SwiftVerify: A Multi-Modal Smart Attendance System

[1] **Bhukya Veeranna**
CSE(AI&ML)
GCET
Hyderabad, India
20r11a6607@gcet.edu.in

[2] **Madanu Shalini**
CSE(AI&ML)
GCET
Hyderabad, India
20r11a6631@gcet.edu.in

[3] **Peladolu Sai Kiran**
CSE(AI&ML)
GCET
Hyderabad, India
20r11a6643@gcet.edu.in

[4]**V. Madhusudhan Rao**
Professor & Dean school of CS&I
GCET
Hyderabad, India
madhuveldanda.cse@gcet.edu.in

***Abstract* - In response to the growing demand for enhanced attendance systems in educational institutions, this paper proposes a ground breaking Multi-Factor Attendance System. Vulnerabilities in traditional approaches include inaccuracies in human data entry and vulnerability to unauthorised access. Our technology offers a multi-layered authentication procedure by combining voice matching, facial recognition, and barcode scanning technologies to overcome these issues. By doing this, security is improved and human data entry errors are reduced. In addition, our system's centralised database allows for real-time attendance updates, providing relevant information on attendance trends and patterns. We hope to enhance attendance management and make a major technological contribution to the development of educational institutions with this creative approach.**

Keywords- Multi-Factor Attendance System, Educational Institutions, Vulnerabilities, Security, Real-time Attendance Updates, Centralized Database, Attendance Trends, Attendance Management

I. INTRODUCTION

Traditionally, maintaining student involvement and operational efficiency in the context of educational institutions has depended heavily on the regulation of attendance. Historically, manual techniques like paper-based registers or crude electronic systems have been used for attendance tracking. These methods, however, are time-consuming, prone to error, and devoid of the strong security features required to protect confidential attendance information. The demand for more advanced attendance systems has arisen due to the rapid growth of technology. These systems must be able to reliably record attendance, ensure strict authentication, and provide meaningful data for decision-making processes.

To overcome these issues, this study presents a ground breaking Multi-Factor Attendance System. Our solution combines voice matching, facial recognition, and barcode scanning technologies, drawing on the development of attendance management systems and biometric technology improvements. Our system's cornerstone, multi-factor authentication, requires numerous kinds of authentication to ensure thorough user verification. This strategy reduces the drawbacks connected to single-factor authentication techniques while also improving security. By using a range of biometric modalities, our system provides a strong and dependable authentication method, reducing the possibility of identity theft and unwanted access.

By offering a complete and safe solution that expedites procedures and improves data accuracy, our research aims to completely transform attendance management in educational institutions. In addition to providing increased security, our system makes use of cutting-edge technology like voice-recognition and facial identification to deliver insightful data about attendance patterns and trends. With the ability to make decisions and allocate resources more efficiently based on real-time attendance data, educational institutions will be better equipped as a result. Ultimately, our Multi-Factor Attendance System contributes to increased effectiveness, security, and transparency in learning environments by marking a substantial technological development in attendance management systems.

II. RELATED WORK

[1] Despite technological developments, the outdated practice of human attendance logging has continued, leading to errors and inefficiencies. Using speech recognition technology presents a viable way to solve this problem and provide accurate, automatic attendance tracking. Utilising Google's speech recognition module is proposed system, which is incorporated into an easy-to-use Kivy application that runs in a Python environment. This technology guarantees precision and dependability in attendance recording while also doing away with the need for personal intervention. Furthermore, stakeholders in corporate offices and educational institutions can easily access thorough attendance status thanks to the integration of a sophisticated user interface.

Through the implementation of this novel strategy, this successfully address the persistent issue of imprecise attendance recording, opening the door to more efficient and streamlined operations. Approach, which is based on speech - recognition technology, reduces errors and improves accessibility for both staff members and students. Moreover, the accuracy rate of 95% indicated in “Mary Meeker's annual Internet Trends Report highlights” how well answer meets the exacting requirements of attendance tracking.

[2] The manual method of keeping track of student attendance in classes is prone to manipulation and is therefore often unsuccessful. In an attempt to automate the process of tracking attendance, the Automated Attendance System (AUDACE) was created in response to this problem. AUDACE uses face recognition technology to identify pupils in the classroom automatically and in real time. The technology precisely tracks attendance by taking pictures in real time and comparing them to reference faces stored in the dataset.

This eliminates the need for human entry and lowers the possibility of mistakes or record manipulation. A speech conversion system that audibly announces the list of absentees is another feature of AUDACE that offers a dependable confirmation method for attendance tracking.

The inherent problems of manual attendance logging in educational settings are successfully alleviated by using AUDACE. The precise and automatic attendance tracking features of the system address students' propensity for proxy attendance or absenteeism. With the use of speech converter technology and facial recognition, AUDACE guarantees the accuracy and dependability of attendance records while simultaneously improving tracking efficiency. The system's capacity to classify the gender of the pupils present in the class enables more detailed attendance management methods within educational institutions. This capability adds another layer of information to attendance demographics, allowing for a deeper understanding of the composition of the class and potentially influencing various educational strategies and interventions.

