iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** VI **Month of publication:** June 2026

DOI: https://doi.org/10.22214/ijraset.2026.83524

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue VI June 2026- Available at www.ijraset.com

Smart Attendance System: A Two-Factor BLE and Biometric Authentication Framework for Academic Integrity

Aditya Kiran Kumbhar, , Tushar Parasharam Mane, Sanket Shrikant Shinde, Avishkar Anil Shinde, Raviraj Uddhav Patil, Jayan Juned Mulla, Ashok Sadavare
Department of Computer Science & Engineering, Shree Santkrupa Institute of Engineering and Technology, Ghogaon, Maharashtra, India

Abstract - Attendance management in educational institutionsremainsachallengingtaskduetoissuessuch as proxy attendance, manual record maintenance, and insecure verification methods. Existing attendance systems based on QR codes, GPS tracking, RFID cards, or basic biometric authentication often fail to provide reliable protection against spoofing and unauthorized attendance marking. This paper presents a Smart AttendanceSystemthatcombinesBluetoothLowEnergy (BLE) proximity verification with AI-based facial authentication to improve security, accuracy, and automation in academic attendance management.

The proposed system uses a two-factor verification mechanism. In the first stage, BLE Received Signal Strength Indicator (RSSI) analysis is used to verify whether the student is physically present within the classroom environment. In the second stage, facial recognitionandlivenessdetectiontechniquesareapplied using TensorFlow Lite and Google ML Kit to confirmtheidentityofthestudent.Theframeworkisimplementedas an Android application using Kotlin, Jetpack Compose,CameraX,FirebaseFirestore,andTensorFlow Lite. Most biometric operations are executed directly on the device to reduce latency and improve user privacy.

The system is designed to minimize proxy attendance, reduce dependence on additional hardware, and provide secureattendancerecordsthroughcloudsynchronization. The proposed architecture offers a cost-effective and scalable solution suitable for modern educational institutions. This paper discusses the system design, implementation methodology, advantages, limitations, and possible future enhancements of the framework.

KeyWords: Attendance System, Biometric Authentication, Bluetooth Low Energy, BLE RSSI, Face Recognition,TensorFlowLite,LivenessDetection,Proxy Attendance, Two-Factor Authentication, Mobile Computing, Android, Firebase Firestore, FaceNet, Google ML Kit, Academic Integrity.

I. INTRODUCTION

Attendance management is an essential part of academic institutions because it helps maintain discipline, evaluate student participation, and monitor academic progress. Traditional attendance methods such as manual roll calls and paper-based registers consume valuable lecture time and are highlyvulnerabletoproxyattendanceandrecordmanipulation. In large classrooms, maintaining accurate attendance records becomes even more difficult for faculty members.

To improve efficiency, many institutions have adopted digital attendance systems based on technologies suchasQRcodes,GPStracking,RFIDcards,andbiometric authentication.Althoughthesesystemsreducemanualwork, theystillfaceseveralsecurityandreliabilitychallenges.QR-code systems can be bypassed through screenshot sharing, GPS-based systems are vulnerable to mock-location applications, and RFID cards may be exchanged between students. Similarly, simple facial recognition systems without liveness verification can be deceived using photographs or pre-recorded videos.

Recentdevelopmentsinmobilecomputing,Bluetooth Low Energy (BLE), and edge-based artificial intelligence have created opportunities for building more secure and cost-effectiveattendancesystems.BLEtechnologyprovides reliable short-range communication with low battery consumption, making it suitable for indoor proximity verification. At the same time, TensorFlow Lite and mobile AI frameworks allow facial recognition models to run directly on smartphones without requiring continuous cloudprocessing.

This research proposes a Smart Attendance System that combines BLE-based proximity verification with AI-powered facial authentication. The proposed frameworkuses a two-factor verification process.

The first factor verifies whether the student is physically present inside the classroomareausingBLERSSIsignalanalysis.Thesecond factor confirms the identity of the student using facial recognitionandlivenessdetectiontechniques.

Bycombining these two verification stages, the system reduces the possibility of proxy attendance, location spoofing, and biometric spoofing attacks.

