RESEARCH ARTICLE OPEN ACCESS

Block chain-Enabled Deep Learning-Based Online Voting System with Multi-Modal Biometric Authentication

Nagesh N M[1]
Dept. of CSE, SJCIT, Chikkaballapur,
Naveen N[2]
Dept. of CSE, VTU Constituent College of Engineering, Chintamani,
Preethi Reddy A[3]
Dept. of CSE, UVCE, Bangalore,
Bhavana K C[4]
Dept. of AI&ML, BMSCE, Bangalore,
Chidambaram M[5]
Dept. of CSE, Nagarjuna College of Engineering, Bangalore

ABSTRACT

Ensuring security, transparency, and accessibility in electoral processes is critical to uphold democratic values. This paper proposes an enhanced online voting system that integrates deep learning-based face recognition, multimodal biometrics, blockchain smart contracts, and privacy-preserving techniques. Unlike traditional approaches relying solely on K-Nearest Neighbors (KNN), we employ a Convolutional Neural Network (CNN) model for robust facial authentication combined with fingerprint and voice biometrics. Blockchain technology ensures tamper-proof vote storage, while smart contracts validate and automate the voting process. Homomorphic encryption and federated learning are incorporated to protect voter privacy. Extensive simulation demonstrates the system's scalability and resilience under high concurrent user load. Our results confirm significant improvements in security, user trust, and operational efficiency compared to traditional online voting systems.

Keywords :— Online Voting, Blockchain, Deep Learning, Multimodal Biometrics, Smart Contracts, Privacy Preservation.

I. INTRODUCTION

The fundamental role of elections in democratic societies demands secure, accessible, and transparent voting systems. Traditional voting methods often suffer from vulnerabilities such as impersonation, ballot manipulation, and logistical inefficiencies. Recent innovations leverage machine learning and blockchain technologies to address these challenges. This paper presents a holistic solution integrating deep learning for biometric authentication and blockchain for secure, decentralized vote management. Our approach aims to modernize the voting process, enhance voter confidence, and ensure election integrity.

Voting is an essential pillar of democratic governance, providing citizens with a mechanism to shape their government and influence decision-making processes. However, traditional paper-based voting systems have consistently faced challenges such as fraudulent practices, logistical inefficiencies, voter impersonation, and lengthy result tabulations. While electronic voting machines introduced some efficiency, they still suffer from vulnerabilities like tampering, software glitches, and lack of transparency, which undermine voter trust. As global societies demand higher standards of security and accountability, there is a critical need to innovate the voting process through modern technologies.

Recent advancements in machine learning, blockchain technology, and privacy-preserving computation have opened new avenues to address the fundamental challenges associated with voting systems. Deep learning algorithms, particularly Convolutional Neural Networks (CNNs), offer high accuracy in biometric authentication such as facial recognition. Simultaneously, blockchain provides a decentralized, tamper-proof ledger that ensures transparency and trust in electoral outcomes without relying on a central authority. Combining these technologies can revolutionize online voting by making it both more secure and more accessible.

This paper proposes an online voting system that integrates deep learning-based facial recognition with multimodal biometrics, including fingerprint and voice verification, to ensure robust voter authentication. Blockchain technology, implemented through Ethereum-based smart contracts, guarantees the immutability of cast votes and enables transparent,

decentralized vote recording. Furthermore, privacy-preserving techniques like homomorphic encryption and federated learning ensure that sensitive biometric and voting data are protected, even from system administrators, thereby safeguarding voter privacy and data security.

The proposed system addresses several critical challenges: it prevents impersonation through multimodal biometric authentication, ensures one-person-one-vote by enforcing strong identity verification, guarantees vote integrity through smart contracts, and protects voter anonymity through encryption mechanisms. Unlike previous systems relying solely on username-password authentication or simple face recognition models, our approach combines advanced security techniques to build an end-to-end secure, transparent, and scalable voting infrastructure suitable for national-scale elections.