[3] Face recognition technology is a valuable biometric solution for security, authentication, and identity in today's digital world. It is applicable to many different industries. Face recognition is more generally applicable due to its non-invasive and contactless nature, even though its accuracy is lower than that of other biometric techniques like iris or fingerprint recognition. The inefficiencies and vulnerability to proxy attendance inherent in manual attendance systems have led to an increased adoption of facial recognition systems for attendance marking in offices, educational institutions, and other settings.

An innovative face-recognition-based class attendance system is suggested as a solution to these problems. Using four main automated processes—database construction, face detection, face recognition, and updating—this system simplifies the process of tracking attendance. Utilising cutting-edge methods like the Local Binary Pattern Histogram algorithm and the Haar-Cascade classifier, the system reliably and efficiently manages attendance by correctly identifying people from live streaming video in the classroom. The adoption of this automated system ultimately provides an easy and transparent method of tracking attendance, which helps to increase responsibility and productivity in organisational and educational contexts.

[4] Many years have passed since the manual attendance systems gave way to biometric-based ones. But current methods frequently have flaws, especially when it comes to overseeing those who work off-site. In this study, a novel attendance system designed specifically to efficiently record off-site employees' attendance. This technology allows the accounting department to easily compute and report salaries, including overtime expenditures, because it integrates seamlessly with the payroll system. Solution provides fingerprint and voice recognition identification using smartphones for verification. Investigation revealed that voice recognition has a false negative rate of 5.88% and fingerprint verification produces a false positive rate of 95%. These results highlight the dependability and usefulness of our suggested attendance method for managing remote workers.

[5] Particularly since the development of image processing methods, facial features have become an important identifier for identification. Conventional attendance practices, such summoning students verbally, take up valuable class time. We suggest an automatic attendance system based on facial detection and identification to overcome this. The system uses a camera-equipped Raspberry Pi module to record the entire classroom, and student databases with names, photos, and roll numbers allow for precise attendance monitoring. This method allows attendance to be taken at any time during class, saving time and providing convenience. Face detection guarantees accurate identification, and recognition effectively logs student attendance. Our technology ensures the best possible use of instructional time by automating this procedure, which simplifies attendance management in educational environments.

Here are some drawbacks in present system:

1. Traditional attendance systems are prone to inaccuracies due to human data entry errors and susceptibility to manipulation, such as proxy attendance.

2. Manual attendance methods are inefficient and time-consuming, leading to wasted instructional time, with attendance recording taking up to 10 minutes per lecture.

3. Existing systems lack robust security measures, making them vulnerable to unauthorized access and compromising the integrity of attendance records.

4. Current systems rely heavily on human intervention for data entry and verification, increasing the likelihood of errors and inefficiencies.

5. Many systems lack real-time updates, making it challenging for administrators to track attendance trends and patterns effectively, hindering decision-making and proactive intervention.

6. Traditional systems often rely on single-factor authentication, such as manual sign-ins or ID card scanning, which may not adequately verify the identity of individuals.

7. Existing systems may operate in silos, making it difficult to integrate attendance data with other administrative or educational platforms, hindering data analysis and decision-making.

8. Some attendance systems struggle to scale effectively, particularly in large organizations or classrooms, leading to inefficiencies and delays in attendance tracking.

9. Maintaining traditional attendance systems, such as manual logbooks or card readers, can be labour-intensive and costly, requiring frequent upkeep and repairs.

III. PROPOSED WORK

In response to the growing demand for enhanced attendance systems in educational institutions, this paper proposes a ground breaking Multi-Factor Attendance System. Vulnerabilities in traditional approaches include inaccuracies in human data entry and vulnerability to unauthorised access. Our technology offers a multi-layered authentication procedure by combining barcode scanning, facial recognition, and voice matching technologies to overcome these issues. By doing this, security is improved and human data entry errors are reduced. Furthermore, the centralised database of our system enables real-time attendance updates, providing insightful information on attendance trends and patterns.

A. *Barcode Scanning*

Barcode scanning is a vital first step in many automated systems, providing quick decoding of barcoded data for activities like identification and inventory control.

Two crucial steps are involved in this process:

1. **Detection:** where the system locates possible barcode candidates in a picture
2. **Decoding:** where the encoded data is taken out of these areas

Measuring precision and reading rate—which indicate the system's capacity to provide accurate results among all returned results and barcodes present, respectively—are two ways to evaluate the accuracy of barcode scanning.

[6] Multiple barcode scanning engines—both open-source and commercial—are thoroughly analysed and contrasted according to reading rate and precision criteria. Zbar and ZXing are two well-known open-source solutions that are compared to other commercial SDKs while evaluating Dynamsoft's barcode SDK. Performance tests are carried out on datasets that include barcode images captured in various settings. Test results include metrics for each engine, including precision, reading rates, misreads, and correctly recognised barcodes.

Figure 1 is the flow diagram of the barcode scanning system with internal processing and evaluation.

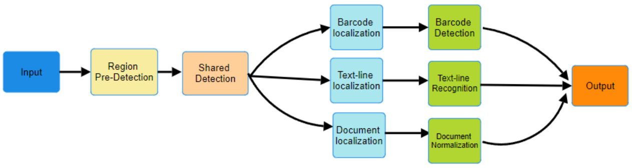


Fig.1 Flow Diagram of Barcode Scanning System

B. *Face Recognition*

Liveness detection technology plays a crucial role in discerning between real and fake faces presented to a system. This involves determining if the face in front of the device is genuine or an imitation, such as a printed photo or a mask. Mainstream liveness solutions encompass coordinated and non-cooperative methods. Coordinated detection prompts users to perform specific actions for verification, while silent detection conducts verification without user involvement.