ThesystemisimplementedasanAndroidapplication using Kotlin, Jetpack Compose, CameraX, Firebase Firestore, TensorFlow Lite, and Google ML Kit. The architecture is designed to work on standard smartphones without requiring expensive external hardware. Attendance recordsaresecurelystoredinFirebaseFirestore,whilemost biometricprocessingoperationsareperformedlocallyonthe user's device to improve privacy and reduce latency.

Themainobjectiveofthisworkistodevelopasecure, scalable, and user-friendly attendance management frameworksuitableformoderneducationalinstitutions.The proposedsystemaimstoimproveattendancereliability, reduce administrative workload, and provide a practical solutionforacademicenvironmentswhereproxyattendance remains a significant issue.

Theremainderofthispaperisorganizedasfollows.Section II discusses the literature review and research gap analysis. Section III explains the objectives of the proposed system. Section IV presents the system architecture and workflow. Section V describes implementation details and technologies used in development. Section VI discusses advantages and limitations, while Section VII presents future enhancements. Finally, Section VIII concludes the paper.

II. LITERATURE REVIEW AND RESEARCH GAP ANALYSIS

The rapid growth of mobile computing and smart technologies has encouraged educational institutions to adopt digital attendance systems for improving efficiency and reducing manual work. Researchers have proposed multiple attendance management approaches using technologies suchas RFID, QR codes, GPS tracking, biometric authentication, andwirelesscommunicationsystems.Althoughthesemethods improve attendance automation, many of them still face security,reliability,andscalabilitychallenges.

A. Traditional and Existing Digital Attendance Systems

The continuous expansion of mobile computing capabilities alongsidesmartinfrastructurehasdrivenacademicinstitutions toward automated alternatives for recording student participation. Historically, conventional documentation relied on manual roll calls or paper ledger systems handled directly byinstructors.Theselegacyapproachessignificantlydecrease active instructional time, exhibit high vulnerability to human reporting errors, and fail to prevent unauthorized proxy attendance. In large lecture halls, manual logging becomes entirelyinefficientanderror-prone.Toaddressthesestructural bottlenecks, introductory automated solutions emerged utilizing Radio Frequency Identification (RFID) networks. In an RFID configuration, individuals present physical transponder cards to specialized reading devices positioned at classroomperimetersorcampusentrances.Whilethisshortens the transactional logging time, it demands expensive infrastructural outlays and continuous terminal maintenance. Furthermore, physical card sharing remains a major security vulnerability, allowing present students to easily falsifyattendance records for absent peers.To mitigate high hardware requirements, developers shifted toward Quick Response (QR) code platforms due to their easeof deployment on personal mobile devices. Instructors typicallyprojectatime-sensitiveQRtokenthatstudentsscanviacustom mobile software. However, as discussed later in Sec. 2.1.3, these frameworks fail to ensure genuine physical presence sincedigitalimagesofthetokencanbeeffortlesslydistributed via instant messaging platforms to off-site locations, allowing absent individuals to register attendance. Alternatively, telemetry data from the Global Positioning System (GPS) has been utilized by researchers to enforce strict geographic barriers. Although GPS tracking handles outdoor boundaries adequately,itssignalfidelitydropssignificantlywithinmodern multi-story academic buildings and dense campus layouts. In addition, current mobile operating systems allow users to exploit mock-location tools to fake telemetry information, making GPS-restricted platforms highly susceptible to location-spoofing attacks.

B. BluetoothLowEnergyandBiometricSolutions

Tocircumventthearchitecturalconstraintsofindoor localization, Bluetooth Low Energy (BLE) technology offers an energy-efficient paradigm for short-range device interactions.ByreadingtheReceivedSignalStrengthIndicator (RSSI)valuefromalocalized wirelessbeacon,clientsoftware canestablishareliableproximitythresholdinsideaclassroom. Priorinvestigationsdemonstratet hatBLEpositioningprovides far superior indoor precision compared to satellite alternatives in educational spaces. Because modern consumer devices possess integrated BLE transceivers natively, the framework functions smoothly without requiring external hardwareinstallations.

