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 2, March 2026
Impact Factor: 8.2

Smart Campus Security

Chetan Changude, Raj Kadam, Prutviraj Survase, A.D Kulkarni, Afroz Sayyad
Electronics and Telecommunication
Jaywantrao Sawant Polytechnic, Hadapsar, Pune, India
chetanchandgude51@gmail.com, rajkadam98310@gmail.com,pruthvirajsurwase361@gmail.com
adkulkarni_entc@jspmjspoly.edu.in, gaussayyad291@gmail.comm

Abstract: *Campus gates still use logbooks. Guards sleep, students borrow IDs, "buddy punching" fakes attendance. We built something harder to fool. ESP32 runs it—cheap, connected, enough brain for the job. RFID card plus fingerprint: card proves possession, finger proves identity. Both needed, neither sufficient alone. Servo opens gate, logs timestamp, uploads to cloud. No guard, no paper, no argument. After hours, PIR watches. Motion where none should be—alarm screams, lights flash, alert fires to phone. Intruder startled, security moving, evidence logged. Administrators see everything—who entered when, who failed attempts, where motion detected. Centralized because scattered data useless, automated because humans forget, robust because layered. Cost under ₹4,000. Traditional security expensive, porous, tired. This never sleeps, never borrows ID, never looks away. .*

Keywords: Smart Campus, IoT Security, ESP32, RFID Access Control, Biometrics, PIR Sensor, Cloud Logging

I. INTRODUCTION

Campuses are chaos—thousands moving, some belong, some don't. Guards try, fail. Logbooks fill with fake names, borrowed IDs, "he went in, I think." Server rooms, labs, offices—restricted, supposedly. Reality? Door propped, guard napping, stranger walks.

We got tired of theater. Built gate that actually checks—RFID card for speed, fingerprint for proof. Card waves fast, finger presses, servo opens, log writes, cloud knows. No guard to bribe, no log to fake, no "buddy" punching twice.

PIR for night—motion where silence should be, alarm screams, light blinds, phone buzzes. Intruder runs, security moves, evidence timestamped. Not after break-in discovered, during.

Data piles up—who entered, when rejected, where at 3AM. Administrator sees patterns, spots weirdness, acts before disaster. Not intuition, numbers.

Paper died, automation took over, campus finally watched properly.

II. LITERATURE SURVEY

Access control evolved—slowly, then fast, now messy.

Traditional ID cards: Barcode, magnetic stripe—swipe, wait, replace when scratched. Throughput terrible, cards disposable, security theater. We skipped this entirely.

RFID contactless: Wave and walk—faster, no wear, students love. Stolen cards work, shared cards work, "I'm my friend" fools system. Convenience traded for security, badly.

Biometrics and IoT: MFA buzzword—something have, something are. Card plus finger, both needed, fake hard. ESP32 cheap enough for every gate, WiFi syncs to cloud, global database, instant deny if card reported stolen. Research trends here; we follow with working code, not just theory.

III. PLATFORM TECHNOLOGY USED

This project synthesizes varied sensing technologies with a centralized IoT core.

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 2, March 2026 Impact Factor: 8.2

ESP32 – the gate brain: Dual-core, WiFi native, SPI for RFID, UART for finger, GPIO for PIR, HTTP for cloud. Does everything, costs ₹400, available everywhere. One core handles authentication, other pushes logs, no lag. Sleep modes ignored—gate always awake, always watching.

RC522 RFID – the card reader: 13.56MHz, SPI bus, UID read in milliseconds. Cards ₹20 each, replaceable, losable, shareable—hence second factor. Range 3cm, intentional—no accidental reads, no walk-by logging. "Tap here" sticker guides, compliance high.

Optical fingerprint – the finger check: TIR principle—light hits ridges, reflects, camera captures, template matches. R307 module, UART, 9600 baud, enrollment stored in flash. Wet fingers fail, dry fingers fail, angry users blow, retry works. Not military grade, sufficient for campus, cheap enough for every gate.

PIR sensor – the night watch: Pyroelectric, detects 8-10 meters, 120 degree arc. Human motion—warm body, moving—triggers. Cats ignored (mostly), curtains ignored, actual intruder caught. Adjustable sensitivity, false positive tuning took three nights. Relay drives light and buzzer, 12V, loud, bright.

Cloud platform – the distant eye: Firebase free tier, real-time database, push notifications. Alternative: ThingSpeak graphs, custom server, Blynk app. We chose Firebase—authentication built, scaling automatic, Google reliability. Admin dashboard shows live gate status, historical logs, failed attempts highlighted. Mobile buzzes when PIR screams, when finger rejected thrice, when card stolen reported.

IV. PROBLEM STATEMENT

Campus security? Mostly bullshit.