Fig 2 is the overall architecture of silent face anti spoofing where the model detects whether the provided input is real or fake based on the Fourier transform and Normalization.

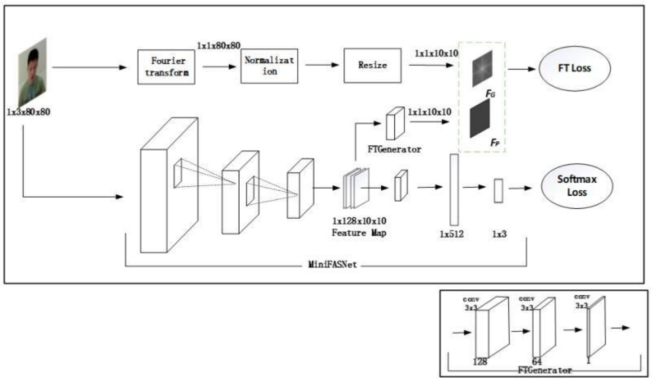


Fig.2 Silent Face Anti Spoofing Architecture

Using supervision aided by Fourier spectrogram, the suggested face recognition model uses a quiet liveness detection technique. Using Fourier spectrograms, this method identifies frequency domain differences between real and fake faces. The model architecture consists of a supervised branch aided by a Fourier spectrogram and a primary branch for classification. To maximise efficiency, the model also includes a self-developed pruning technique. For example, MobileFaceNet's Flops were lowered from 0.224G to 0.081G using this method, improving performance with little loss of accuracy.

The evaluation method involves displaying information such as speed (in milliseconds), confidence level (ranging from 0 to 1), and the outcome of liveness detection (real or fake face). This comprehensive approach ensures efficient and accurate assessment of the face recognition model's performance.

[7] The comparison of facial recognition models demonstrates the efficiency gains made possible by an in-house pruning technique. The computational complexity of MobileFaceNet decreased from 0.224G to 0.081G, while the computational needs of MiniFASNetV1 and MiniFASNetV2 also significantly decreased. These improvements preserve accuracy levels and improve the liveness detection efficiency of the models.

C. Voice Verification

Voice verification, also referred to as voice authentication, relies on distinctive vocal characteristics to identify individuals, offering a seamless and passive authentication approach. Through the analysis of voice features like pitch and tone, it ensures robust security while eliminating user friction. [8] The authentication process involves enrolling voice samples, either through self-service methods or passive collection during interactions with Interactive Voice Response (IVR) systems or call centre agents. Verification is executed through text-dependent or text-independent methods, or via web/mobile applications, where the system assesses confidence scores to validate identity.

Voice verification finds widespread applications in call centres and phone banking, revolutionizing user authentication over the phone and enhancing operational efficiency compared to traditional methods.

Fig.3 outlines the sequential steps involved in voice verification, including sample capture, template creation, and comparison for authentication.

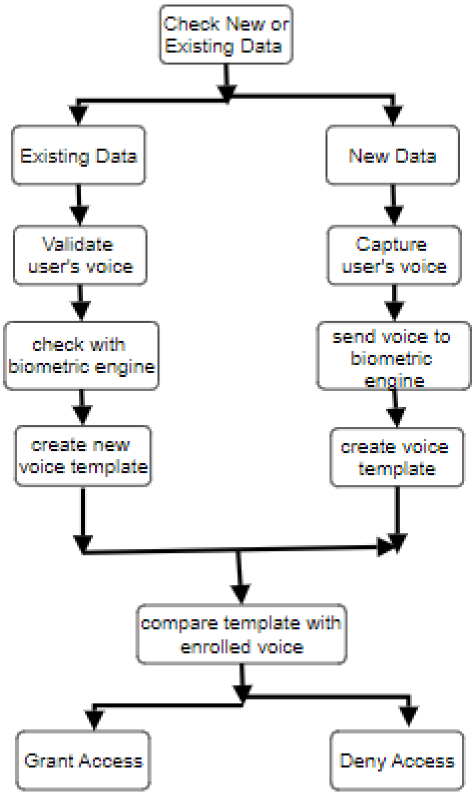

Check New or Existing Data
Existing Data
New Data
Validate user's voice
Capture user's voice
check with biometric engine
send voice to biometric engine
create new voice template
create voice template
compare template with enrolled voice
Grant Access
Deny Access

Fig.3 Flow Diagram of Voice Verification

[9]-[11] Voice verification technology employs advanced algorithms, including biometric voice recognition and liveness detection, to analyse vocal characteristics for authentication. These algorithms leverage machine learning and signal processing techniques to create unique voiceprints and ensure data security. Integration with IVR systems and mobile/web applications enhances user experience and operational efficiency. Through these technologies, voice verification provides reliable authentication while meeting stringent security requirements.

D. Central Database

The centralised database that houses all of the attendance-related data is the fundamental component of the Multi-Factor Attendance System. Time stamps for attendance entries, user identifying data, and extra metadata related to every attendance record are all stored in this database. The solution guarantees accuracy and consistency in tracking attendance across several locations and user interactions by centralising the data. Additionally, real-time attendance updates are facilitated by the central database, which also provides insightful information about attendance patterns and trends. The information contained in the central database can be utilised by educational institutions to improve overall operational efficiency and optimise attendance management tactics by employing advanced data analysis techniques.

