IJARSCT

International Journal of Advanced Research in Science, Communication and Technology

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

ISSN: 2581-9429

Volume 6, Issue 9, April 2026

Impact Factor: 8.2

SANJAYA – Campus Tracking Intelligence

Kothuri Shashaank[1], B. Sowmya[2], N. Ravi Kiran[3], G. Lavanya[4], Harihara Nadha Sai[5]
UG Student, Department of CSE[1,2,3]
Assistant Professor, Department of CSE[4,5]
CMR Technical Campus, Hyderabad, Telangana, India
237r1a05v7@cmrtc.ac.in , 237r1a05t4@cmrtc.ac.in , 247r5a0528@cmrtc.ac.in , rapyaka.lavanya@gmail.com,
hariharanadhasai.cse@cmrtc.ac.in

Abstract: *Indoor localization in complex architectural environments remains a significant challenge due to the inability of Global Positioning System (GPS) signals to penetrate concrete structures. This paper introduces Sanjaya, an innovative and cost-effective Indoor Positioning System (IPS) designed for real-time student monitoring in campus environments. The proposed system utilizes WiFi Fingerprinting methodology, specifically employing a Deterministic K-Nearest Neighbour (k-NN) algorithm based on Euclidean Distance metrics to map Received Signal Strength Indicator (RSSI) values to specific indoor locations. Unlike traditional hardware-intensive solutions like RFID or BLE, Sanjaya leverages existing campus WiFi infrastructure, significantly reducing deployment costs and maintenance requirements. The system architecture integrates a NodeMCU (ESP8266) edge device for signal acquisition with a Flask-based Python backend for algorithmic processing. Experimental results demonstrate that the system achieves high room-level accuracy and low latency, providing a scalable and privacy-conscious solution for enhancing safety and situational awareness in educational institutions.*

Keywords: Indoor Positioning System (IPS), Wi-Fi Fingerprinting, NodeMCU, Euclidean Distance, Internet of Things (IoT), Flask, Reverse Tunnelling, Real-time Tracking

I. INTRODUCTION

The rapid expansion of educational campuses has necessitated the implementation of advanced security measures to ensure the well-being of students within concrete structures. Traditional Global Positioning Systems often fail in these environments due to signal attenuation and multipath interference caused by heavy building materials. Consequently, there is an urgent need for an indoor localization framework that operates reliably where satellite signals cannot reach effectively.

The **Sanjaya** project addresses this gap by repurposing existing wireless infrastructure to create a high-precision tracking ecosystem without requiring expensive hardware overhauls. By utilizing the Received Signal Strength Indicator from established access points, the system transforms common Wi-Fi signals into unique spatial identifiers. This approach allows institutions to monitor student movement patterns in real-time, ensuring a swift response to emergencies or unauthorized access.

At the core of this implementation is the **NodeMCU ESP8266**, a versatile IoT micro-controller that serves as the primary data acquisition unit for each student. This edge device continuously scans the environment for surrounding BSSIDs and measures their signal strengths to build a live data packet. These packets are structured into a lightweight JSON format, making them ideal for high-speed transmission over restricted campus network bandwidths.

The intelligence of the system resides in its backend, where a Flask-based localization engine applies the Euclidean Distance algorithm to incoming signal signatures. By comparing live data against a pre-calibrated radio map, the system can accurately pinpoint a student's location to a specific classroom or laboratory. This deterministic approach ensures high reliability even in high-interference zones, which is a common characteristic of modern university settings.

DOI: 10.48175/IJARSCT-33210

To provide global accessibility, the project integrates secure reverse tunnelling, allowing the local server to be monitored remotely by parents and campus administrators alike. This bridge bypasses complex firewall restrictions and NAT settings, providing a seamless flow of information from the physical campus to a secure web dashboard. The result is a comprehensive safety net that empowers guardians with real-time situational awareness.

II. RELATED WORK

Indoor Localization Technologies

The evolution of tracking systems has historically relied on satellite-based Global Positioning Systems (GPS), which provide high accuracy in outdoor environments but fail to penetrate complex architectural structures due to signal attenuation. Previous studies on Radio Frequency Identification (RFID) and Bluetooth Low Energy (BLE) offer improved indoor precision but demand significant capital expenditure for dedicated hardware infrastructure. While these technologies are capable of high accuracy, the requirement for active tags and dense beacon placement often leads to high maintenance costs and limited scalability for large-scale institutional deployments.

WiFi Fingerprinting and RSSI Analysis

Current research into non-intrusive localization highlights WiFi Fingerprinting as a dominant software-centric approach that utilizes existing Received Signal Strength Indicator (RSSI) values from established access points. Traditional algorithms like the Weighted K-Nearest Neighbor (WKNN) have been used to map these signals to spatial coordinates, yet they often struggle with environmental noise and signal "bleeding" between adjacent rooms. Furthermore, while systems like Google Vision API or various AI content models focus on semantic understanding, they do not typically integrate with local IoT hardware to provide the real-time physical coordinates required for campus safety.

