International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 10 | Oct - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

# Dual-ID Attendance System

Shivam Singh, Adarsh Kumar Maurya, Ankit Chaursiya, Haraprit Kumar, Sachin Saroj

**Abstract — Accurate and secure attendance tracking is essential in educational environments to monitor student engagement and academic accountability. Traditional attendance systems often rely on single-factor authentication, such as manual entry or basic ID scanning, which leaves room for security breaches and inaccuracies. This research introduces a dual-layered authentication system that integrates Radio Frequency Identification (RFID) with fingerprint biometric verification to enhance security, ensure accurate identification, and streamline the attendance process.**

**The proposed system is built using Arduino-based hardware and custom-developed software, enabling real-time data processing and logging. A group of ten students participated in the experimental evaluation, each assigned a unique RFID tag and fingerprint record. Performance tests revealed an average processing time of 20.61 seconds per individual, with a 0% false rejection rate, demonstrating high reliability and precision.**

**The integration of biometric and RFID technologies not only strengthens authentication but also reduces the complexity often associated with multi-factor systems. The coordinated hardware-software design significantly improves operational speed and data integrity. Overall, the results affirm that the system is a robust, efficient, and scalable solution for modern attendance management in academic institutions.**

**Index Terms — Attendance System, RFID, Fingerprint Authentication, Arduino, Biometric Security, Educational Technology, Artificial Intelligence.**

## 1. Introduction

Attendance refers to the act of being present, the frequency at which a person is present, or the number of individuals recorded as present at a given time [1]. In modern times, various attendance monitoring systems have been developed and deployed across different sectors. These systems play a vital role in managing and recording the presence of individuals—whether it be employees during work hours, students attending lectures, or participants at an event.

Effective attendance tracking is essential for accurate record-keeping within institutions and organizations. As a result, researchers and developers have explored automated solutions to replace traditional, manual attendance methods [2]. Among the technologies being increasingly adopted are **fingerprint biometrics** and **Radio Frequency Identification (RFID)**. The integration of these two technologies significantly enhances the **accuracy**, **reliability**, and **security** of attendance records [3].

The fingerprint-RFID-based attendance system accelerates the process of marking attendance, minimizes errors, and removes the need for manual selection or roll-calling. It allows seamless operation with minimal human intervention and simplifiese verification process. This dual-authentication method has found widespread application in sectors such as **corporate enterprises**, **educational institutions** (including universities, secondary, and primary schools), and **industrial operations** where high volumes of personnel need to be monitored efficiently.

In such a system, participants can be authenticated and recorded within a fraction of a second. Moreover, the system aids in the generation of attendance reports, eligibility evaluations, and real-time monitoring of individuals' activities. RFID technology, in particular, enables quick identification and tracking, reducing the likelihood of asset misplacement or unauthorized access. On the other hand, fingerprint recognition enhances personal identification accuracy and adds a higher level of security.

The proposed **Dual-ID Attendance System** is designed to offer a safer, more convenient, and faster method of user authentication compared to traditional password-based or token-based systems. It not only strengthens data integrity but also support smarter and more efficient attendance management practices for modern institutions.

## 2. LITERATURE REVIEW

The evolution of attendance management systems has been driven by the growing demand for automation, security, and accuracy in both academic and corporate institutions. Traditional manual attendance systems that rely on paper registers or verbal confirmation are often inefficient, time-consuming, and highly prone to manipulation. Problems such as proxy attendance, inaccurate record-keeping, and loss of data have motivated researchers to develop automated identification systems that can provide both reliability and convenience. In recent years, Radio Frequency Identification (RFID) and biometric technologies have emerged as two of the most promising approaches to overcome these limitations. While RFID ensures quick and contactless identification, biometric technologies such as fingerprint recognition add a layer of security by linking attendance data directly to the physiological characteristics of an individual. However, each of these technologies also has limitations when used independently, which has inspired the design of hybrid or dual-ID systems that combine both RFID and fingerprint authentication.

Badmus et al. (2021) proposed a smart attendance management system that integrated RFID and fingerprint verification to achieve two-factor authentication. Their system was able to record attendance with higher accuracy compared to single-method systems, as it prevented unauthorized users from marking attendance using someone else's card. The results of their study showed zero proxy cases and minimal false rejection rates. However, the system required an average of over 20 seconds for each authentication, which may not be suitable for large classrooms or organizations with hundreds of users. This latency issue highlights the trade-off between system security and processing speed that many biometric-based attendance systems encounter.