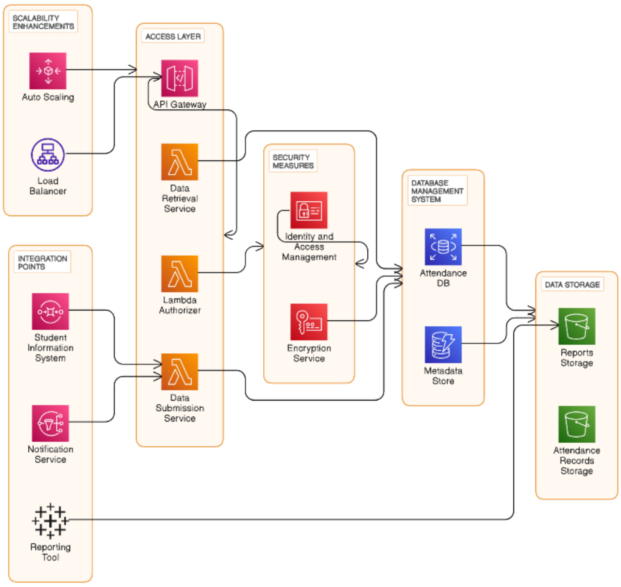


Fig.4 Central Database Architecture for Multi-Factor Attendance System

The central database in the Multi-Factor Attendance System serves as the backbone for storing, managing, and retrieving attendance-related data. It operates by utilizing a Database Management System (DBMS) to organize attendance records into structured tables within the database. These tables typically include user information, attendance logs, timestamps, and metadata.

Data access layers facilitate interactions with the central database, handling tasks such as querying, inserting, updating, and ensuring data integrity. Robust security measures, such as role-based access control and encryption, safeguard the database against unauthorized access and ensure data integrity.

Managed by database administrators, the central database undergoes regular maintenance, including backups, optimization, and monitoring for performance and security. It integrates with other system components, such as user interfaces and reporting tools, enabling seamless data exchange and real-time updates.

E. System Architecture & Process

The system architecture of our Multi-Factor Attendance System is a sophisticated framework integrating facial recognition, voice matching, and barcode scanning technologies. It revolves around a robust central database managed by DBMS, ensuring efficient storage and retrieval of attendance data. Security measures such as role-based access control and encryption protect data integrity, while scalability enhancements ensure responsiveness under varying workloads. Integration points with other system components enable seamless data exchange, supporting real-time updates and analysis. This architecture represents a forward-thinking solution to enhance attendance management in educational institutions.

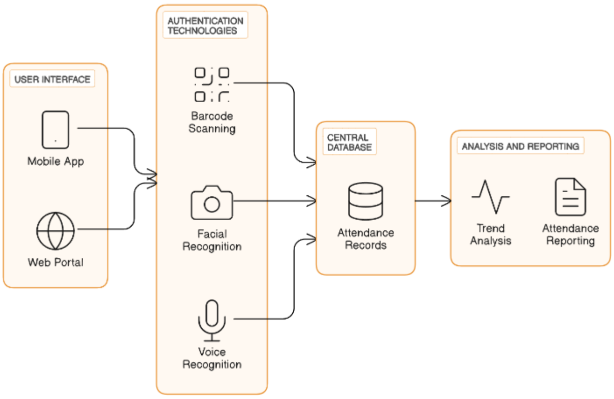


Fig.5 System Architecture

The process diagram outlines the workflow of the Multi-Factor Attendance System, illustrating steps from user interaction to data processing and storage. It delineates actions such as capturing input data, processing it through biometric engines, and making decisions based on user status. The diagram distinguishes between existing and new users, guiding them through authentication or registration processes accordingly. Emphasizing key decision points and system interactions, it provides a concise overview of the system's functionality.

Multi-factor authentication (MFA) is a pivotal security measure that bolsters access control by necessitating users to provide multiple forms of identification. MFA typically incorporates a combination of factors: knowledge (such as passwords or PINs), possession (like smartphones or tokens), inherence (biometric data like fingerprints or facial recognition). By requiring verification across multiple factors, MFA significantly heightens security, even in the event of a compromised factor.

IV. RESULTS AND DISCUSSIONS

The results and discussion section provides an in-depth analysis and interpretation of the findings obtained from the study. This section synthesizes the outcomes of research and engages in a critical examination of their implications, significance, and potential applications.

