, ballot manipulation, and logistical inefficiencies are just a few of the long-standing problems with traditional voting systems that may be resolved by using a Blockchain-based voting software [2]. Through the utilisation of a Blockchain's unchangeable vote records, every vote can be tracked back to its original source while maintaining voter privacy. This system makes sure that a vote cannot be removed or changed once it has been recorded, creating an auditable and verifiable trail that raises the election process's legitimacy [3].

Moreover, Blockchain's decentralised structure naturally thwarts power consolidation and potential manipulation by a single party. By distributing trust throughout a network of nodes, it makes sure that the voting mechanism is resistant to both technological breakdowns and cyberattacks [4]. Since every transaction on the Blockchain is verified by consensus and the ledger is duplicated among several nodes, the integrity of the vote cannot be jeopardised by a single point of failure.

Machine learning is a force multiplier that increases the system's ability to recognise and react to new threats by being integrated into this ecosystem. ML systems may notify administrators of any fraudulent activity in real-time by analysing voting patterns and identifying abnormalities. Adaptive security measures, in which the system changes to fight new strategies used by malevolent actors, can also be facilitated by advanced data analytics driven by machine learning [6].

The accessibility and scalability issues are also addressed by the combination of blockchain technology and machine learning in a voting software. Voting services may be distributed via the peer-to-peer network of blockchain, which eliminates the need for centralised infrastructure that may become congested or vulnerable to intrusions [7]. In addition, machine learning algorithms have the capacity to enhance network performance by managing substantial amounts of data and transactions, guaranteeing that the system can evolve to meet the needs of an expanding electorate .

This study explores how to create a voting app that uses blockchain technology in conjunction with machine learning (ML) algorithms to guarantee the accuracy, security, and dependability of the voting procedure. Because votes can be recorded in a safe, impenetrable environment thanks to blockchain's distributed ledger, voting is more transparent and less prone to fraud. Furthermore, the use of ML can strengthen the system's resilience by assisting in the identification and mitigation of unusual patterns and possible security risks [8].

Voting systems that are easier to use and more secure have grown more and more necessary in recent years. The goal of this study is to rebuild public confidence in voting institutions, which has been damaged by ongoing problems with voter

suppression, security lapses, and questions about the accuracy of vote tallying [9]. Blockchain and machine learning have enormous potential to solve these issues, providing not just little fixes but a radical change in the way votes are cast, tallied, and verified. The belief that technology may greatly improve the democratic process and guarantee that every vote is not only tallied but also secure against the flaws in conventional voting methods is the driving force behind this paper [10].

The paper is organized importance of the research are established in the Introduction, which also sets the scene. The Literature Review section identifies gaps that this research attempts to solve by surveying previous studies, technology, and approaches. The theoretical foundation, the Voting App's system design, and the particular algorithms used are all covered in depth in the Methodology section. The performance and security analysis of the Voting App, along with other discoveries from its deployment, are presented in the Results and Discussion section. The last section, Conclusion and Future Scope, summarises the main lessons learned and considers the ramifications for the subject of digital democracy.

II. Literature Review

The authors [11] suggested blockchain-based electronic voting method provides confidence, transparency, and treasury while guarding against network interference. Machine learning techniques are employed by the system to improve voting process security and accuracy. Blockchain technology guarantees the vote data's integrity and immutability, making it impervious to manipulation or tampering. To further improve system security, machine learning techniques can be used to identify abnormalities or suspect activity during the voting process. A reliable and secure platform for electronic voting is offered by the combination of blockchain technology with machine learning, which addresses issues with privacy, trust, and transparency. By providing a decentralised approach, the system lowers the possibility of single points of failure and does away with the necessity for a central authority.

The authors [12] study's goal is to use blockchain technology to develop a simple, safe, and electronic voting method. When compared to conventional voting techniques, the approach makes voting easier by enabling individuals to utilize their phones. By avoiding vote manipulation or tampering, the usage of blockchain assures the security and integrity of the voting process.