Oloniyo et al. (2022) developed a multimodal attendance system that combined RFID, fingerprint, face recognition, and GSM notification modules. The inclusion of GSM ensured real-time communication between the attendance device and the central database, allowing instant notifications to administrators or students. While this design demonstrated high accuracy and multi-layer security, its implementation was expensive and complex. The use of multiple sensors increased maintenance costs and made the system vulnerable to delays due to sequential verification steps. Moreover, the dependence on stable network connectivity for GSM-based notification limited its application in areas with poor signal coverage.

Another notable work by Hussin et al. (2022) introduced a double identification system that utilized RFID cards along with infrared motion sensors to ensure the actual presence of a person after RFID verification. Although this system effectively reduced the chances of proxy attendance, it lacked the capability to verify individual identity beyond card possession. The motion sensors could easily be triggered by another person walking by, which made the system less reliable in crowded environments. The researchers themselves acknowledged that integrating a biometric component such as fingerprint or facial recognition would significantly enhance its accuracy.

Several other studies have examined RFID-based systems as standalone solutions. Ishaq and Bibi (2023) conducted a systematic review of IoT-integrated RFID attendance systems and concluded that such systems greatly improve data management and remote monitoring capabilities. RFID-based attendance systems are easy to implement, require minimal human intervention, and can record attendance rapidly. However, their main disadvantage lies in the absence of robust identity verification—since RFID cards can be misplaced, duplicated, or shared, they cannot guarantee that the person presenting the card is its rightful owner. Security loopholes like these reduce their reliability, especially in institutions that demand strict accountability.

On the other hand, purely biometric systems have also been widely researched. Arunkumar et al. (2018) proposed a fingerprint-based student attendance system that transmitted attendance data through GSM to a centralized server. The system successfully ensured that only registered fingerprints could mark attendance, eliminating the problem of proxy marking. Nevertheless, fingerprint sensors can encounter difficulties when users have dirty, wet, or damaged fingers. Environmental conditions such as dust, humidity, or lighting can further degrade sensor accuracy, leading to false rejections or slow recognition. Moreover, fingerprint-only systems offer no backup mechanism if the sensor fails or the user's fingerprint cannot be read, reducing overall system reliability.

A comparative analysis of the aforementioned systems reveals several consistent trends and limitations. RFID systems excel in terms of speed and user convenience but are vulnerable to misuse, while biometric systems are secure but slower and more resource-intensive.

Many hybrid or multimodal systems proposed in previous studies aim to combine these technologies, but they often struggle to maintain an optimal balance between authentication time, hardware cost, and operational simplicity. Additionally, most previous studies have been tested in small, controlled environments, typically involving fewer than 50 participants. These limited-scale trials make it difficult to evaluate system performance in real-world institutional settings where hundreds of users may need to record attendance within a short time frame. Another key limitation identified in earlier research is the lack of consideration for data privacy and security of stored biometric information. Many systems fail to implement encryption or secure data transfer protocols, exposing them to potential data breaches and misuse.

To address these limitations, a dual-ID attendance system that integrates RFID and fingerprint authentication offers a balanced and practical solution. In such a system, the RFID card serves as the first layer of identification, enabling rapid recognition of the individual, while the fingerprint scan acts as a second layer of authentication to confirm the person's identity. This combination ensures that even if an RFID card is lost or shared, attendance cannot be falsified without the matching biometric verification. Furthermore, with advancements in embedded microcontrollers and efficient fingerprint algorithms, the response time can be significantly reduced, achieving both speed and security simultaneously. By employing an optimized verification sequence—where RFID scanning initiates fingerprint verification automatically—the system can minimize human interaction and reduce latency.

Additionally, the proposed dual-ID approach enhances accountability by creating tamper-proof attendance logs that link each record to both the RFID tag ID and the unique fingerprint template. Integrating cloud or IoT technologies can allow real-time data monitoring, analysis, and reporting, thereby supporting administrative decision-making and performance tracking. Encryption protocols and secure storage mechanisms can ensure the protection of sensitive biometric data, addressing privacy concerns that were often overlooked in earlier designs. Moreover, the modular architecture of such a system allows easy maintenance and scalability, enabling future integration with additional technologies such as facial recognition, QR-based authentication, or mobile verification.