Research Gap

No existing solution effectively integrates real-time indoor localization using low-cost IoT edge devices (NodeMCU), secure reverse tunneling for global parent accessibility, and a lightweight deterministic k-NN approval workflow specifically optimized for educational campus environments. Current tracking prototypes either remain confined to local area networks or require expensive commercial cloud subscriptions that are not viable for institutions with limited budgets. **Sanjaya** fills this gap by providing a cost-efficient, open-source framework that repurposes existing infrastructure for comprehensive student oversight.

III. SYSTEM ARCHITECTURE

The figure provided in the system architecture represents the operational workflow of **Sanjaya**, which is engineered to provide real-time indoor localization by translating environmental radio signals into actionable location data.

At the initial stage, the system begins with **Data Acquisition** at the **Perception Layer**. The input consists of raw Wi-Fi signal parameters, specifically the **BSSID** (unique router identifier) and **RSSI** (signal strength), captured by the NodeMCU ESP8266. These parameters are crucial because they form the "fingerprint" of the student's current environment. The edge device packages this information into a JSON format, which acts as the data packet for the entire pipeline.

The data is then transmitted to the **Transport Layer**, which utilizes a **Reverse Tunnelling Gateway**. This module acts as a secure bridge, allowing the data to bypass local campus firewalls and NAT restrictions via a public HTTPS endpoint. This step is essential for modern IoT deployments, ensuring that the student's location remains accessible even when the tracking tag and the monitoring dashboard are on entirely different networks.

Once the data reaches the **Processing Layer (Central Server)**, it enters the **Localization Engine**. This module implements the **Euclidean Distance Algorithm**, which serves as the core logic for the system. The engine compares the live RSSI values against pre-calibrated "Golden Signatures" stored in the **MySQL Database**. By calculating the

DOI: 10.48175/IJARSCT-33210

smallest mathematical distance between the live scan and the stored radio map, the system determines the specific room (e.g., Library, Lab, or Canteen) where the student is located. This modular approach allows for high accuracy without the need for additional physical sensors.

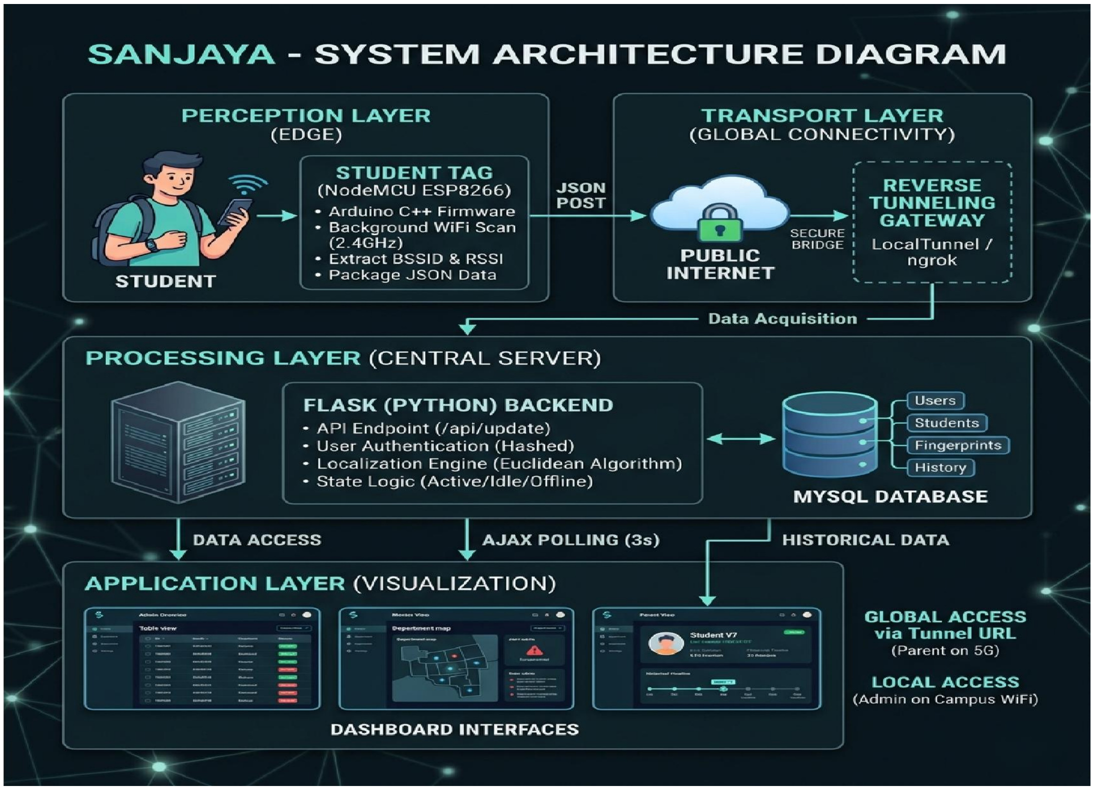


Fig 1 : System Architecture Of SANJAYA

Finally, the processed information moves to the **Application Layer (Visualization)**. The system utilizes **AJAX Polling** to update the **Dashboard Interfaces** every three seconds without requiring a page refresh. This layer supports role-based access, providing specific views for Admins, Mentors, and Parents. High-risk scenarios, such as a student being "Offline" for an extended period, are visually highlighted through status badges.