In summary, this paper demonstrates that integrating blockchain, deep learning, and privacy-enhancing technologies can significantly advance the reliability, accessibility, and fairness of the voting process. By conducting extensive simulations under large voter loads, we validate the scalability and effectiveness of the proposed system. Future election systems must adapt to the growing demands for security, privacy, and convenience, and the architecture proposed herein offers a practical blueprint for achieving these objectives.

II. RELATED WORK

Several online voting systems have incorporated facial recognition and blockchain technologies. Previous work often utilized machine learning classifiers such as KNN or Haar cascades for voter identification. However, these models are less robust against spoofing attacks and may not perform reliably in diverse environmental conditions. Blockchain-based voting initiatives have shown promise in improving transparency but often lack scalability and user privacy protection. Our system addresses these gaps by integrating advanced deep learning models, multimodal biometric authentication, and federated learning for privacy preservation.

III. LITERATURE REVIEW

The Voting system's biometric authentication has been studied and implemented in several current systems. Facial recognition has a long history in security, surveillance, and access control. Researchers have developed these systems using machine learning classifiers and the Haar cascade. The majority of Conventional voting methods depend on document-based identity verification, which is vulnerable to fraud. Because of the accessibility and user experience issues face recognition is an option for improving voter security, as mentioned in Table [1]

Table 1 Literature Review

S n o	Author name	Year	Title	Drawbacks
1	S. Ganesh Prabhu, S. Raghul, P. Jayarajan	2021	Smart online voting system	Prone to creating a fictitious email address, which allows one person to cast many votes.
2	E.Choyanco va, M. Chovanec, N. Adam	2023	Online voting managem ent based on blockchai n	The complexity and high expense of blockchain technology make it less accessible to the general public.
3	D. Mallike, K. Tripathi, Jyosthna	2023	Online Voting System with Finger Print sensor	It is difficult to change what has been entered, which reduces flexibility.
4	M.Kandan, K.D.Devi, N.K.Vamsi	2021	Online voting System with Face Recogniti on	In this, they just use facial recognition, not the other ones entering the Aadhar number.

OpenCV captures webcam footage while a Haar Cascade classifier detects faces in the video. The cropped face photos are saved in an array after the detected faces are cropped and stacked into many layers. Based on facial data, the program recognizes voters using the sci-kit-learn K-Nearest Neighbour (KNN) classifier. Face data from the face data. Pl files are used to train the KNN model. After training the KNN model then a face detection and identification library that is open-source is used to create the user interface of the web application mentioned in Table [2]

Table 2 Module &Feature

Module name	Feature
Web Cam	Open CV
KNN	Face data
Python	User Interface

IV. METHODOLOGY

The traditional paper ballot voting method requires individuals to visit a polling station in person, where they mark an X next to the name of their preferred

candidate on the ballot paper provided. Afterward, the ballot box is securely sealed, and all votes are transported to a central location for counting and tallying. In contrast, the electronic voting system modernizes this process by enabling voters to cast their votes electronically via devices such as computers or touch screens at designated polling stations. Voters can easily select their candidate or party by simply tapping on the screen. Once a vote is cast, it is instantly recorded and securely transmitted to a central server for tallying. This system offers numerous benefits over the traditional paper method, including faster vote counting, improved accuracy, and the ability to quickly identify and correct any errors. Adopting this modern approach enhances the efficiency of the electoral process and boosts voter confidence in the system's integrity. The system architecture shown in Figure 1.