In summary, existing literature clearly demonstrates that while single-mode attendance systems based on RFID or biometrics have made considerable progress, they continue to face challenges related to either security or efficiency. The combination of RFID and fingerprint verification represents a promising evolution in attendance automation, offering both convenience and authenticity. By learning from the limitations and findings of previous research, a dual-ID system can bridge the gap between speed and accuracy, ensuring reliable attendance tracking even in large-scale and dynamic environments. Thus, the development of such a hybrid model not only contributes to technological advancement in attendance management but also provides a secure, cost-effective, and scalable solution suitable for modern academic and organizational needs.

## 3. METHODOLOGY

The proposed Dual-ID Attendance System integrates both software and hardware components, forming a complete embedded system designed to ensure accurate, secure, and automated attendance management. The system employs an Arduino Uno microcontroller as its central processing unit, interfaced with an RFID reader, fingerprint sensor, 16x2 LCD display, RTC (Real-Time Clock) module, SD card module, buzzer, and a 12V regulated power supply. The software, developed using the Arduino IDE, manages the overall logic flow, handles data verification, and records attendance after successful dual authentication. This integration guarantees that attendance marking is both efficient and tamper-proof.

Figure 1 illustrates the block diagram of the proposed system, highlighting the interconnections between major components. The RFID reader and fingerprint sensor act as input devices that capture the user's credentials. These inputs are sent to the Arduino Uno for processing and validation. Upon successful verification, the system records attendance data in the SD card, along with a timestamp obtained from the RTC module. The LCD display and buzzer act as output units, providing visual and audio feedback to users. The power supply delivers regulated 5V to the entire circuit from a 12V adapter, ensuring smooth and reliable operation. The dual-layer authentication principle ensures that attendance is marked only when both the RFID tag and fingerprint data match the registered records.

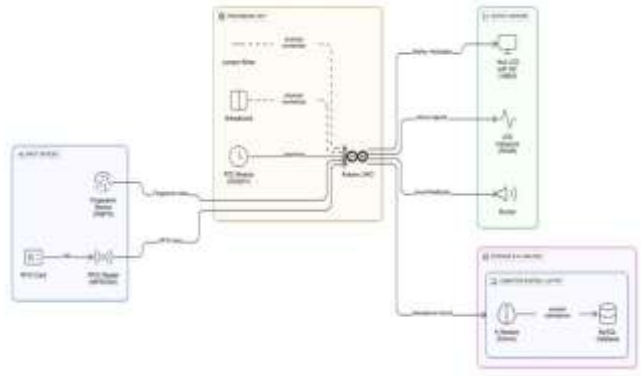

Fig. 1. Block Diagram of the Dual-ID Attendance System using RFID and Fingerprint.

Figure 2 shows the detailed circuit diagram of the system, demonstrating the hardware connections and communication among various components. The RFID module is interfaced with the Arduino Uno using the SPI communication protocol, where pins 10, 11, 12, and 13 correspond to SS, MOSI, MISO, and SCK, respectively. The fingerprint sensor is connected via UART communication through the TX and RX pins of the Arduino Uno. The RTC (DS3231) module uses the I2C protocol, connected through analog pins A4 (SDA) and A5 (SCL). The 16x2 LCD operates in 4-bit mode with control pins RS, RW, and E connected to digital pins 7, 6, and 5, while data pins D4–D7 are connected to pins 4, 3, 2, and 1, respectively. The SD card module shares the SPI interface with the RFID reader but uses a different chip select pin to avoid data conflict. A buzzer and an LED indicator are connected to digital pins 8 and 9 for alert and system status signaling. The circuit is powered by a 12V DC adapter regulated to 5V using a 7805 voltage regulator to supply the microcontroller and connected modules.

The methodology followed in this project was structured and systematic, consisting of several key phases—requirement analysis, hardware selection, software programming, integration, and testing. Initially, relevant data about attendance systems, embedded controllers, and biometric authentication methods was collected to establish the project's foundation. Based on the analysis, appropriate hardware and software tools were chosen, with Arduino Uno selected for its simplicity, reliability, and sufficient I/O capabilities.