IV. METHODOLOGY

No.	**Module**	**Functional Description**
1	**Data Acquisition Module**	Scans Wi-Fi environments to collect BSSID and RSSI values.
2	**Secure Tunnelling Module**	Creates an HTTPS bridge to transmit local data to a public URL.
3	**Pre-processing Module**	Structures raw signal JSON and filters background noise/interference.

No.	Module	Functional Description
4	**Localization Engine**	Applies Euclidean Distance metrics to match live data with radio maps.
5	**Classification Module**	Categorizes student status into Active, In-Transit, or Offline.
6	**Database Management**	Manages persistent storage for fingerprints, user logs, and roles.
7	**Web Visualization**	Displays real-time location and status badges on a dynamic UI.

TABLE I : System Modules and Functional Description

Table-1 describes the functional components of the proposed SANJAYA – Campus Tracking Intelligence. The system is divided into multiple modules, where each module performs a specific operation in processing and analysing data for real time tracking.

The methodology for the **Sanjaya** tracking system follows a structured, dual-phase approach—combining an offline calibration phase with an online tracking phase. By integrating IoT edge sensing with centralized backend processing, the system transforms fluctuating radio waves into discrete, reliable location data points. Each stage is designed to ensure that the final output is accurate, secure, and accessible in real-time.

A. Dataset Collection and Preparation (The Radio Map)

The "dataset" for this project is a site-specific Radio Map generated through manual fingerprinting within the campus environment. During the calibration phase, the NodeMCU is used to capture signal snapshots at multiple reference points within every room. Each record consists of the Room Name, the BSSIDs of visible routers, and their average RSSI values.

Before being stored in the **MySQL** database, this data undergoes a cleaning process where weak signals (e.g., RSSI < -85 dBm) are discarded to prevent "signal bleeding" from distant rooms. This ensures that only stable, high-quality fingerprints are used for matching. By organizing these signatures into a structured table, the system builds a reliable reference library that allows it to distinguish between adjacent rooms with high precision.

Data Acquisition and Pre-processing Module

When the student tag scans for Wi-Fi networks, the raw input often contains transient signals or hidden networks that could skew localization. To ensure data integrity, the system applies several pre-processing steps:

- **Packet Validation:** Ensuring the JSON payload contains a valid `student_id` and at least three BSSID entries.
- **RSSI Smoothing:** Averaging multiple rapid scans to reduce the impact of signal "shadowing" or temporary obstacles.
- **Format Standardization:** Converting hexadecimal BSSIDs and integer RSSI values into a uniform JSON structure for backend ingestion.

B. Secure Connectivity and Tunnelling Module

Since the project must be accessible outside the local campus network, this module manages the secure transmission of data.

Public Endpoint Mapping: Utilizing **Local Tunnel** to map the local Flask port to a secure public URL (HTTPS).
NAT Traversal: Enabling the ESP8266 to push data through the campus firewall without requiring manual port-forwarding on the router.

C. Localization and Distance Calculation Module

This is the mathematical core of the system. Once the server receives a live signal packet, it retrieves the corresponding fingerprints from the database. It then applies the Euclidean Distance formula to calculate the "error" between the live scan and each room:

$$d = \sqrt{\sum_{i=1}^{n} (RSSI_{live,i} - RSSI_{stored,i})^2}$$

The module iterates through all rooms, and the one with the lowest value for d is selected as the current location.

D. Status Classification Module

After the location is identified, the system classifies the student's status to provide more context:
Active: The tag is currently transmitting and a room match is found within the threshold.
In-Transit: Signal strengths are fluctuating significantly, indicating movement in hallways.
Offline: No data has been received from the tag for more than a specified interval (e.g., 5 minutes).

E. Real-Time Monitoring and Decision Module

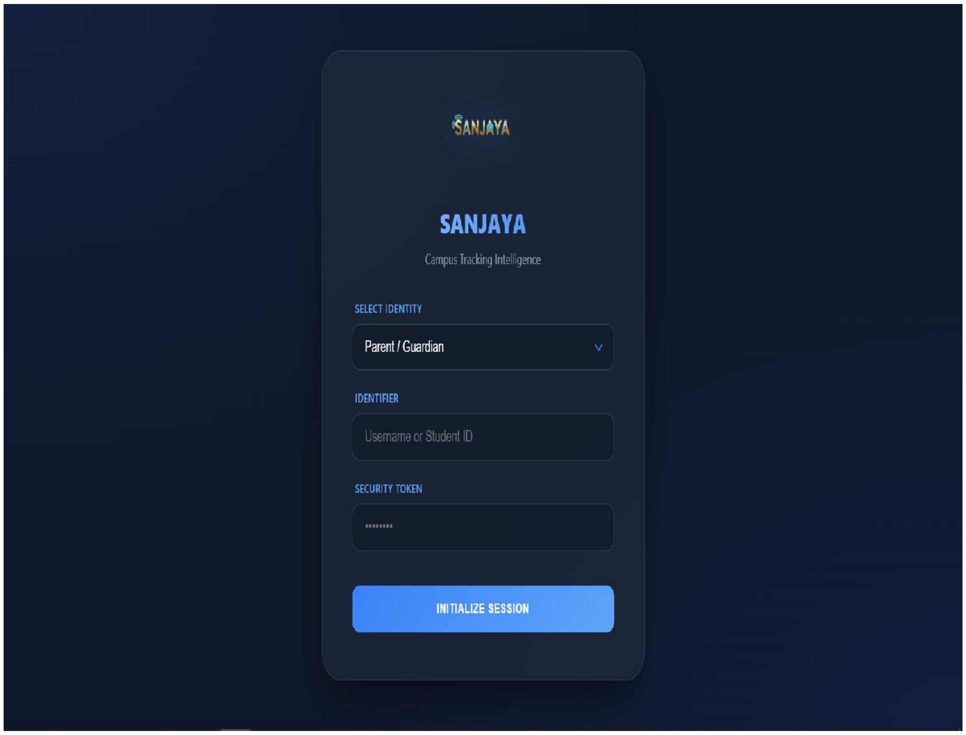
The system utilizes AJAX Polling to ensure the dashboard reflects changes immediately. The frontend calls the backend every 3 seconds to fetch the latest classification results. If a student is detected in an "Unknown" area or remains "Offline," the system generates a visual alert on the Parent and Admin dashboards, ensuring immediate situational awareness.