Concurrently, biometric parameters such as fingerprint scanning and computerized facial validation have been explored to ensure authentic student identity. Fingerprint architectures offer robust verification but recreate the problem of expensive peripheral procurement and installation constraints.Automatedfacialanalysisrepresentsacontactless, frictionless alternative. The introduction of compressed execution runtimes like TensorFlow Lite (TFLite) along with lightweight deep learning networks—including FaceNet and MobileNet—permits high-dimensional embedding extraction to run directly on the client handset. Nevertheless, baseline visionframeworksremainvulnerabletofacialspoofingattacks carried out via printed photographs or digital video playbacks. Researchers mitigate these presentation threats by incorporating dynamic liveness checking strategies, which monitorhuman-specificindicatorslikeocularblinking,smiling expressions, structural landmark variances, and multi-axis headrotations.Combiningstructuralpositionlogswithunique biometrics yields multi-factor validation architectures; yet, existing iterations remain restricted due to a heavy reliance on continuous cloud processing or cost-intensive externalhardware arrays.

C. Identified Research Gaps

Asystematiccritiqueofcurrentacademicliteratureexposes severalcriticalvulnerabilitiesacrosslegacyanddigital architectures. First, a major portion of contemporary solutions dependsexclusivelyonasinglevalidationlayer,which inherentlyintroducessingle pointsoffailureforspoofingor proxybehavior.Second,satellitepositioningtechniques remaindeeplyimpreciseindoor sandareroutinely manipulated via simple software-based coordinate overrides. Third, visual matrix tokens lack room-level confinement properties due to their ease of remote transmission. Fourth, both RFID systems andlegacyfingerprinttopologiesnecessitatesubstantialcapital investmentsforspecializedlocalizedreaders,limitingscalabilityinresource-constrainedenvironments.Fifth,deployed automated face verification systems frequently lack real-timelivenessinspectionlayers,renderingthemhelplessagainst physical presentation attacks.Mostimportantly,thereisanevidentlackofresearchexploringtheconvergenceofBLERSSIbasedroomboundaryverificationwithedgecomputedArtificialIntelligence(AI)facialclassificationinsideaunified,clientsidemobileecosystem.Extantframeworksfailtoexploitlocalsmartphone environmentstoprocesssensitivebiologicaltemplates, creatingmassivecloudoverheadandintroducing security exposures.Section2.1outlinesthesefundamentalvoids,which the proposed Smart Attendance System directly addresses by mergingshort-rangenetworktelemetry,on-deviceneuralinferencing,andliveinteractionchallengesintoascalable, secure,andcompletelyhardware-independentframework.

III. SYSTEM OBJECTIVES -

The development of the Smart Attendance System is guided by five primary architectural and operationalobjectives:

A. SecurityandIntegrityGoals

The foremost directive of this framework is the absolute mitigation of proxy attendance and the presentation vulnerabilities highlighted in Sec. 2.1. To accomplish this, the architecture is specifically engineered to guarantee a False Acceptance Rate (FAR) of strictly less than 0.1 percent. This uncompromising security threshold is operationalized through a mandatory Two-Factor Attendance Protocol (TFAP). By requiring the simultaneous satisfaction of localized proximity constraints and live biometric validation, the system theoretically and practically eliminates systemic attendancefraud.

B. ExecutionEfficiencyandTechnicalGoals-

Despite introducing advanced cryptographic and biometric layers, the platform must remain frictionless to avoid consuming valuable instructional time. Consequently, the primary efficiency benchmark limits the entire verification sequence—from the initial proximity handshake to the finalgraphicalconfirmation—toamaximumdurationof15seconds.This metric ensures the workflow remains temporally competitivewithlegacydigitaltokensystemswhileproviding vastly superior data integrity.

To meet these stringent execution speeds, the system completely decentralizes its core biometric processing. A dedicated TensorFlow Lite (TFLite) machine learning model is embedded natively within the mobile application environment. This edge-computing paradigm allows for instantaneous facial embedding generation and identity validation—calculated via a Cosine Similarity mathematical model—without relying on continuous cloud connectivity. By offloading these heavy processing tasks to the client device, the architecture prevents server bottlenecks during peak concurrent check-ins. Finally, all resulting verification logs and metadata are securely synchronized with a FirebaseFirestore cloud architecture, where strict role-based governanceprotectstheconfidentialityofstudentrecords.