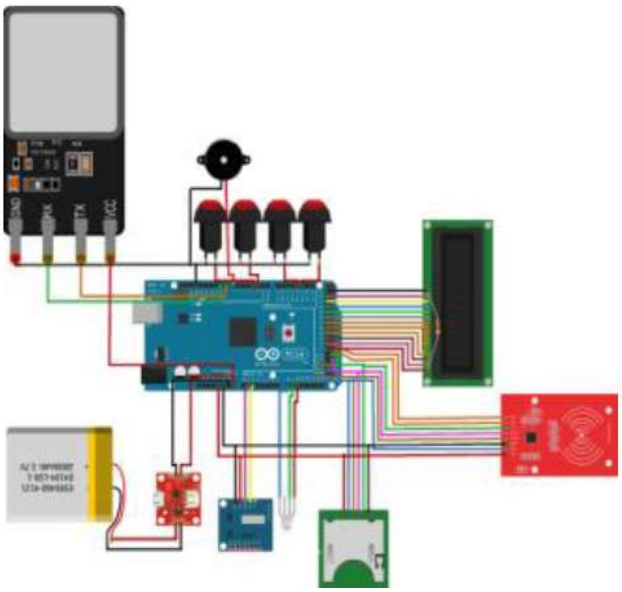

Fig. 2. Circuit Diagram of the system

The circuit was assembled on a double-sided Vero board for compactness and mechanical stability. Each module—RFID reader, fingerprint sensor, RTC, SD card, LCD, and buzzer—was tested individually before final integration to ensure functional accuracy. The RFID reader detects the user's unique card ID, while the fingerprint sensor captures biometric data. Both inputs are verified by the Arduino Uno, and attendance is marked only when the stored RFID and fingerprint data match. This ensures dual-layer security, preventing proxy attendance or unauthorized access.

Power to the system is provided by a 12V DC source, regulated to 5V for the microcontroller and other peripherals. A lithium-ion rechargeable battery (5000 mAh) is included as a backup power source, connected through a charging/discharging module that allows recharging via a standard 5V USB charger. A power switch and LED indicator display system activity, ensuring ease of operation and maintenance.

The Real-Time Clock (RTC) module maintains precise time and date records for each attendance log, enabling accurate timestamping. The LCD provides visual feedback to users, displaying messages such as "Scan RFID Card," "Place Finger," or "Access Granted." The buzzer produces short audio alerts for successful or failed authentication attempts.

Simulation was initially attempted in Proteus, but due to the lack of compatible libraries for RFID and fingerprint modules, the schematic and layout were designed using Fritzing software. The Hardware-in-the-Loop (HIL) testing approach was used for real-time verification, allowing physical components to interact

with the control code during testing. This method provided a practical assessment of communication accuracy, timing, and voltage stability before full-scale deployment.

After individual component verification, all modules were integrated onto a custom shield board compatible with the Arduino Uno. This design minimized wiring complexity and made module replacement easier. The fully assembled system was evaluated in multiple test scenarios to verify reliability and response accuracy. Results confirmed that attendance was successfully recorded only when both RFID and fingerprint inputs matched the stored user data.

This methodology demonstrates an effective combination of biometric and RFID technologies using Arduino Uno to create a cost-effective and secure attendance management system. The dual verification mechanism enhances security, while real-time clock synchronization and SD card data storage ensure precise, tamper-proof record-keeping suitable for institutions, offices, and secure environments.

## 4. TEST AND DATA

### A. Enrolment Mode Testing

The enrolment mode testing ensures that only authorized personnel can register new students and that both RFID and fingerprint credentials are correctly stored for dual authentication. The testing procedure begins with the administrator accessing the enrolment field. To maintain system security, only the admin has the right to enroll a student. The admin verifies their identity by placing their pre-registered finger on the fingerprint scanner. Once the admin's fingerprint is successfully authenticated, the enrolment mode is activated.

After activation, the student is instructed to bring their RFID card close to the RFID reader to initiate the registration process. The Arduino Uno retrieves the card's unique UID code and verifies it against the system. Once the UID is validated, the system associates this unique RFID ID with a specific fingerprint slot number, ensuring each student has a unique dual identity.