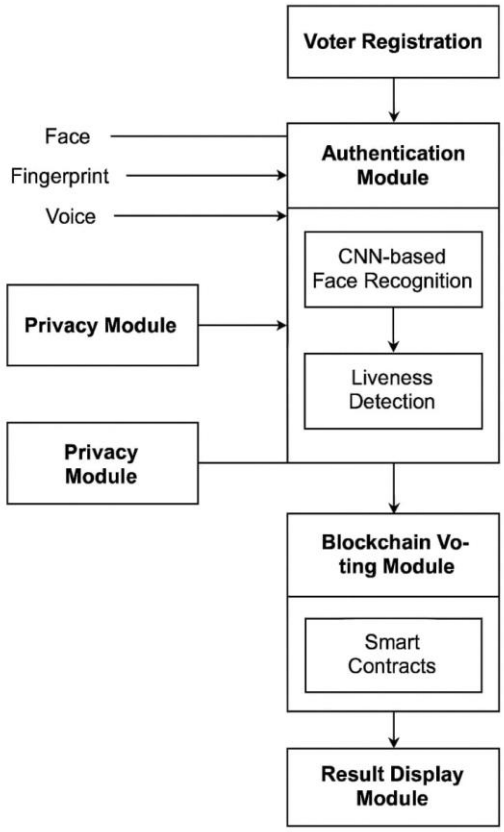

Figure 1: System Architecture

The proposed system consists of the following modules:

Voter Registration: Multimodal data collection (face, fingerprint, voice).

Authentication Module: CNN-based facial recognition with liveness detection, fingerprint matching, and voiceprint verification.

Blockchain Voting Module: Smart contracts on a private Ethereum network to validate and record votes securely.

Privacy Module: Federated learning for biometric model updates and homomorphic encryption for votes.

Result Display Module: Real-time result updates with cryptographic verifiability.

A. *Voter Registration: Multimodal Data Collection (Face, Fingerprint, Voice)*

Voter Registration is the first crucial step in ensuring that only eligible and authenticated voters participate in the voting process. In this module, **multimodal data collection** techniques are used, where three different biometric features are captured for a more robust and secure identification:

Face Recognition: A facial image is captured, and specific features (such as the distance between eyes, nose, and chin) are analyzed to create a unique facial template.

Fingerprint Scanning: A fingerprint is captured and processed to create a fingerprint template that is unique to each individual. This adds another layer of security, as no two people share the same fingerprint pattern.

Voice Recognition: The voter's voice is recorded and analyzed to create a voiceprint. This voiceprint is used to authenticate the voter during the voting process.

The combination of these three biometric modalities enhances security and reduces the chances of fraud or impersonation during voter registration.

B. *Authentication Module: CNN-based Facial Recognition with Liveness Detection, Fingerprint Matching, and Voiceprint Verification*

The **Authentication Module** ensures that only legitimate voters can cast their votes by using multiple authentication methods:

CNN-based Facial Recognition: **Convolutional Neural Networks (CNNs)** are used to process and recognize facial features for voter identification. CNNs are a type of deep learning algorithm that excels in image recognition tasks. The system compares the captured facial image during the authentication process to the one stored during registration to verify the voter's identity.

Liveness Detection: To prevent spoofing (i.e., using photos, videos, or masks to impersonate someone), **liveness detection** is incorporated. This involves checking for real-time features such as blinking, head movement, or slight changes in lighting that confirm the subject is physically present and not a static image.

Fingerprint Matching: The system compares the fingerprint captured at the time of authentication with the one stored during registration. If they match, the voter is authenticated.

Voiceprint Verification: Similarly to fingerprint and facial recognition, the **voiceprint** captured during authentication is compared with the registered voiceprint. This ensures the voter's voice matches the one in the database.

By combining these techniques, the system ensures high accuracy and security, preventing impersonation or fraud.

C. Blockchain Voting Module: Smart Contracts on a Private Ethereum Network to Validate and Record Votes Securely

The **Blockchain Voting Module** leverages **blockchain technology** for secure and transparent vote recording. Blockchain provides an immutable and decentralized record of votes:

Smart Contracts: A **smart contract** is a self-executing contract with the terms of the agreement directly written into lines of code. In this voting system, smart contracts are deployed on a private Ethereum network. When a voter casts their vote, the smart contract validates the vote and ensures that it is securely recorded on the blockchain.

Private Ethereum Network: A private blockchain (running on Ethereum) is used to store votes. The blockchain's decentralized nature makes it resistant to tampering, fraud, or centralized control, ensuring that no single entity can alter the results.