The authors [13] need an Ethereum client in order to connect to the Ethereum blockchain. The ecosystem of false information on the Web is made up of many kinds of misleading information, actors, and their motivations. Political disinformation spreads more quickly and widely than other forms of disinformation and can have disastrous effects.

It authors [14] has suggested that blockchain technology can help overcome the drawbacks of the current electronic voting methods. The authors' work concentrated on employing a network that timestamps transactions and creates an immutable record using hash-based proof-of-work to address the double-spending issue. The goal of the proposed blockchain-based electronic voting system is to improve the integrity and reliability of electronic voting by using the security and transparency offered by blockchain frameworks. This work-in-progress article assesses different blockchain frameworks to see if they can be used to build an electronic voting system based on blockchain.

The authors [15] used potential of electronic voting technologies to improve voting process security, transparency, and efficiency has drawn a lot of interest. Because it offers a decentralized, tamper-proof platform for recording and confirming votes, blockchain technology has emerged as a

possible alternative for electronic voting systems. Since every vote is registered as a transaction on the blockchain, the use of blockchain in electronic voting systems guarantees immutability and transparency and makes it more impossible for any unauthorized entity to tamper with or manipulate the results. Because blockchain technology guarantees the accuracy and integrity of the voting process, blockchain-based electronic voting systems also do away with the need for middlemen like election officials.

In the framework of safe and intelligent electronic voting, blockchain technology is used to guarantee the transparency and integrity of votes. The authors [16] process of verifying eligible voters is automated with the use of machine learning (ML). The face authentication process is carried out using an AI-powered oracle platform, which boosts the e-voting system's intelligence and security. The problems with safe and thoughtful electronic voting are addressed by the blockchain, machine learning, and artificial intelligence- powered oracle platform. Voting systems utilising blockchain technology have drawn interest from the literature, and several authors and organizations are actively pursuing this line of inquiry.

The authors [17] Deep learning and computer vision have been used to create a smart voting system that secures voter passwords and confirms that the right voter is casting their ballot. Voters can use the system to confirm that their vote was received by the designated party.

To reduce fraudulent activity and guarantee safe transactions, a permissioned blockchain voting mechanism is suggested. The authors [18] improve trustworthiness and dependability in data sharing across communication channels, the system makes use of a permissioned blockchain network. To enhance privacy, security, and latency in information exchange, the system integrates RSA digital signatures with a Java programming version. The goal of the suggested approach is to guarantee vote integrity by creating a voting environment devoid of incentives. The approach lowers the possibility of manipulation and fraud by providing a transparent and safe voting platform through the use of blockchain technology.

The authors [19] study provides a proof-of-concept for a

blockchain-based distributed and decentralized electronic voting application in an Internet of Things embedded device. End-to-end security and total voter privacy are guaranteed by the proposed solution for all parties involved in the electronic voting process. Transparency, immutability, and tamper-proofing of the vote data are all provided by using blockchain technology in the voting process. The integrity of the voting process is ensured by the integration of IoT devices, which enables efficient and secure communication between the voting units. By using the advantages of blockchain and Internet of Things technology, the system seeks to overcome the shortcomings of conventional voting methods, including voter identity, ballot confidentiality, and result integrity.

The study by the authors [20] offers a thorough examination of the blockchain-based electronic voting system. The authors point out possible issues with the existing voting method and provide fixes to make it safer and more conducive to system reconstruction. The study highlights the usage of decentralized apps (DAPPs) that take advantage of blockchain

technology to facilitate electronic voting. In the context of electronic voting, the writers go over the benefits of using blockchain technology, including security, immutability, and transparency. The study also cites 28 other sources that shed further light on the subject of blockchain- based decentralized electronic voting systems.

III. Methodology

Nearest Neighbours (KNN) is a useful algorithm for classification tasks given its simplicity and efficacy. It is particularly adept at detecting anomalies in voting patterns. A hybrid approach combining Random Forest and KNN modelling should be used to benefit from their respective strengths. Ensemble methods or a voting mechanism needs to be employed to determine the final outcome based on both models.