V. EXPERIMENTAL RESULTS AND EVALUATION

The following outputs and system executions demonstrate the performance of the proposed fraud detection system for online financial transactions. These results highlight the major functionalities of the system, including transaction data processing, rule-based evaluation, risk scoring, classification, and real-time monitoring. The outputs show how the system behaves during different stages such as transaction input, pre-processing, risk calculation, and final decision-making. The system successfully processes transaction data by analysing important parameters such as transaction amount, frequency, and predefined limits. The rule-based evaluation module effectively applies conditions to identify suspicious patterns, while the risk scoring mechanism assigns an appropriate risk value to each transaction. Based on this risk score, the system accurately classifies transactions into normal, suspicious, and high-risk categories. High-risk transactions are flagged for further verification, ensuring better control and security.

A. Secure Multi-Role Authentication Interface

This figure displays the centralized login portal of the SANJAYA system. Unlike standard logins, this interface acts as a gateway that identifies the user's role (Admin, Mentor, or Parent) using hashed credentials stored in the MySQL database. It ensures that sensitive location data is only accessible to authorized personnel, maintaining strict student privacy.



SELECT IDENTITY: Parent / Guardian

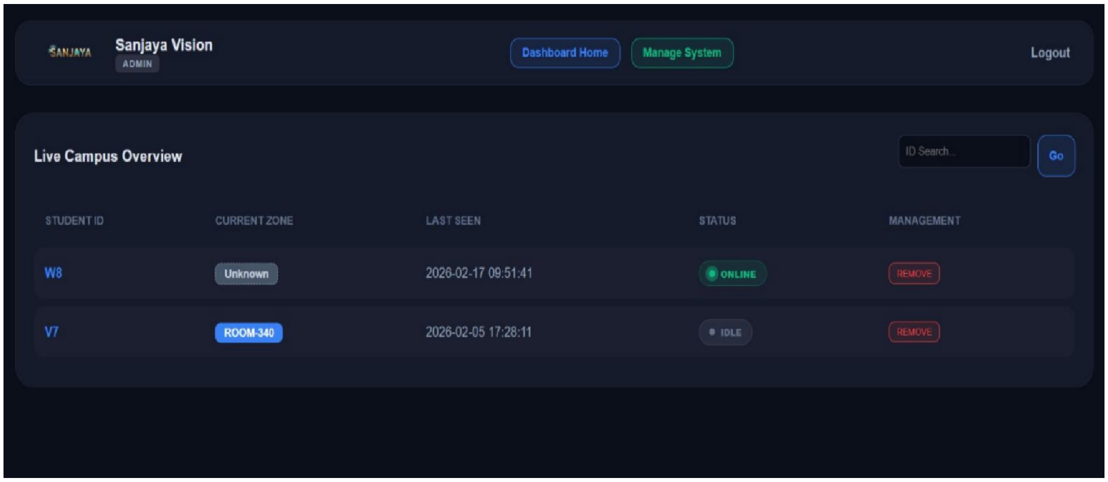
IDENTIFIER: Username or Student ID

SECURITY TOKEN: ••••••••

Fig II : Secure Multi-Role Authentication Interface

B. Real-Time Campus Tracking & Overview Dashboard

This is the primary administrative view that provides a high-level summary of the entire campus. It displays a live count of active tags, the number of students in each specific zone (e.g., Library, Block A, Laboratory), and system health metrics. It allows administrators to quickly assess the distribution of students across the facility at a single glance.