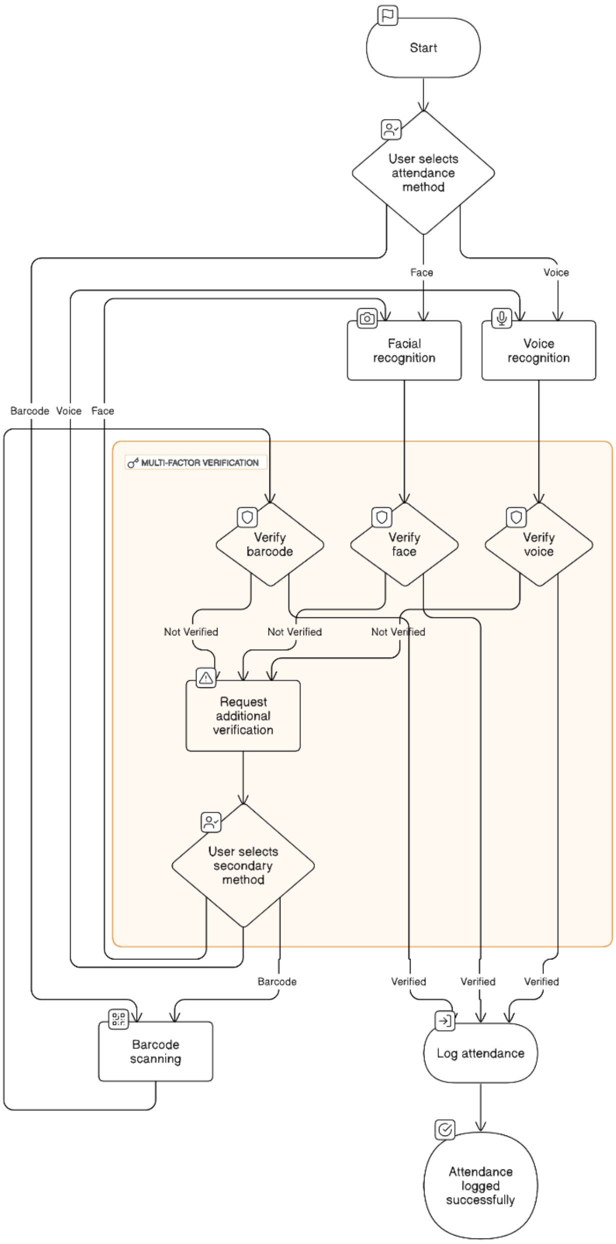
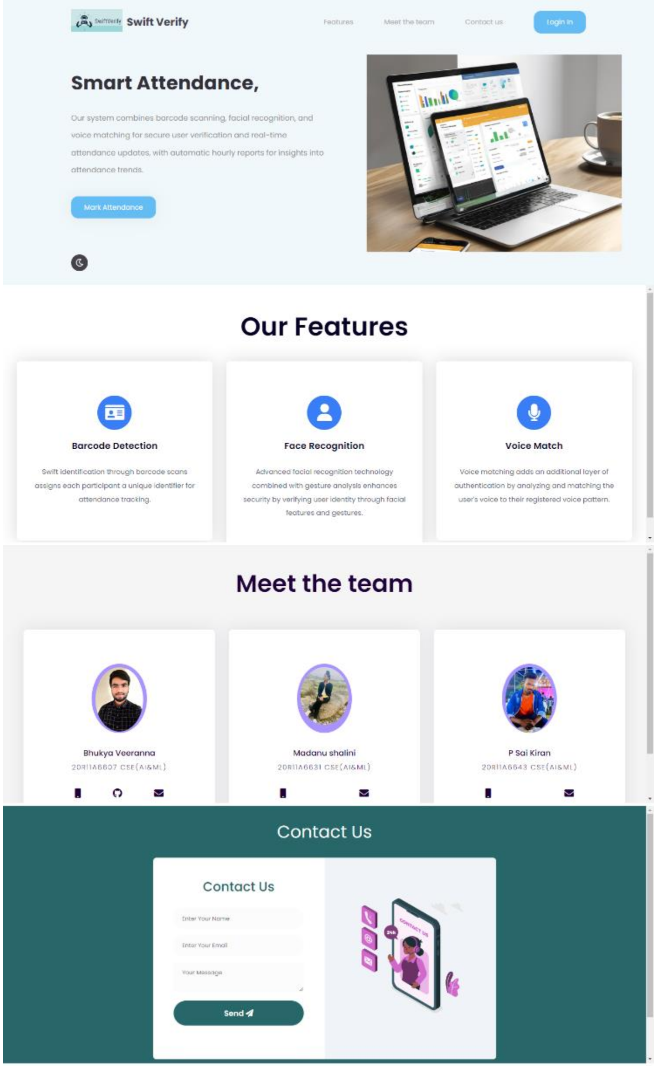


Fig.6 System Model

A. User Interface

The user interface (UI) features a homepage with project details and a contact form for inquiries. Faculty members access a dashboard to view attendance records and utilize biometric authentication methods for marking attendance.

Ease, clarity, and productivity are highlighted in a user-friendly user interface. Clear navigation menus, instantly recognisable buttons and icons, an intuitive layout and style, adaptable and adaptive device display, succinct and informative error messages, contextual assistance choices, and customisable preferences are just a few of its characteristics.


Swift Verify

Smart Attendance,

Our system combines barcode scanning, facial recognition, and voice matching for secure user verification and real-time attendance updates, with automatic hourly reports for insights into attendance trends.

Our Features

Barcode Detection

Swift identification through barcode scans assigns each participant a unique identifier for attendance tracking.

Face Recognition

Advanced facial recognition technology combined with gesture analysis enhances security by verifying user identity through facial features and gestures.

Voice Match

Voice matching adds an additional layer of authentication by analyzing and matching the user's voice to their registered voice pattern.