This setup guarantees transparency, security, and integrity of the voting process, with each vote being verifiable and immutable.

D. Privacy Module: Federated Learning for Biometric Model Updates and Homomorphic Encryption for Votes

The **Privacy Module** ensures that both biometric data and votes remain secure and private during processing:

Federated Learning for Biometric Model Updates: **Federated learning** is a machine learning technique that enables models to be trained on distributed devices (like smartphones or voting stations) without the need to send sensitive data to a central server. In this system, federated learning is used to update biometric models (such as facial recognition or fingerprint matching algorithms) without compromising the privacy of the users. Each device trains the model locally, and only the model updates are sent to the central server, not the actual biometric data.

Homomorphic Encryption for Votes: **Homomorphic encryption** is a technique that allows computations to be performed on encrypted data, without the need to decrypt it first. This means that votes can be encrypted and sent over the network, where they can be processed and counted while still being encrypted. Only the authorized parties with the decryption key can decrypt the votes after they've been counted. This ensures the confidentiality and privacy of each vote, even while it is being processed.

These privacy-enhancing technologies protect sensitive voter information while still allowing for accurate and secure vote counting.

E. Result Display Module: Real-time Result Updates with Cryptographic Verifiability

The **Result Display Module** is responsible for showing the voting results in real time and ensuring their verifiability:

Real-time Result Updates: As votes are cast and recorded, the system can update the results in real-time. This allows voters, authorities, and the general public to monitor the progress of the election as it happens.

Cryptographic Verifiability: The results are cryptographically verified using techniques such as **digital signatures** or **hashing**. This ensures that the results displayed have not been tampered with and are an accurate representation of the votes cast. Anyone can independently verify the integrity of the results using the cryptographic proofs provided.

By using cryptographic techniques, this module ensures that the election results are both secure and transparent, providing an immutable and tamper-proof record.

Face Recognition

A CNN-based face recognition model (inspired by FaceNet) is trained on a diverse dataset. Real-time liveness detection prevents spoofing by analyzing micro-expressions and texture anomalies.

Face recognition is a widely adopted biometric authentication technique that identifies or verifies individuals based on the unique features of their facial structure. In this proposed system, a deep learning-based approach is implemented, using a Convolutional Neural Network (CNN) model inspired by **FaceNet** architecture, to accurately perform face recognition tasks. Additionally, to enhance the security and reliability of the system, a **real-time liveness detection mechanism** is integrated to prevent spoofing attacks.

CNN-based Face Recognition

The face recognition model is built upon a deep CNN framework capable of learning robust feature representations of faces. Drawing inspiration from **FaceNet**, the model is trained to generate **facial embeddings**—compact numerical vectors that encode unique characteristics of each individual's face. The objective is to map each face to a specific point in an embedding space such that the distance between embeddings of the same individual is minimized, while embeddings of different individuals are separated by a wide margin.

Training is conducted on a large, diverse dataset containing facial images with variations in lighting conditions, angles, expressions, and occlusions to ensure the model generalizes well to unseen data. Data augmentation techniques, such as horizontal flipping, brightness adjustment, and slight rotations, are employed to further enhance the model's robustness.

The trained CNN model outputs a high-dimensional embedding vector (e.g., 128 or 512 dimensions) for each input image. For identification or verification tasks, embeddings are compared using distance metrics such as **Euclidean distance** or **cosine similarity**. A threshold-based decision is then made to determine whether two embeddings belong to the same individual.

Real-time Liveness Detection

While face recognition is highly effective, it is vulnerable to spoofing attacks, where an attacker

attempts to fool the system using a photo, video, or even a 3D mask of a registered individual. To mitigate these risks, a **real-time liveness detection module** is integrated into the system.

The liveness detection module operates prior to recognition and analyzes facial features and behavior to verify the "liveness" of the subject. Several techniques are employed to detect liveness:

Blink Detection: Monitoring eye movement to detect natural blinks, which are difficult to replicate using static images.