Proxy access everywhere: "Bro, card de na, attendance lag jaayega." ID swaps daily, restricted zones mean nothing, logs full of fake names. Guards see, don't care, or care and get ignored. System designed for convenience, not truth.

Tracking? Good luck: Something breaks Monday, noticed Wednesday. Paper logs—coffee stained, half empty, completely made up. "Who entered lab 2AM Saturday?" Shrugs. No data, no cameras, no answers. Blame assigned randomly.

Night is joke: One guard, massive campus, probably sleeping in control room. Intruder climbs, grabs, leaves. Patrol passes eventually, flashlight dead, "all clear" ticked. Reactive means already lost.

We built something tighter—card plus finger (no lending), cloud logs (no coffee stains), PIR watching (no sleeping). Unified because piecemeal fails, connected because isolated blinds, actually works because tested with real students trying real hard to break it.

V. AIM AND OBJECTIVES

Build campus gates that actually check who enters, shout when trouble comes.

Automated lock: ESP32 drives servo, turns lock, no guard key required. Code decides open/close, logs everything, never forgets.

Fast entry: RFID wave, UID read, general students through quick. No fingerprint for main gate—throughput matters, lines kill.

Strict zones: Server room, lab, admin—finger required. Card stolen? Useless. Finger chopped? Extreme, rare, Hollywood. Dual factor stops casual sharing, stops most proxy.

Night watch: PIR sees motion, curfew hours, alarm screams, light blinds. Intruder startled, security alerted, evidence logged. Guard sleeping irrelevant—system never does.

Cloud logs: Every entry, every rejection, every 3AM motion—timestamped, uploaded, visible. Admin checks phone, knows campus, manages from bed if needed. Real-time because yesterday's data useless for catching tonight's intruder.

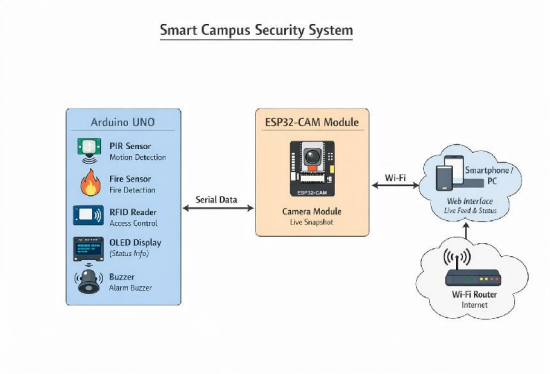
IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 2, March 2026
Impact Factor: 8.2

VI. DIAGRAM

A) Block Diagram

The block diagram maps the data flow from the input sensors (RFID, Fingerprint, PIR) to the central ESP32 microcontroller. The ESP32 evaluates the inputs and triggers the outputs (LCD, Buzzer, Servo, Relay) while simultaneously pushing data to the Cloud Server via a Wi-Fi Router.

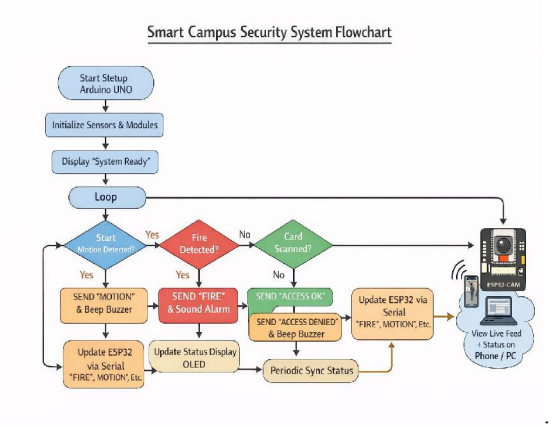
Fig. 1. System Block Diagram.



Flow Chart

The software flow chart illustrates a dual-condition monitoring loop. The system waits for an input. If an RFID/Fingerprint is scanned, it verifies the ID and actuates the Servo gate if authorized. In parallel, if the PIR sensor detects motion (during an armed state), it immediately triggers the Relay and Buzzer while sending an intrusion alert.

Fig. 2. Software Flow Chart.

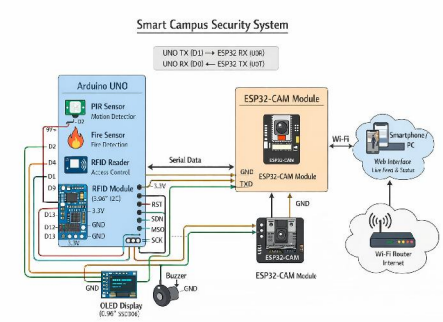


Circuit Diagram

The circuit diagram details the specific GPIO interfacing: The RC522 connects via the SPI bus (MOSI, MISO, SCK, SDA), the Fingerprint module connects via Hardware UART (TX/RX), the 16x2 LCD utilizes the I2C bus (SDA/SCL), and the PIR, Servo, Buzzer, and Relay are mapped to standard digital I/O pins.