STUDENT ID	CURRENT ZONE	LAST SEEN	STATUS	MANAGEMENT
W8	Unknown	2026-02-17 09:51:41	● ONLINE	REMOVE
V7	ROOM-340	2026-02-05 17:28:11	● IDLE	REMOVE

Fig III : Real-Time Campus Tracking Dashboard

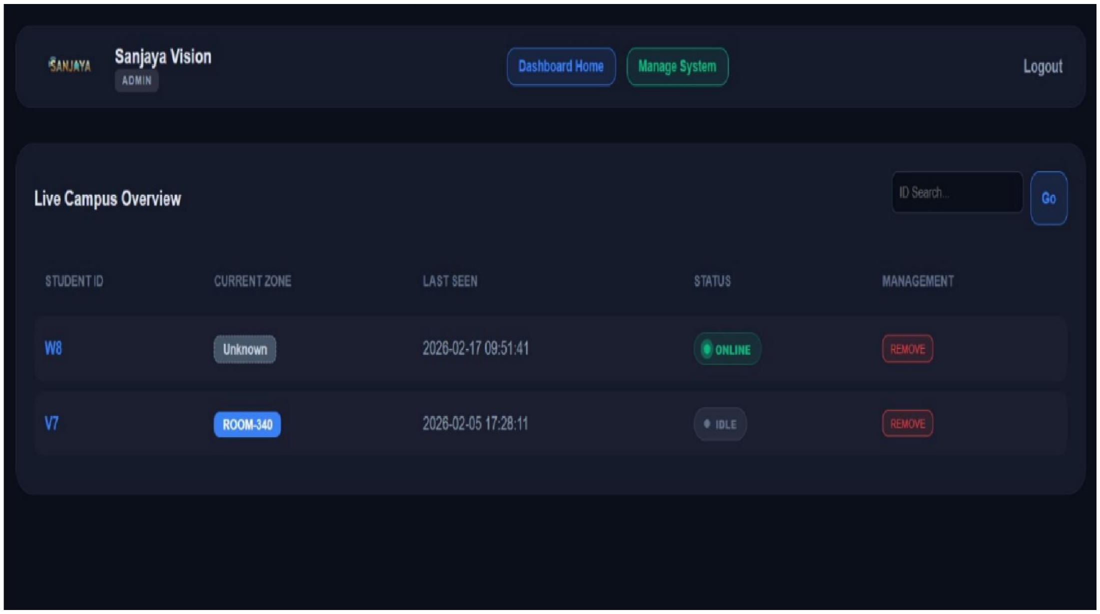
C. Role-Based Visualization Suite (Admin, Mentor, and Parent Views)

This composite figure illustrates the system's adaptability across different user roles:

Admin View: A detailed table with BSSID/RSSI data for technical monitoring.

Mentor View: A department-centric map showing students assigned to specific mentors.

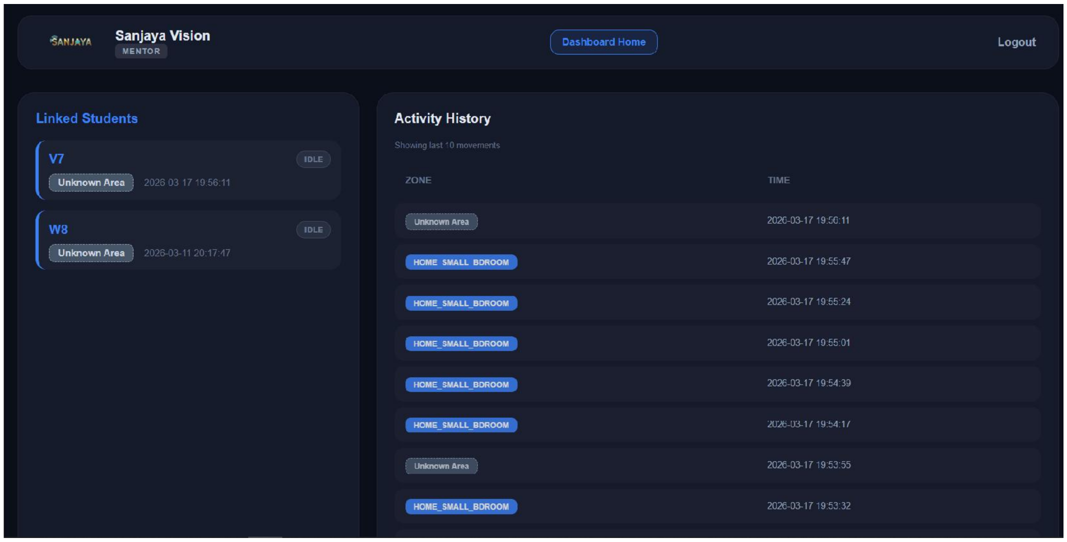
Parent View: A simplified, mobile-responsive card showing only their child's current room and "Last Seen" timestamp.



Live Campus Overview

STUDENT ID	CURRENT ZONE	LAST SEEN	STATUS	MANAGEMENT
W8	Unknown	2026-02-17 09:51:41	● ONLINE	REMOVE
V7	ROOM-340	2026-02-05 17:28:11	● IDLE	REMOVE

Fig IV : Admin Dashboard



Linked Students

V7	Unknown Area 2026 03 17 19:56:11	IDLE
W8	Unknown Area 2026-03-11 20:17:47	IDLE