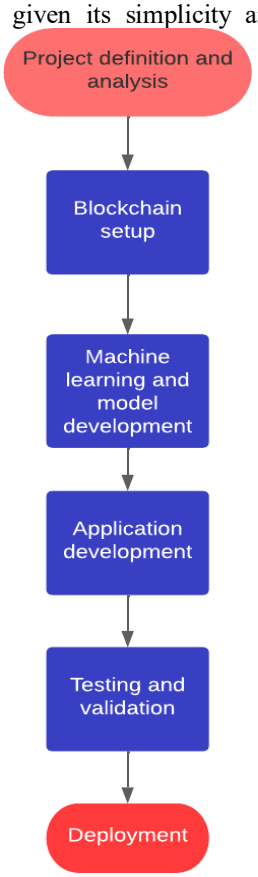

Figure 2 Proposed methodology

A. Project Organization and Analysis

A secure and fair voting mechanism needs to be developed. Utilizing blockchain and machine learning could secure the voting process's correctness and integrity. The affected stakeholders need to be identified. The functional needs - including registration, voting, and result tallying - must be determined. Security standards like anonymity, non-repudiation, and tamper evidence need to be established.

B. Blockchain Setup

An appropriate blockchain platform, such as Ethereum for smart contracts, needs to be selected. The blockchain network structure needs to be created, deciding on whether it should be private or public and the number of nodes. Smart contracts need to be developed for registration and verification of voters, vote casting, and counting votes.

C. Machine Learning Model Development

Anonymous voting data needs to be obtained through simulations to train and evaluate machine learning models. Random Forest should be utilized due to its ability to handle large, multidimensional datasets. It can assign relevance scores to features and manage missing data effectively. K- An intuitive interface needs to be created for voters and election authorities, with secure login and registration functionality. Blockchain technology needs to be leveraged for transaction management and smart contract execution. Machine learning models need to be incorporated to detect anomalies in real-time and assure voting integrity.

D. Application Development

E. Testing and Validation

Testing including unit, integration, and system testing must be conducted. Security audits and vulnerability assessments need to be performed. Machine learning models should be validated on unseen data. Pilot simulations with mock users should be run to validate system functioning and security.

F. Deployment and Monitoring

The application needs to be deployed on secure, scalable infrastructure. System efficiency, privacy violations, and user input need to be monitored closely to ensure continuous improvement.

IV. Result

Analysing performance metrics like precision, recall, accuracy, F1 score, and error rate can provide crucial insights for the developers and stakeholders of the Voting Application. Carefully evaluating these metrics enables a nuanced understanding of how well the random forest and KNN machine learning algorithms are classifying votes as either fraudulent or legitimate.

A. Precision

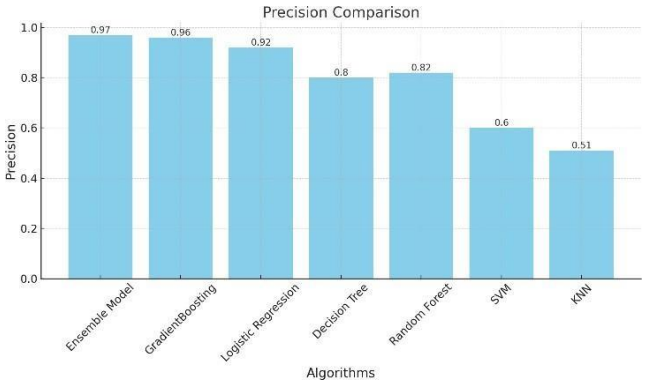

Figure 3 Precision proposed by different algorithms

Precision specifically measures the percentage of votes correctly classified as legitimate out of all votes predicted as valid by the system as shown in figure 1. High precision is critical, as it indicates a low incidence of false positives - votes incorrectly labelled as real when they are actually fraudulent. Maximizing precision minimizes false positives and helps preserve the integrity of the electoral process by preventing invalid votes from being counted.