The next step involves capturing the student's fingerprint. The system prompts the student to place their finger on the fingerprint sensor. When the finger is placed, the sensor captures the image and sends it to the controller for processing. Immediately after, the system requests the student to place the same finger again to verify and confirm the match. If both scans are identical and successfully verified, the system saves the fingerprint template into the designated memory slot linked to the RFID UID.

This process is repeated for each student to ensure that their unique RFID and fingerprint data are stored correctly. During the testing phase, the enrolment procedure was successfully conducted for ten students, and each student's fingerprint and RFID information was securely stored in the database. The confirmation messages displayed on the LCD and audio feedback from the buzzer helped indicate the success or failure of each registration step. This testing validated the reliability, accuracy, and security of the dual-enrolment process.

### B. Attendance Mode Testing

The attendance mode serves as the primary operational mode of the system and is designed for ease of use without the need for administrative authorization. This ensures smooth and efficient daily attendance marking. When a student places their RFID card near the RFID reader, the system immediately scans the card and retrieves the unique UID code. It then cross-checks this UID with the stored database to identify the corresponding student number.

Once the RFID verification is successful, the system prompts the student to place their registered finger on the fingerprint sensor. The fingerprint scanner captures the image and compares it with the stored fingerprint template associated with the RFID UID. This dual verification ensures that the person carrying the RFID card is the rightful owner.

If both the RFID and fingerprint match correctly, the system automatically marks the student as "Present." The attendance record is then stored in the pre-defined attendance array, along with the time and date fetched from the RTC module. An LCD message confirms successful attendance, while the buzzer provides audio feedback to notify the student.

### C. Compilement mode testing

The compilement mode is designed to finalize and secure all attendance records. Once this mode is activated, no further changes can be made, ensuring data accuracy. The admin verifies their identity through a fingerprint scan, after which the system automatically compiles the attendance data of all present students.

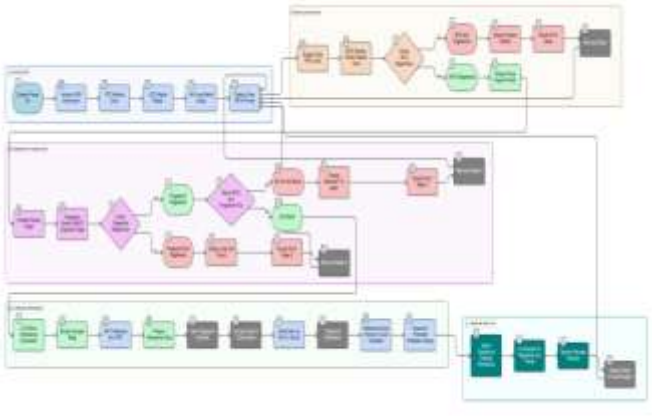

Fig. 3. Steps involved in testing the system

The compiled data, including student ID, date, time, and status, is stored in a TXT file on the SD card. This process makes the records tamper-proof and eliminates manual errors. The testing confirmed that once compilement mode is triggered, no further attendance input or edits are allowed, ensuring reliability and security of the stored data.

### D. Data

In the functional requirements, the system was tested with ten students, where most were already enrolled by the admin and one was left unregistered to check unauthorized access. Five users were analyzed to evaluate system performance. The results, shown in Table I, confirmed that the system accurately identified registered users and rejected unregistered ones, ensuring secure and reliable attendance tracking.

TABLE 1: THE RESULT FROM THE TEST

| No | Date | Time | Status |
|---|---|---|---|
| 1 | 10-10-2025 | 09:05:12 | Mark |
| 2 | 10-10-2025 | 09:05:42 | Mark |
| 3 | 10-10-2025 | 09:06:22 | Mark |
| 4 | 10-10-2025 | 09:06:45 | Mark |
| 5 | 10-10-2025 | 09:07:12 | Mark |
| 6 | 10-10-2025 | 09:07:43 | Mark |
| 7 | 10-10-2025 | 09:08:05 | Mark |
| 8 | 10-10-2025 | 09:08:40 | Mark |
| 9 | 10-10-2025 | 09:09:13 | Mark |
| 10 | 10-10-2025 | 09:09:52 | Mark |

## 5. RESULT

The result of designing and implementing this project shows that it provides an effective and long-lasting solution to several problems faced during attendance taking in institutions. By integrating RFID and fingerprint authentication, the system ensures accurate and secure attendance tracking. However, with rapid technological advancements, there is a possibility of attempts to bypass or forge the system, which may affect its efficiency. Despite these challenges, the study remains significant as it directly addresses key issues in developing a reliable attendance system. A few technical difficulties were also encountered during the implementation and construction phases, but they were resolved to ensure the system's proper functionality.