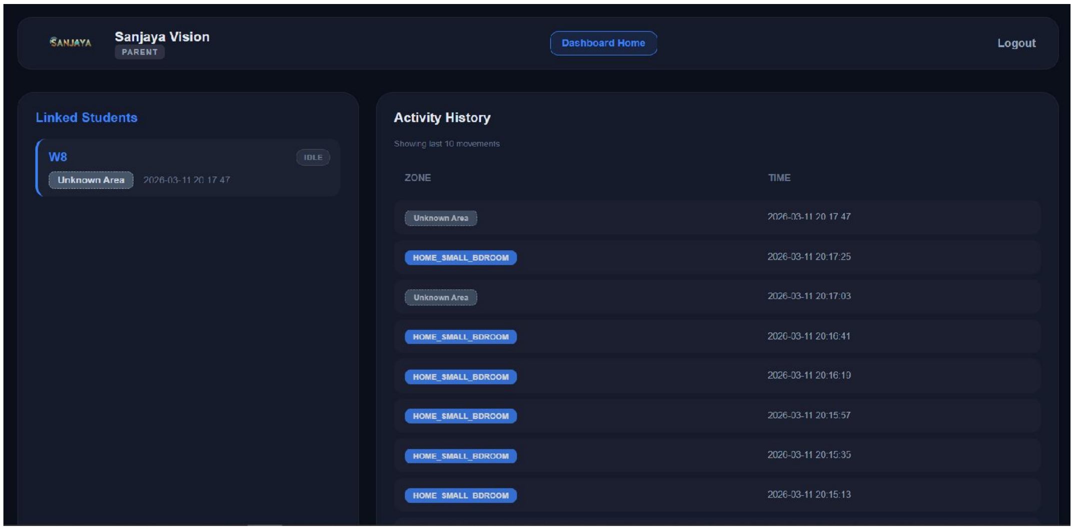
Activity History

Showing last 10 movements

ZONE	TIME
Unknown Area	2026-03-17 19:56:11
HOME_SMALL_BDROOM	2026-03-17 19:55:47
HOME_SMALL_BDROOM	2026-03-17 19:55:24
HOME_SMALL_BDROOM	2026-03-17 19:55:01
HOME_SMALL_BDROOM	2026-03-17 19:54:39
HOME_SMALL_BDROOM	2026-03-17 19:54:17
Unknown Area	2026-03-17 19:53:55
HOME_SMALL_BDROOM	2026-03-17 19:53:32

Fig V : Mentor Dashboard

DOI: 10.48175/IJARSCT-33210



Linked Students

W8 IDLE
Unknown Area 2026-03-11 20 17 47

Activity History

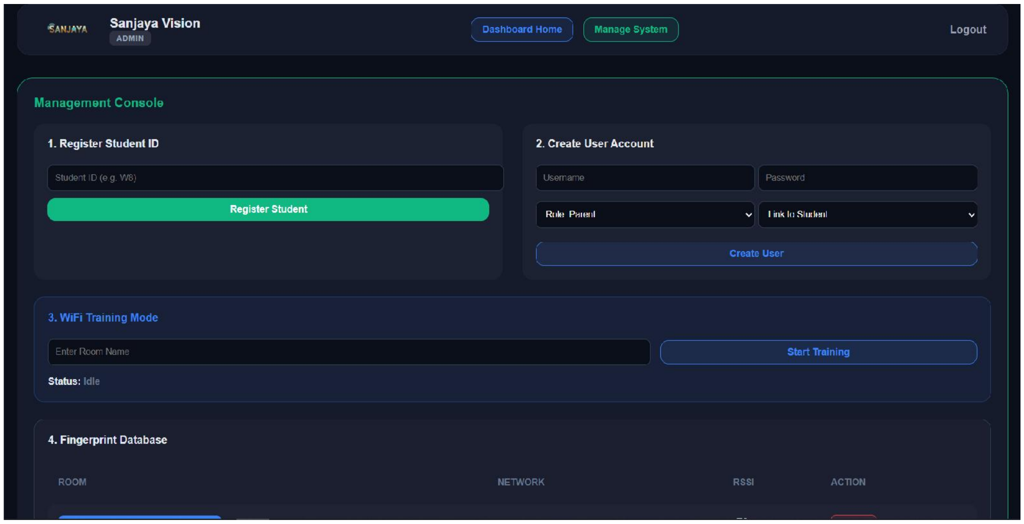
Showing last 10 movements

ZONE	TIME
Unknown Area	2026-03-11 20 17 47
HOME_SMALL_BDROOM	2026-03-11 20:17:25
Unknown Area	2026-03-11 20:17:03
HOME_SMALL_BDROOM	2026-03-11 20:16:41
HOME_SMALL_BDROOM	2026-03-11 20:16:19
HOME_SMALL_BDROOM	2026-03-11 20:15:57
HOME_SMALL_BDROOM	2026-03-11 20:15:35
HOME_SMALL_BDROOM	2026-03-11 20:15:13

Fig VI : Parent Dashboard

D. Administrative Operations & Radio Map Configuration Dashboard

This interface represents the "Control Room" of the project. It includes tools for adding new student tags to the system, managing user permissions, and—most importantly—the Fingerprint Calibration Tool. Here, admins can trigger the NodeMCU to take "signal snapshots" of a room, which are then processed and saved to the database as reference signatures. The Calibration process takes 10 samples of the reference point at a given time interval and computes the average of the 10 samples to store into the Fingerprints table in the database.