Meet the team

Bhukya Veeranna
20R11A6607 CSE(AI&ML)

Madanu shalini
20R11A6631 CSE(AI&ML)

P Sai Kiran
20R11A6643 CSE(AI&ML)

Contact Us

Contact Us

Fig.7 Home Page

B. *Barcode Results*

The evaluation's findings show that the Dynamsoft Barcode Reader outperformed competing barcode scanning engines, achieving an impressive reading rate of 96.5%. Its superior capacity to identify and recognise different barcode types makes it a very good choice for attendance systems, even though it may take a little longer to process data.

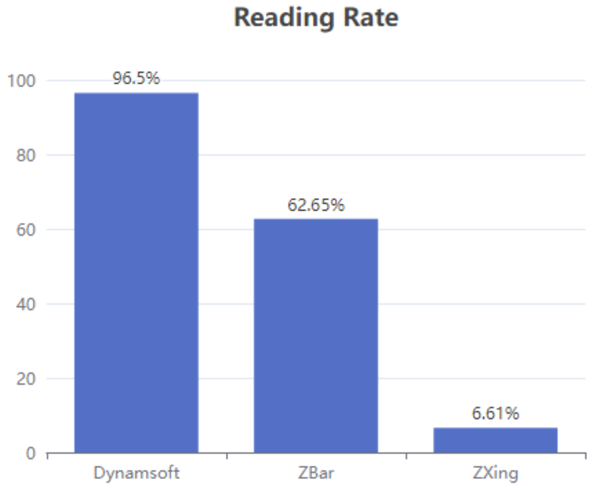


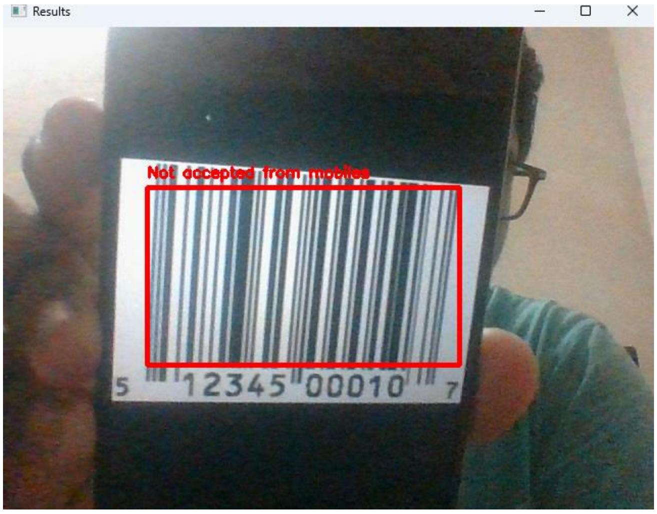
Fig.8 Reading results of barcode scanning

Evaluation Metrics

$$\text{Reading rate: } \frac{\text{correctly detected barcodes}}{\text{Total barcodes}}$$

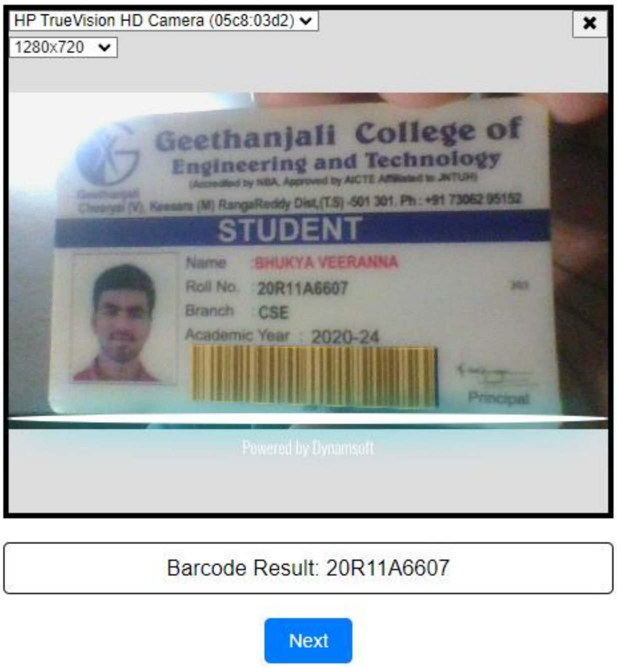
$$\text{Average time: } \frac{\text{Total time elapsed}}{\text{Total files}}$$

Distinguishing between real and fake barcodes to enhance security. By analysing various factors such as movement, texture, and depth, liveness detection technology ensures that only authentic barcodes are recognized, thereby mitigating the risk of fraudulent activities. This feature adds an additional layer of verification, safeguarding the integrity of attendance records and enhancing the overall reliability of the system.


Results

Not accepted from mobiles

Fig.9 Barcode Scan Rejected from mobile screen


HP TrueVision HD Camera (05c8:03d2)

1280x720

Barcode Result: 20R11A6607

Fig. 10 Barcode accepted

C. *Face Recognition Results*

The face recognition system employs different models to detect and classify faces as real or fake. The models utilized include MobileFaceNet, MiniFASNetV1, and MiniFASNetV2. Each model is assessed based on its computational efficiency and parameter size, crucial factors for real-time face recognition tasks.