B. Recall

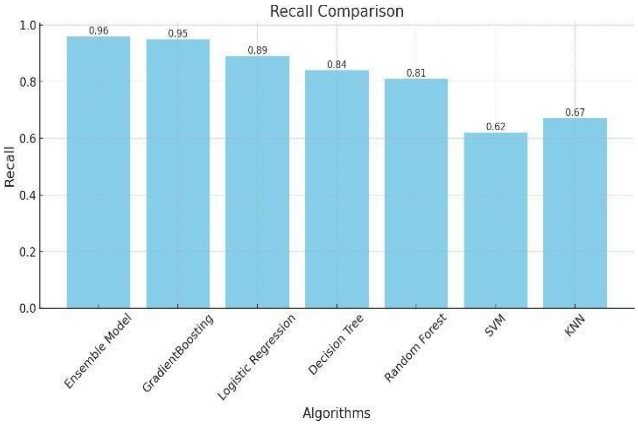

Figure 4 Recall proposed by different algorithms

Recall refers to the percentage of total valid votes correctly identified as such by the algorithms as shown in figure 2. High recall means the algorithms are successfully flagging the vast majority of actual valid votes, rather than mislabeling them as fraudulent (false negatives). Robust recall ensures all legitimate votes are properly tallied and voter intent is accurately captured. It is an important metric for ensuring fairness and representation.

C. Accuracy

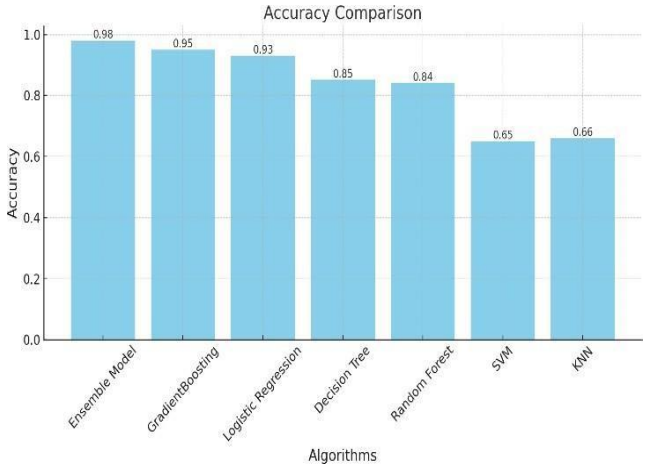

Figure 5 Accuracy proposed by different algorithms

Accuracy reflects overall predictive performance - the percentage of total votes, both legitimate and fraudulent, that are classified correctly. However, accuracy rates can be misleading if fraudulent votes make up a small fraction of total votes as shown in figure 3. In skewed datasets, accuracy may remain high even with poor detection of the rare fraudulent votes.

D. F1score

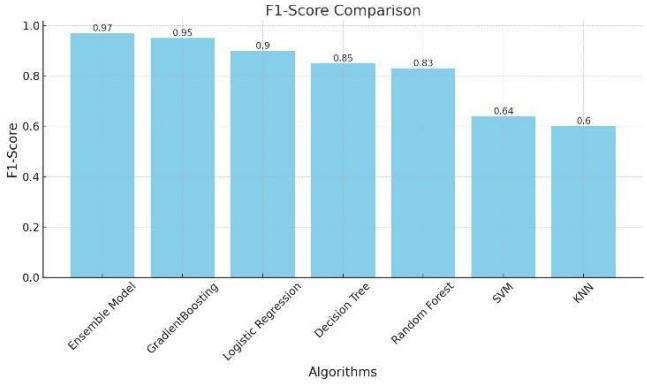

Figure 6 F1-Score proposed by different algorithms

The F1 Score offers a more holistic view by combining precision and recall into one harmonic mean. It balances the ability to correctly identify valid votes while avoiding improper classification of invalid votes. Strong F1 performance indicates the algorithms are reliably distinguishing legitimate and fraudulent votes, minimizing both false positives and false negatives as shown in figure 4.