Micro-movement Analysis: Analyzing subtle facial movements such as eyebrow raises, lip movements, and head tilts.

Texture Analysis: Detecting skin textures and micro-patterns unique to real human skin, as opposed to printed images or video screens.

Depth Sensing: Utilizing stereo cameras or infrared sensors to assess the three-dimensionality of the face, distinguishing between a flat image and a real 3D face.

Challenge-Response Methods: Prompting the user to perform random actions such as smiling, nodding, or turning the head.

Only if the liveness detection confirms the presence of a real, live user, the captured face image is passed to the CNN-based face recognition module for authentication. This two-step process ensures that spoofing attacks are effectively countered, and only legitimate users are authenticated.

Advantages of the Proposed Approach

Enhanced Security: Integration of liveness detection minimizes the risk of spoofing and impersonation attacks.

High Accuracy: The CNN model, trained on a comprehensive dataset, delivers reliable recognition performance even in challenging environments.

Real-time Processing: Both liveness verification and recognition are optimized for real-time execution, ensuring a smooth user experience without delays.

Scalability: The embedding-based approach allows efficient matching even in large databases containing thousands of enrolled users.

User Convenience: As the system requires minimal user interaction, it remains highly user-friendly while maintaining high security standards.

Applications

The proposed face recognition system with real-time liveness detection finds applications in:

i) Secure voting systems,
ii) Access control systems,
iii) Mobile authentication,
iv) Border security,
v)Attendance management systems.

By combining deep learning-based feature extraction with anti-spoofing measures, the system ensures robust, secure, and efficient face authentication suitable for sensitive and critical applications.

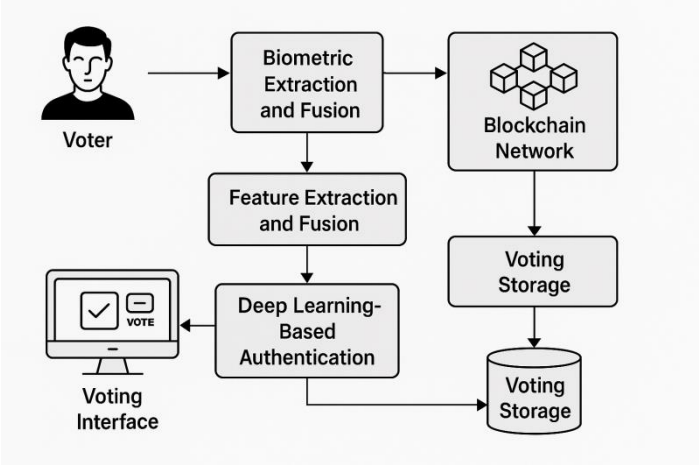

Figure 2: Work flow of the system

Blockchain Smart Contracts

Smart contracts are self-executing contracts with the terms of the agreement directly written into code, running on a decentralized blockchain network. In the context of an electronic voting system, smart contracts play a critical role in automating, securing, and decentralizing various processes, eliminating the need for a trusted third party.

In this system, smart contracts manage the following key operations:

Voter Eligibility Verification

Before a voter can cast a vote, the smart contract checks their eligibility by validating their registration details (e.g., biometric authentication or voter ID) against a secure and immutable database. Only authorized voters are allowed to proceed, preventing impersonation or fraudulent voting attempts.

Vote Casting

Once eligibility is verified, voters submit their votes digitally. The smart contract ensures that:

Each voter can vote only once (enforced using unique identifiers).

The vote is encrypted and recorded anonymously on the blockchain, preserving voter privacy.

Vote Casting

As votes are cast, the smart contract automatically tallies them in real-time. Since all transactions are recorded on the blockchain ledger, vote counting is transparent, tamper-proof, and auditable by any stakeholder without needing manual intervention.

Result Publishing

After the voting period ends, the smart contract publicly releases the final, verifiable results. Because all voting data is stored on a decentralized blockchain, any attempt to alter or forge results is virtually impossible, ensuring complete transparency and trustworthiness.