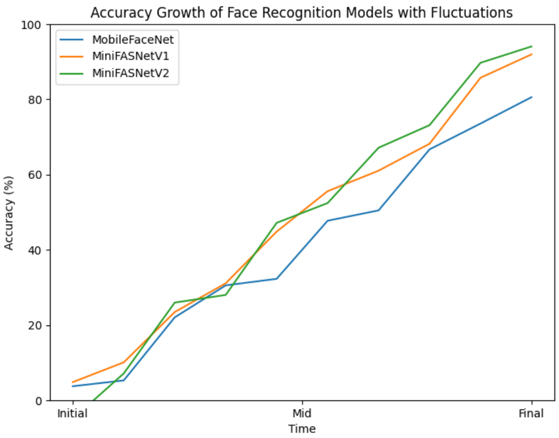


Fig.11 Accuracy of models used

These sample frames demonstrate the effectiveness of a silent face spoofing technique in distinguishing between real and fake faces. This capability enhances security in authentication systems by accurately identifying genuine facial appearances from fraudulent ones.

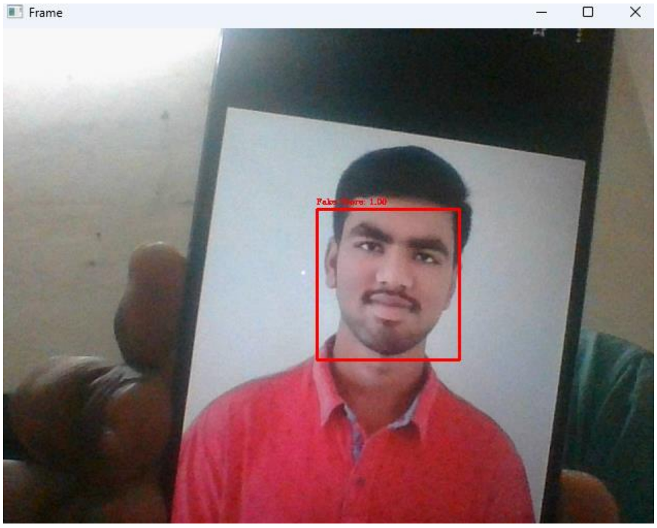


Fig.12 Fake face detection

Real face detection, combined with face grading, uses advanced technology to distinguish between genuine and fraudulent faces based on various facial features. This enhances security by ensuring that only authentic users are identified and granted access.

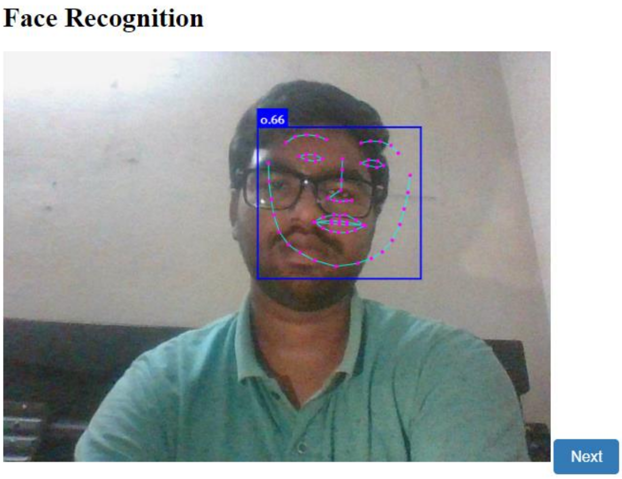
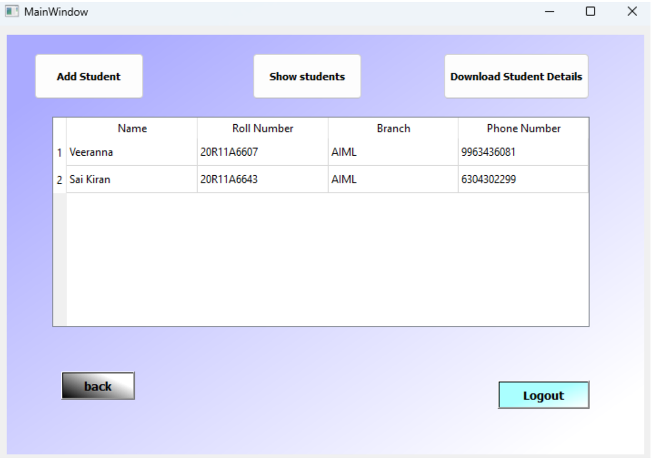


Fig.13 Real Face Detection

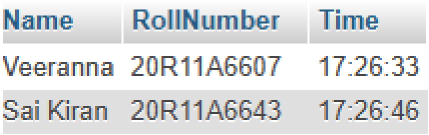
To enhance security and streamline attendance tracking, student data is securely stored in a centralized database. This database employs robust encryption protocols and access control measures to safeguard sensitive information. Additionally, it facilitates real-time updates and comprehensive reporting, ensuring accurate attendance records.



	Name	Roll Number	Branch	Phone Number
1	Veeranna	20R11A6607	AIML	9963436081
2	Sai Kiran	20R11A6643	AIML	6304302299

Fig.14 Display of Student data

The use of a secured database ensures data integrity and confidentiality, promoting trust and compliance with privacy regulations. Moreover, it enables efficient management of attendance data, contributing to the overall effectiveness of educational institutions.