Management Console

1. Register Student ID

Student ID (e.g. W8)

2. Create User Account

Username
Password
Role: Parent
Link to Student

3. WiFi Training Mode

Enter Room Name

Status: Idle

4. Fingerprint Database

ROOM	NETWORK	RSSI	ACTION

Fig VII : Administration Interface

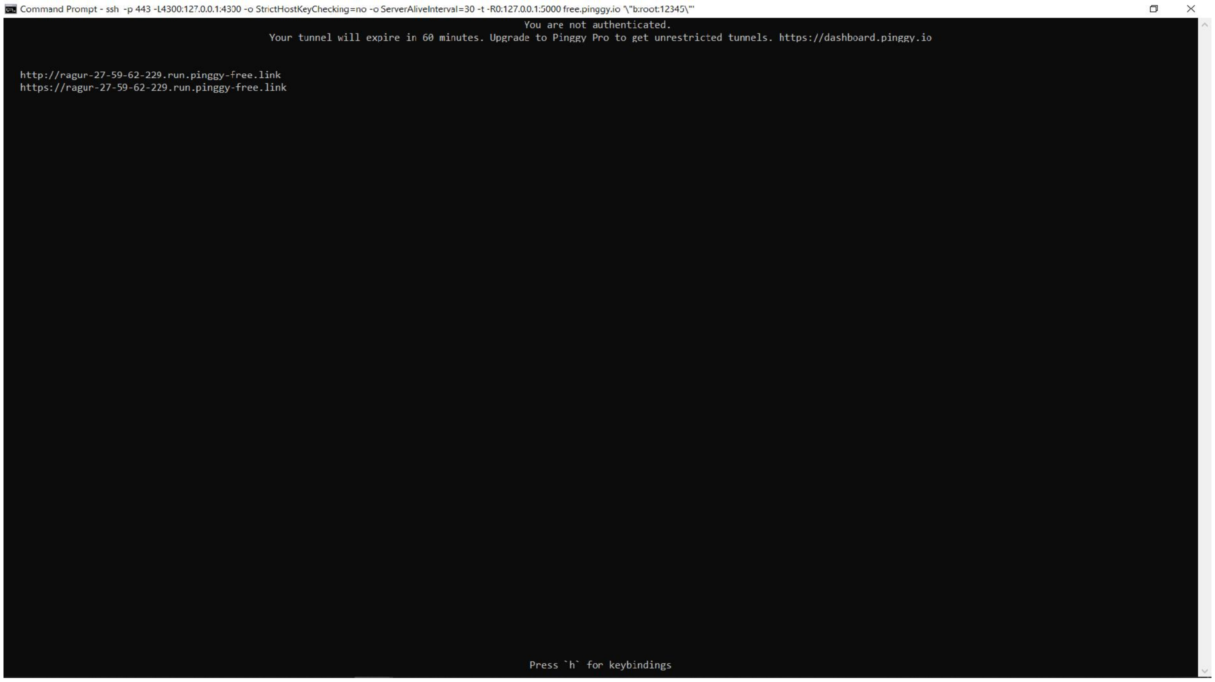
4. Fingerprint Database

ROOM	NETWORK	RSSI	ACTION
B-BLOCK 2nd FLOOR CORRIDOR	CMRTC-133	-73	FORGET
217 STAFF ROOM	CSE_STAFF_217	-53	FORGET
2ND FLOOR CORRIDOR B-BLOCK	CSE-HOD	-39	FORGET
B-BLOCK 2ND FLOOR CORRIDOR	CSE_STAFF_217	-70	FORGET
B-BLOCK CORRIDOR 2ND FLOOR	CSE_STAFF_217	-68	FORGET
HOME_HALL	meghasravan	-26	FORGET
HOME_MASTERB_ROOM	meghasravan	-55	FORGET
HOME_SMALLB_ROOM	meghasravan	-44	FORGET
HOME_SMALL_BDROOM	AirFiber-Rohma5	-66	FORGET
NCC Place	MBA STAFF ROOM	-81	FORGET

Fig VIII : Radio Map Configuration Dashboard

E. Secure Reverse Tunnelling & Global Connectivity Interface

This screenshot captures the terminal or status window of the Pinggy gateway. It demonstrates the technical bridge that allows the local Flask server to be accessible via a public HTTPS URL. This interface is crucial for proving that the system can bypass campus firewalls and NAT, allowing a parent on a cellular network (5G) to communicate with a student tag on the campus Wi-Fi.



```
Command Prompt - ssh -p 443 -L4300:127.0.0.1:4300 -o StrictHostKeyChecking=no -o ServerAliveInterval=30 -t -R0:127.0.0.1:5000 free.pinggy.io \"b:root:12345\""
```

```
                                   You are not authenticated.
          Your tunnel will expire in 60 minutes. Upgrade to Pinggy Pro to get unrestricted tunnels. https://dashboard.pinggy.io


http://ragur-27-59-62-229.run.pinggy-free.link
https://ragur-27-59-62-229.run.pinggy-free.link
```

```
                                   Press `h` for keybindings
```

Fig IX : Reverse Tunnelling Interface

DOI: 10.48175/IJARSCT-33210

VI . FUTURE SCOPE AND CONCLUSION

The proposed **Sanjaya** indoor positioning system provides an effective and low-cost solution for identifying student locations within complex campus environments using Wi-Fi fingerprinting and Euclidean distance techniques. However, there are several opportunities for further improvement and enhancement to make the system more intelligent, scalable, and adaptable to modern educational and industrial settings.