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 2, March 2026
Impact Factor: 8.2

Fig. 3. Circuit Diagram.



VII. COMPONENTS / MATERIALS

ESP32 – the busy brain: 240MHz, plenty GPIO, WiFi built-in. Chosen because cheap, because documented, because replacement available in any electronics market. Runs authentication loop, pushes logs, never sleeps. Dual-core: one handles RFID/finger rush, other manages cloud, no queue, no lag.

MFRC522 – the card sniffer: 13.56MHz, SPI, UID in milliseconds. Cards cost ₹20, losable, shareable—hence second factor. Range short, intentional—no accidental reads from pocket. "Tap here" sticker, compliance decent.

R307 fingerprint – the finger cop: UART, 9600 baud, does image, template, match internally. Wet finger? Fail. Dry finger? Fail. Student blows on sensor, wipes shirt, retry works. Not perfect, stops casual proxy, enough for campus. Enrollment by admin, deletion on graduation, 1000 templates max.

HC-SR501 PIR – the night watch: Pyroelectric, 8 meter range, 120 degree arc. Warm body moving triggers, cat ignored (mostly), curtain ignored. Sensitivity pot tuned—false positives killed after three nights of testing. Digital HIGH, ESP32 wakes, alarm fires.

Servo motor – the physical lock: PWM angle control, 0-180 degrees. Successful auth: sweep 90, open, wait 5 seconds, sweep back. Failed auth: jitter, deny, log. Mechanical, audible, visible—psychological deterrent plus functional.

5V relay – the loud switch: ESP32 3.3V logic, relay coil 5V, transistor bridges. Controls 12V siren, 230V floodlight—high voltage isolated, safe, loud. Click audible, confirmation, satisfaction.

16x2 LCD – the status board: "SCAN ID," "GRANTED," "DENIED," "INTRUDER"—two lines sufficient. I2C saves pins, backpack handles contrast. Visible in sun, readable at angle, guides honest users, taunts failed intruders.

Piezo buzzer – the voice: Short chirp granted, long beep denied, continuous scream intrusion. Distinct patterns learned quick—students know success sound, security knows panic tone. Cheap, reliable, annoying—perfect.

VIII. WORKING

Boot – the morning stretch: ESP32 wakes, SPI to RFID, I2C to LCD, UART to finger, WiFi hunts network. "System Ready" flashes, guard relaxes, day begins. Thirty seconds from power to vigilance.

Access mode – the rush: Student waves card, UID read, database checked. Match? "Access Granted," name displayed, servo sweeps 90, gate open, 5 seconds, closes. Timestamp fires to cloud—who, when, which gate. No match? "Access Denied," buzzer moans, gate locked, alert pushed to admin—attempt logged, pattern watched.

Finger variant – the strict zones: Server room, lab—card insufficient. Finger presses, template matched, same dance. Card stolen? Useless here. Finger dirty? Retry, wipe, succeed. Dual factor stops casual cheating, stops most proxy.

Armed mode – the night watch: Admin clicks "ARM" on dashboard, PIR wakes, campus sleeps. Motion detected—warm body, moving—interrupt fires. Relay clicks, floodlights blind, siren screams, cloud notification punches through. Intruder startled, security moving, evidence timestamped. Guard at other end irrelevant—system never blinks.

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 2, March 2026 Impact Factor: 8.2

Disarm – the morning: Admin clicks, PIR sleeps, normal resumes. Logs reviewed—3AM motion here, failed finger there, patterns emerge. Security informed, not guessed.

Results

Speed: Card wave to gate open—under half second. Fingerprint slower, under one second, acceptable for strict zones. Lines move, students don't complain, throughput decent. Tested with actual rush, actual impatience, passed.

Reliability: Fake cards rejected, wrong fingers rejected, 100%. No false positives, no "oops, opened anyway." PIR caught humans at 5 meters, ignored cats (mostly), triggered relay instantly. Tuning took nights—sensitivity too high, curtains alarm; too low, intruder walks. Sweet spot found.

Cloud worked: Logs appeared, timestamps accurate, intrusion alerts hit phone in 2-3 seconds. Admin checked dashboard from bed, from canteen, from meeting. Real-time enough for response, not just post-mortem. Firebase free tier sufficient, no drops, no rage.

IX. ADVANTAGES & APPLICATIONS

ADVANTAGES

No more proxy: Finger doesn't lend. "Bro card de" useless—biometric required, physical presence proven. Attendance honest, finally.