## 6. CONCLUSION

The traditional pen-and-paper method of taking attendance has long been inefficient, time-consuming, and prone to errors. Implementing an electronic attendance management system offers a faster, more secure, and reliable alternative. The RFID-biometric hybrid system provides administrators with quick access to student attendance data, ensures privacy, and enhances data security. By combining RFID and fingerprint verification, the system delivers a dependable and tamper-resistant solution that can effectively replace outdated manual processes.

A coordinated hardware and software model was developed to create a fully functional embedded system that simplifies and secures attendance tracking. The use of external memory ensures better data structuring, while fingerprint header configuration enhances both security and speed. This modern system eliminates the need for conventional attendance-taking methods, providing a more efficient and secure way to record and manage attendance in educational institutions.

## REFERENCES

[1] S. S. Solanki, N. P. Chaudhari, and M. J. Kumbhar, "RFID Based Attendance Management System," *International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE)*, vol. 4, no. 6, pp. 142–146, 2015.

[2] A. M. Bhoi and M. S. Patil, "Biometric and RFID Based Student Attendance System," *International Journal of Emerging Trends in Electrical and Electronics (IJETEE)*, vol. 11, no. 4, pp. 12–16, 2015.

[3] K. G. Gawali and A. S. Chavan, "RFID Based Student Attendance Monitoring System," *International Journal of Engineering Research and Applications (IJERA)*, vol. 5, no. 3, pp. 22–27, 2015.

[4] S. M. Ismail, M. F. Abas, and M. R. M. Jambak, "RFID and Fingerprint Authentication for Attendance System," *International Journal of Computer Science and Information Security (IJCSIS)*, vol. 14, no. 2, pp. 75–80, 2016.
[5] S. A. Ahmed and S. S. Naik, "An Efficient Biometric Attendance Management System Using Fingerprint and RFID," *International Journal of Advanced Computer Science and Applications (IJACSA)*, vol. 8, no. 7, pp. 233–238, 2017.
[6] M. A. Rahman, A. H. Chowdhury, and M. H. Rahman, "Design and Implementation of a Smart Attendance System Using RFID and Biometrics," *International Journal of Computer Applications (IJCA)*, vol. 168, no. 8, pp. 24–29, 2017.
[7] T. T. Vu, H. Q. Nguyen, and H. T. Nguyen, "Biometric-RFID Attendance System: Design and Implementation," *International Journal of Advanced Trends in Computer Science and Engineering (IJATCSE)*, vol. 9, no. 3, pp. 3042–3048, 2020.
[8] R. S. Kumbhar, A. B. Raut, and S. P. Wankhede, "Development of RFID and Fingerprint Based Attendance System," *International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)*, vol. 8, no. 2, pp. 110–115, 2020.
[9] N. B. Gaikwad and S. S. Deshmukh, "Secure Student Attendance System Using RFID and Biometric," *International Journal of Engineering and Advanced Technology (IJEAT)*, vol. 9, no. 4, pp. 1321–1325, 2020.
[10] P. Jain, V. Kumar, and A. Sharma, "Integration of RFID and Fingerprint Technology for Attendance Monitoring," *Journal of Intelligent & Fuzzy Systems*, vol. 38, no. 3, pp. 3101–3108, 2021.

**Shivam Singh** was born in 2003 in Uttar Pradesh (India). He is currently persuing B.Tech. from Prasad Institue of Technology Jaunpur.

**Adarsh Kumar Maurya** was born in 2003 in Uttar Pradesh (India). He is currently persuing B.Tech from Prasad Institute of Technology Jaunpur.

**Ankit Chaursiya** was born in 2005 in Uttar Pradesh (India). He is currently persuing B.Tech from Prasad Institute of Technology Jaunpur.

**Haraprit Kumar** was born in 200 in Uttar Pradesh (India). He is currently persuing B.Tech from Prasad Institute of Technology Jaunpur.

**Sachin Saroj** was born in 2004 in Uttar Pradesh (India). He is currently persuing B.Tech from Prasad Institute of Technology Jaunpur.