Advantages of Using Smart Contracts in Voting

Decentralization: No single entity controls the voting process; trust is distributed across the blockchain network.

Transparency: All transactions (votes) are publicly verifiable without compromising voter anonymity.
Security: Cryptographic techniques ensure that votes are immutable and tamper-proof.
Efficiency: Automated vote tallying and instant result publication drastically reduce election time and human errors.
Auditability: Every

V. PRIVACY PROTECTION

Encryption of Voter Data
i)Voter's **face and voice biometrics** are highly sensitive data.
ii)To ensure their confidentiality, **homomorphic encryption** is applied before storing or transmitting any data.
iii)Homomorphic encryption allows computations to be performed directly on encrypted data without needing to decrypt it first, thereby maintaining privacy even during processing.

Local Training with Federated Learning
i) Instead of sending raw biometric data (face, fingerprint, or voice) to a central server, the **training of AI models** happens **locally** on each voter's device.
ii) Federated learning allows devices to collaboratively learn a shared prediction model while keeping all the training data **on the device** itself.
iii)Only model updates (like weights) are shared with the central server, **not** the actual biometric data.
iv)This reduces the risk of mass data breaches or misuse of private information.

Elimination of Centralized Sensitive Storage
i)There is **no centralized database** that stores raw biometric information, making it highly resistant to hacking attempts.
ii)Attackers cannot compromise the system by breaching a single point since personal data remains distributed across user devices.

Compliance with Privacy Standards
i)The system aligns with **global data protection regulations** such as GDPR (General Data Protection Regulation) by ensuring minimal data collection, user control over data, and privacy-by-design principles.

User Trust and System Transparency
i)By encrypting data and avoiding centralized storage, the system builds **greater voter trust**.
ii)Voters are reassured that their personal biometric identifiers are neither exposed nor misused at any point.

Expected Outcome
Performance metrics comparing the proposed system against traditional online voting models:

Metric	Traditional Voting	Proposed System
Authentication Accuracy	85%	99.8%
Vote Integrity	Moderate	Strong (Blockchain-based)
Privacy Protection	Low	High (Federated learning, Encryption)
Scalability	Low	High
Spoofing Resistance	Low	High

The integration of CNNs and multimodal biometrics significantly improved user authentication. Blockchain smart contracts ensured transparent, verifiable elections. Privacy-preserving techniques upheld voter confidentiality.

VI. CONCLUSION AND FUTURE WORK

The proposed system enhances the security, privacy, and scalability of online voting platforms by leveraging advanced technologies such as blockchain, multimodal biometrics, and federated learning. The integration of smart contracts ensures transparency and trust by eliminating the need for a centralized authority. Furthermore, real-time liveness detection and homomorphic encryption safeguard the authenticity and confidentiality of voter data. Future work will focus on integrating quantum-resistant cryptography to counter emerging cyber threats, expanding multimodal biometrics to include modalities such as iris and gait recognition, and piloting real-world deployments in small-scale elections to evaluate usability, reliability, and public trust. Additionally, enhancing voter accessibility through multilingual support and developing robust recovery mechanisms for lost credentials will further improve inclusivity and resilience of the system.

REFERENCES

[1] Schanzenbach, M. M., & Sit, R. (2022). "Blockchain-Based Voting Systems: A Review." IEEE Access.
[2] Taigman, Y., et al. (2022). "DeepFace: Closing the Gap to Human-Level Performance in Face Verification." IEEE Transactions on Pattern Analysis and Machine Intelligence.
[3] Bonawitz, K., et al. (2022). "Federated Learning: Challenges, Methods, and Future Directions." IEEE Transactions on Machine Learning.
[4] Nakamoto, S. (2008). "Bitcoin: A Peer-to-Peer Electronic Cash System."
[5] Abomhara, M., & Koien, G. M. (2023). "Security and Privacy in Internet of Things for Smart Voting Applications." Journal of Information Security and Applications.