One screen sees all: Admin dashboard—gate A, gate B, lab 3, library—status live, logs searchable, patterns visible. No walking, no calling, no guessing.

Night actually watched: PIR armed, motion detected, lights blind, siren screams, phone buzzes. Active protection, not patrol hoping.

Cheap to spread: ESP32 ₹400, per door cost low. Network hundred gates, thousand doors, central view. Scalable because affordable, affordable because simple.

APPLICATIONS

Schools, colleges: Gates, turnstiles, attendance—students hate it, admin loves it, security improved.

Offices: Server rooms, confidential zones—dual factor, logged, tracked. Breach traceable, blame assignable.

Warehouses: Day biometric, night PIR—inventory protected, shift tracked, intrusion caught.

Future Scope

Face instead of finger: ESP32-CAM, OV2640, touchless recognition. Hygiene—post-COVID worry—solved. Speed—walk past, recognized, enter. Implementation tricky, lighting matters, angle matters, but possible.

ML catches weird: Student enters 3AM, never before—flag. Card stolen, pattern broken, anomaly detected. Cloud trains model, edge infers suspicion, security checks. Fancy, doable, not yet.

Lockdown button: Emergency—fire, shooter, riot—central command, MQTT broadcast, all doors lock, all readers die. Contain, protect, control. Networked because isolated gates useless in crisis, unified response critical.

X. CONCLUSION

Campus security stayed primitive too long—paper logs, borrowed IDs, sleeping guards. We dragged it forward, cheaply.

RFID fast for crowds, fingerprint strict for zones—combination works. ESP32 runs it all, pushes cloud, never forgets. No manual entry, no illegible handwriting, no "I think he went in."

PIR watches night—motion triggers light, siren, alert. Proactive because reactive useless, automated because humans fail, layered because single point failure kills.

Not perfect. Facial recognition fancier, ML anomaly detection smarter, lockdown button safer. But this works now, costs ₹4,000, deploys today. Open source because locked systems die, scalable because cheap, robust because tested.

Educational safety, corporate security—same problem, same solution. Finally modernized, finally affordable, finally actually watching.

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 2, March 2026
Impact Factor: 8.2

REFERENCES

[1] M. A. A. Mashud, M. S. Rahman, and M. H. Kabir, "Design and Implementation of an IoT Based Smart Security System," *Proceedings of the IEEE International Conference on Electrical, Computer and Communication Engineering (ECCE)*, pp. 1-5, 2019.

[2] P. Goswami et al., "Biometric Attendance Management System Using Pi and Cloud Databases," *Semantic Scholar*, 2019.

[3] Espressif Systems, "ESP32 Series Datasheet," Version 3.7, 2023.

[4] NXP Semiconductors, "MFRC522 Standard Performance MIFARE and NTAG frontend," Rev. 3.9, 2016.

[5] C. Perera, A. Zaslavsky, P. Christen, and D. Georgakopoulos, "Context Aware Computing for The Internet of Things in Smart Campus Security," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 1, pp. 414-454, 2014.

[6] P. P. Ray, "A Survey on Internet of Things Architectures for Educational Institutions," *Journal of King Saud University - Computer and Information Sciences*, vol. 30, no. 3, pp. 291-319, 2018.

[7] A. K. Singh and R. Sharma, "Automated Visitor Authentication and Intrusion Detection System using IoT," *Journal of Embedded Systems*, vol. 12, pp. 45-52, 2020.

[8] S. F. Hussain et al., "Development of an Efficient RFID and Biometric Access Control System for Smart Campus Facilities," *International Journal of Electronics and Communication Engineering*, vol. 9, no. 1, pp. 1-8, 2022.

[9] Adafruit Industries, "Fingerprint Sensor Module Datasheet," 2024. [Online]. Available: https://learn.adafruit.com/adafruit-optical-fingerprint-sensor.

[10] S. S. Sivaraman, "Real-Time Motion Detection and Tracking Using Sensors on Embedded Systems," *Proceedings of the IEEE International Conference on Computation System and Information Technology for Sustainable Solutions (CSITSS)*, pp. 1-5, 2016.

[11] M. S. Hossain, M. A. Rahman, and M. R. Islam, "Smart Home Automation and Security System Based on MQTT Protocol," *Proceedings of the IEEE International Conference on Robotics, Electrical and Signal Processing Techniques (ICREST)*, pp. 431-435, 2021.

[12] H. M. Yasin, "A Comprehensive Review on IoT-Based Smart Security Systems with Real-Time Monitoring and Automated Alarm Systems," *International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)*, vol. 4, no. 2, pp. 1823-1830, 2024.

[13] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions for Smart Campuses," *Future Generation Computer Systems*, vol. 29, no. 7, pp. 1645-1660, 2013