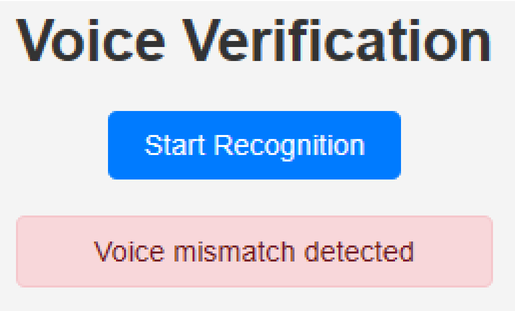
Name	RollNumber	Time
Veeranna	20R11A6607	17:26:33
Sai Kiran	20R11A6643	17:26:46

Fig. 15 Sample Attendance result

D. *Voice Verification Results*

Voice verification is a biometric authentication method that utilizes unique vocal characteristics to verify an individual's identity. It involves analysing various voice features such as pitch, tone, and pronunciation to determine authenticity. This process offers a seamless and passive form of authentication, eliminating the need for traditional methods like passwords or PINs.

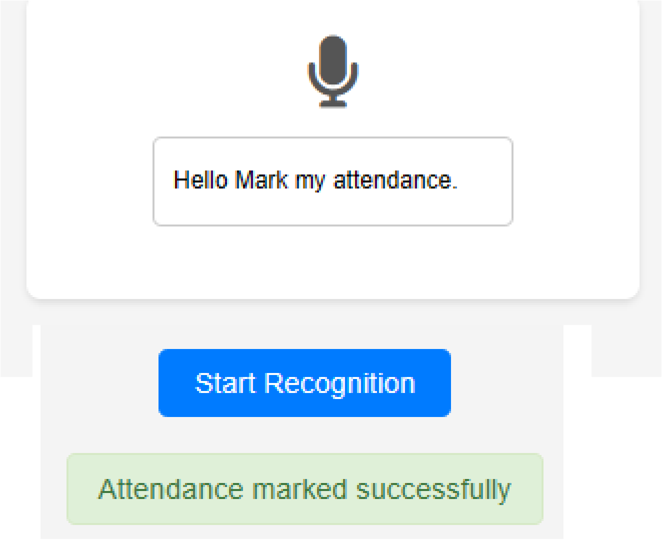
The following are the experimental results for Voice verification.



Voice Verification

Voice mismatch detected

Fig.16 Voice Mismatch



Hello Mark my attendance.

Attendance marked successfully

Fig.17 Voice matched and attendance marked successfully

V. CONCLUSION

The proposed Multi-Factor Attendance System represents a significant advancement in attendance management for educational institutions. By integrating voice matching, facial recognition, and barcode scanning technologies, the system addresses vulnerabilities present in traditional approaches, such as inaccuracies in data entry and susceptibility to unauthorized access. The multi-layered authentication procedure enhances security while reducing human data entry errors, resulting in more reliable attendance records. Additionally, real-time updates provided by the centralized database offer valuable insights into attendance trends and patterns, empowering administrators to make informed decisions. Overall, this innovative approach has the potential to greatly improve attendance management and contribute to the technological advancement of educational institutions.

VI. FUTURE SCOPE

The future scope of the Multi-Factor Attendance System includes leveraging biometric technologies like voice matching, facial recognition, and barcode scanning for accuracy. Integration with IoT devices allows seamless data collection and real-time updates. Machine learning algorithms can predict attendance trends for better resource allocation. Mobile apps enhance remote access, while ensuring data security and privacy remains a priority.

ACKNOWLEDGMENT

We express our gratitude to the Department of Computer Science and Engineering (AI&ML), GCET for their unwavering support throughout the execution of this project.

REFERENCES

[1] Prerak Moolchandani, Shreya Hegde, Muskan Hassanandani, Garv Jhangiani, Gresha Bhatia, Abha Tewari, Shashikant Dugad, "Pehchaan: A Touchless Attendance System", 2023 International Conference on Artificial Intelligence and Applications (ICAIA) Alliance Technology Conference (ATCON-1), pp.1-5, 2023.

[2] Ss, Poornima & Sripriya, N & Vijayalakshmi, B & Vishnupriya, P. (2017). Attendance monitoring system using facial recognition with audio output and gender classification. 1-5. 10.1109/ICCCSP.2017.7944103.

[3] Smitha, & Hegde, Pavithra & Afshin,. (2020). Face Recognition based Attendance Management System. International Journal of Engineering Research and. V9. 10.17577/IJERTV9IS050861.

[4] Soewito, Benfano & Lumban Gaol, Ford & Simanjuntak, Echo & Gunawan, Fergyanto. (2016). Smart mobile attendance system using voice recognition and fingerprint on smartphone. 175-180. 10.1109/ISITIA.2016.7828654.

[5] Ajinkya Patil, Mrudang Shukla(2014) “Implementation of classroom attendance system based on face recognition in class”, International Journal of Advances in Engineering & Technology, Vol. 7 Issue 3, pp976-978.

[6] https://www.dynamsoft.com/codepool/barcode-scanning-accuracy-benchmark-and-comparison.html

[7] https://paperswithcode.com/task/face-anti-spoofing

[8] https://www.pingidentity.com/en/resources/blog/post/introducing-voice-verification.html

[9] https://www.idrnd.ai/voice-biometrics

[10] https://speechprocessingbook.aalto.fi/Recognition/Speaker_Recognition_and_Verification.html

[11] https://domino.ai/blog/building-a-speaker-recognition-model