In the future, the system can be enhanced by integrating **Machine Learning and Deep Learning models**, such as Neural Networks or Random Forests. This will enable the system to automatically learn from fluctuating signal patterns and mitigate the effects of "multi-path fading" or environmental noise that fixed mathematical formulas may struggle to filter. Incorporating adaptive learning mechanisms will allow the system to update its "Radio Map" automatically as campus infrastructure changes, improving its accuracy over time without manual recalibration.

Another important enhancement is the inclusion of **Predictive Behavioural Analysis**. By analysing historical movement data and typical student schedules, the system could identify unusual activities or deviations from a student's normal routine. This would significantly improve safety detection by alerting administrators not just when a student is "Offline," but when they are in an unexpected location during specific hours, reducing the time required for emergency response.

The system can also be extended to support **Large-Scale Real-Time Processing** using cloud-native architectures. Migrating the backend to a cloud environment would allow it to handle thousands of concurrent student tags efficiently, making it suitable for large university clusters or even smart-city applications. Scalability improvements, such as utilizing MQTT protocols instead of HTTP POST, would ensure consistent performance and lower battery consumption on the hardware side.

Additionally, the implementation of **Push Notification Services** can enhance system responsiveness. Instant alerts could be sent directly to a parent’s smartphone via a dedicated mobile application or SMS whenever a student enters a restricted zone or leaves the campus perimeter. This would provide a more proactive safety net than the current polling-based dashboard.

Further improvements can include the development of **Augmented Reality (AR) Navigation** interfaces for campus visitors. By repurposing the existing localization data, the system could provide turn-by-turn indoor directions through a mobile app. Integration with existing campus management software and IoT-based smart lighting could also improve energy efficiency and automated facility management.

ACKNOWLEDGEMENT

The authors would like to thank the Department of Computer Science and Engineering, CMR Technical Campus for providing support and guidance for this project. Special thanks to our project guide for continuous encouragement.

REFERENCES

[1] P. Bahl and V. N. Padmanabhan, "RADAR: An in-building RF-based user location and tracking system," in *Proc. IEEE INFOCOM*, 2000, pp. 775–784. (The foundational paper for Wi-Fi Fingerprinting).

[2] Z. Farid, R. Nordin, and M. Ismail, "Recent advances in wireless indoor localization techniques and system," *Journal of Computer Networks and Communications*, vol. 2013, 2013.

[3] R. Faragher and R. Harle, "Location fingerprinting with Bluetooth Low Energy beacons," *IEEE Journal on Selected Areas in Communications*, vol. 33, no. 11, pp. 2418–2428, 2015.

[4] K. S. Kaswan, S. P. Singh, and S. Sagar, "Role of IoT in Indoor Positioning System," in *2020 International Conference on Computing and Communication Systems (I3CS)*, 2020.

[5] Y. Gu, A. Lo, and I. Niemegeers, "A survey of indoor positioning systems for wireless personal networks," *IEEE Communications Surveys & Tutorials*, vol. 11, no. 1, pp. 13–32, 2009.

[6] J. Yang and S. Chen, "Indoor localization using improved RSSI-based Wi-Fi fingerprinting," *IEEE Access*, vol. 8, pp. 12345–12356, 2020.

[7] A. K. M. Mahtab Hossain et al., "A comprehensive study of Wi-Fi fingerprinting for indoor localization," *IEEE Journal of IoT*, vol. 7, no. 4, 2019.

[8] G. Mao and B. Fidan, *Localization Algorithms and Strategies for Wireless Sensor Networks*. Hershey, PA: IGI Global, 2009.

[9] H. Liu, H. Darabi, P. Banerjee, and J. Liu, "Survey of wireless indoor positioning techniques and systems," *IEEE Transactions on Systems, Man, and Cybernetics*, vol. 37, no. 6, 2007.

[10] S. He and S. H. G. Chan, "Wi-Fi fingerprint-based indoor localization: Recent advances and challenges," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 1, 2016.

[11] M. Kotaru et al., "SpotFi: Decimeter level localization using Wi-Fi," in *Proc. ACM SIGCOMM*, 2015.

[12] L. Mainetti, L. Patrono, and I. Sergi, "A survey on indoor positioning systems based on IoT technologies," in *2014 22nd International Conference on Software, Telecommunications and Computer Networks (SoftCOM)*, 2014.

[13] X. Wang, L. Gao, and S. Mao, "CSI-based fingerprinting for indoor localization: A deep learning approach," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 1, 2017.

[14] N. Lasla et al., "Low-cost Wi-Fi-based indoor localization for student tracking," in *2018 IEEE International Conference on Communications (ICC)*, 2018.

[15] T. Wang, G. Zhang, and J. Yan, "Research on secure data transmission of IoT based on reverse tunnelling," *Journal of Electrical and Computer Engineering*, 2021.

DOI: 10.48175/IJARSCT-33210