E. Error rate

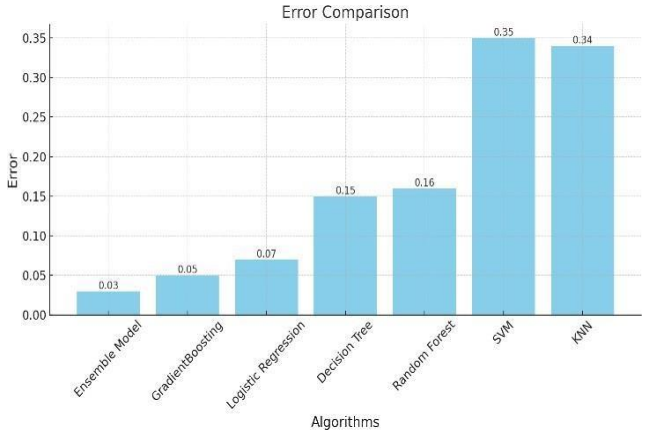

Figure 7 Error proposed by different algorithms

Finally, the overall error rate measures the total percentage of misclassified votes. Lower error signals have greater predictive accuracy and system reliability. Minimizing errors instills confidence that election results reflect true voter intent. The least error is given by hybrid approach as given in figure 7.

V. Conclusion and Future Scope

The development and implementation of a Voting Application utilizing blockchain and machine learning represents significant progress towards secure and transparent electoral processes. This innovative approach demonstrates the potential to address common vulnerabilities in traditional voting infrastructure, including tampering, coercion, and inefficiency. The incorporation of blockchain technology enables encrypted, immutable recording of each vote on a decentralized ledger, conferring unprecedented security and trust in electoral outcomes. Meanwhile, the application of machine learning algorithms enhances real-time identification and prevention of fraudulent activity, further bolstering the reliability of the voting mechanism.

Future iterations could focus on scaling the system to accommodate larger populations and diverse voting scenarios

at state or national levels. Efforts could also be directed towards improving accessibility so that voters with limited technological literacy or disability can readily participate. As machine learning capabilities advance, more sophisticated models may be integrated to strengthen defenses against emerging threats and fraud attempts. Developing interoperability with existing electoral infrastructure could enable smoother adoption by jurisdictions, ensuring continuity and avoiding disruption. Collaborating with international organizations to establish standards and best practices for blockchain-based voting may promote widespread confidence in the security, integrity, and acceptance of these innovations.

REFERENCES

[1] Cheema, Muhammad Asaad, Nouman Ashraf, Asad Aftab, Hassaan Khaliq Qureshi, Muhammad Kazim and Ahmad Taher Azar. "Machine Learning with Blockchain for Secure E-voting System." *2020 First International Conference of Smart Systems and Emerging Technologies (SMARTTECH)* (2020): 177-182.

[2] P M, Abraham and Felix M. Philip. "Electronic Voting System with Blockchain." *YMER Digital* (2022): n. pag.

[3] Arifudin, Akhmad Rizal, Ray Novita Yasa and Girinoto. "Securing Indonesian Hoax News Dataset with Blockchain, IPFS, and Voting Mechanism." *2023 3rd International Conference on Electronic and Electrical Engineering and Intelligent System (ICE3IS)* (2023): 104-109.

[4] H. Prasad, A. Singh, J. Thakur, C. Choudhary and N. Vyas, "Artificial Intelligence Based Fire and Smoke Detection and Security Control System," 2023 International Conference on Network, Multimedia and Information Technology (NMITCON), Bengaluru, India, 2023, pp. 01-06.

[5] H. Garg, M. Singh, V. Sharma and M. Agarwal, "Decentralized Application (DAPP) to enable E-voting system using Blockchain Technology," 2022 Second International Conference on Computer Science, Engineering and Applications (ICCSEA), Gunupur, India, 2022, pp. 1-6.

[6] Anurag, C. Choudhary and N. Vyas, "Exploring the Critical Role of Edge Computing in Enhancing IoT Performance and Security," *2023 International Conference on Communication, Security and Artificial Intelligence (ICCSAI)*, Greater Noida, India, 2023, pp. 563-568.