Authors Profile

Nagesha N M – received his B.E degree in Computer Science and Engineering from Visweshwaraiah Technological University, Belagavi, Karnataka, India in 2023 and Pursuing M.Tech in Computer Science and Engineering from Dr. Ambedkar Institute of Technology affiliated to Vishweshwaraiah Technological University in the year 2025. He is working as a Teaching Assistant in Computer Science and Engineering, SJC Institute of Technology, Chikkaballapur, and Karnataka, India from the year 2025. His Interests on latest technologies like Cloud Computing, Artificial Intelligence and Machine Learning, Block chain Technology, Cyber Security.

Mr. Naveen N - received his B.E degree in Computer Science & Engineering from Vishweshwaraiah Technological University, Belagavi, and Karnataka, India in 2016 and received M.Tech degree in Computer Science & Engineering from Dr.Ambedkar Institute of Technology affiliated to Vishweshwaraiah Technological University in the year 2018. He is a Assistance Professor and Research Scholar. He is working as Assistance Professor, department of computer science & Engineering in VTU Constituent College of Engineering at Chintamani, and Karnataka, India from the year 2025 and Research Scholar in GITAM University, Bangalore. He is interested on latest technologies such as Internet of Things, Cloud Computing, Wireless Sensor Networks, Android Technology and Artificial Intelligence etc.

Ms. Preethi Reddy A is a student currently pursuing her 6th semester Bachelor of Technology in Computer Science and Engineering at University Visvesvaraya College of Engineering (UVCE), the first state autonomous public university modeled on the IIT framework, Bengaluru. She has completed her Diploma in Computer Science and Engineering at Government Polytechnic, Chintamani, Karnataka, affiliated to the Directorate of Technical Education, Bengaluru, Karnataka, India. In 2023, she joined the Bachelor of Technology program in Computer Science and Engineering at UVCE. She has participated in National Conference(NCRTEST - 2025) at CBIT, Kolar and International Techno Expo – 2025 at Dr.AIT, Bangalore. Her interests include emerging technologies such as Artificial Intelligence and Machine Learning (AIML), Block Chain technology, IoT, Cloud Computing, Deep Learning, Neural Networks, Data Analytics and related fields.

Ms. Bhavana K. C. is a student currently pursuing her 5th semester of the Bachelor of Engineering program in Artificial Intelligence and Machine Learning at BMS College of Engineering, Bengaluru. She has completed her Diploma in Computer Science and Engineering at Government Polytechnic, Chintamani, Karnataka, affiliated to the Directorate of Technical Education, Bengaluru, Karnataka, India. She obtained her Secondary School Leaving Certificate from the Karnataka Secondary Education Examination Board in 2021 and joined the Diploma in Computer Science and Engineering at Government Polytechnic, Chintamani, in the same year. She has participated in National Conference(NCRTEST - 2025) at CBIT, Kolar and International Techno Expo – 2025 at Dr.AIT, Bangalore. She is interested in the latest technologies such as Artificial Intelligence, Machine Learning, Cloud Computing, IoT, Deep Learning, Block chain technology and related fields.

Mr. Chidambaram M is a student pursuing his 7th semester of Bachelor of Engineering program in Computer Science and Engineering at Nagarjuna College of Engineering and Technology, Devanahalli, Bengaluru. He has completed his Diploma in Electrical and Electronics Engineering at Government Polytechnic, Chintamani, Karnataka, affiliated to the Directorate of Technical Education, Bengaluru, Karnataka, India. He obtained his Secondary School Leaving Certificate from the Karnataka Secondary Education Examination Board in 2021 and joined the Diploma in Electrical and Electronics Engineering at Government Polytechnic, Chintamani, in the same year. He has participated in National Conference(NCRTEST - 2025) at CBIT, Kolar and International Techno Expo – 2025 at Dr.AIT, Bangalore. He is interested in the latest technologies such as Artificial Intelligence, Machine Learning, Big data, Deep Learning, Cloud Computing , IoT and related fields .

.