[7] Ali, Youssef Abdelrahman Fekry, Omar Tarek Mohamed Ahmed, Mohamad Ahmad Mohamad Diab, Mohamed Abd Elhalim Sayed, Mohamed Abd Elaziz and Bassam W. Aboshosha. "Blockchain-Based Online E-voting System." *2023 International Conference on Smart Computing and Application (ICSCA)* (2023): 1-8.

[8] A. Raizada and B. Sharma, "Reliable Block chain-Based Digital System of Voting," 2023 International Conference on Artificial Intelligence and Smart Communication (AISC), Greater Noida, India, 2023, pp. 378-382.

[9] R, Nagesh, Guru Prasad M S, Shivaraj B G, Dhawal Jain, Puneeth B. R and M Anadkumar. "E-Voting System Using Blockchain Technology." *2022 4th International Conference on Advances in Computing, Communication Control and Networking (ICAC3N)* (2022): 2106-2111.

[10] Fezzazi, Asmae El, Amina Adadi and Mohammed Berrada. "Towards a Blockchain based Intelligent and Secure Voting." *2021 Fifth International Conference On Intelligent Computing in Data Sciences (ICDS)* (2021): 1-8

[11] Ardak, Rutuja B. and Dr. Aashish S. Bardekar. "Smart Voting System Using Deep Learning and Computer Vision." *International Journal for Research in Applied Science and Engineering Technology* (2022): n. pag.

[12] C. Choudhary, N. Vyas and U. Kumar Lilhore, "Cloud Security: Challenges and Strategies for Ensuring Data Protection," *2023 3rd International Conference on Technological Advancements in Computational Sciences (ICTACS)*, Tashkent, Uzbekistan, 2023

[13] Mishra, Anubhav A., Anuroop Mishra, Abhyudya Bajpai and Abhinav Mishra. "Implementation of Blockchain for Fair Polling System." *2020 International Conference on Smart Electronics and Communication (ICOSEC)* (2020): 638-644

[14] Toma, Cristian, Marius Popa, Cătălin Emilian Boja, Cristian Ciurea and Mihai Doinea. "Secure and Anonymous Voting D-App with IoT Embedded Device Using Blockchain Technology." *Electronics* (2022): n. pag.

[15] C. Choudhary, N. Vyas and U. K. Lilhore, "An Optimized Sign Language Recognition Using Convolutional Neural Networks (CNNs) and Tensor-Flow," *2023 3rd International Conference on Technological Advancements in Computational Sciences (ICTACS)*, Tashkent, Uzbekistan, 2023, pp. 896-901

[16] Garg, Harshita, Mandeep Singh, Vasvi Sharma and Megha Agarwal. "Decentralized Application (DAPP) to enable E-voting system using Blockchain Technology." *2022 Second International Conference on Computer Science, Engineering and Applications (ICCSEA)* (2022): 1-6.

[17] D. Khoury, E. F. Kfoury, A. Kassem and H. Harb, "Decentralized Voting Platform Based on Ethereum Blockchain," 2018 IEEE International Multidisciplinary Conference on Engineering Technology (IMCET), Beirut, Lebanon, 2018, pp. 1-6.

[18] V. Sliusar, A. Fyodorov, A. Volkov, P. Fyodorov and V. Pascari, "Blockchain Technology Application for Electronic Voting Systems," 2021 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (ElConRus), St. Petersburg, Moscow, Russia, 2021, pp. 2257-2261.

[19] V. V. and V. S., "A Novel P2P based System with Blockchain for Secured Voting Scheme," 2019 Fifth International Conference on Science Technology Engineering and Mathematics (ICONSTEM), Chennai, India, 2019, pp. 153-156.

[20] J. Thakur, C. Choudhary, H. Gobind, V. Abrol and Anurag, "Gliomas Disease Prediction: An Optimized Ensemble Machine Learning-Based Approach," *2023 3rd International Conference on Technological Advancements in Computational Sciences (ICTACS)*, Tashkent, Uzbekistan, 2023, pp. 1307-1311.