IV. PROPOSED SYSTEM ARCHITECTURE

The Smart Attendance System (SAS) is designed as a securemobile-basedattendancemanagementframework that combines Bluetooth Low Energy (BLE) proximity verification with AI-powered biometric authentication. The architecture follows a client-server model where Androidsmartphonesactasbothattendancedevicesand

TheSmartAttendanceSystem(SAS)isdesignedasa securemobile-basedattendancemanagementframework that combines Bluetooth Low Energy (BLE) proximity verification with AI-powered biometric authentication. The architecture follows a client-server model where Androidsmartphonesactasbothattendancedevicesand verification nodes, while Firebase Firestore provides centralized cloud data storage.

Theproposedarchitectureconsistsofthreemajorcomponents:

- TeacherDevice(BLE Advertiser)
- StudentDevice(BLEScannerandBiometricClient)
- FirebaseFirestoreBackend

The complete system workflow is based on a Two-FactorAttendanceProtocol(TFAP),whereattendanceis marked only after successful completion of both proximityverificationandbiometricidentityverification.

A. TeacherDeviceConfiguration(BLEAdvertiser)

A lecture, the instructor's smartphone operates as a BLE advertiser. Upon initiating an attendance session, the application begins broadcasting a unique Service Universally Unique Identifier (UUID) utilizing Android's native BLE advertising Application Programming Interfaces (APIs). To establish a strict classroom verification zone, the transmission powerisdeliberatelyconstrainedtoamediumsetting,limiting the signal radius to approximately 5–10 meters. This configurationensuresthatdeviceslocatedoutsidethephysical classroom receive degraded signal strengths and subsequently failproximitychecks.Theinstructor'sdevicemanagessession states, broadcasts these localized packets, and synchronizes finalattendancedatawiththecloudbackendwithoutrequiringany external beacon hardware.

B. Student Device Configuration (BLE Scanner and Client)

The student's smartphone operates dually as a BLE scanner and an edge-computing biometric client. When a student attempts to log their presence, the mobile application actively scans the immediate environment for the instructor's specific BLEUUID.IfthedetectedReceivedSignalStrengthIndicator (RSSI) meets the required proximity threshold, the device immediately transitions to biometric validation. The application engages the front-facing camera, performing liveness detection and facial embedding generation locally via TensorFlow Lite and Google ML Kit. By executing these sensitive biological comparisons entirely on the client device, thearchitecturedrasticallyreducesserverlatencyandpreserves user privacy, as raw facial imagery is never continuouslytransmitted t external servers.

C. Firebase Firestore Backend Structure

Firebase Firestore serves as the centralized NoSQL database for the platform, securely housing session metadata, student profiles, and historical attendance logs. The backend is structured into three primary collections: the Students Collection(storingenrollmentdata,historicalpercentages,and registered facial embeddings), the Sessions Collection (recording subject details, instructor information, and BLE session identifiers), and the Attendance Records Collection (logging individual verification timestamps, RSSI values, and final statuses). Access to these collections is strictly governed by Firebase Authentication and Firestore security rules toprevent unauthorized data manipulation.

D. Two-Factor Attendance Protocol (TFAP)Workflow

The operational core of the system is the Two-Factor Attendance Protocol (TFAP). This protocol mandates a sequential, two-stage verification process. First, the student device must capture a BLE packet with an RSSI value greater than-80dBm,confirmingphysicalproximitytotheinstructor. Second, upon passing the proximity gate, the student must successfully complete randomized liveness challenges (suchasheadmovementorblinking)followedbyasuccessfulfacial identity match against their stored database embedding using Cosine Similarity. An attendance record is committed to the Firestore backend only if both the spatial and biometricconditions are independently satisfied.

V. IMPLEMENTATION DETAILS

The Smart Attendance System (SAS) is implemented as an Android-based mobile application that integrates Bluetooth Low Energy (BLE), facial recognition, liveness detection, and cloud-based attendance management.Thesystemisdesignedtoprovidesecure attendance verification while minimizing hardware dependency and improving user privacy.
The implementation combines Android native technologies, TensorFlow Lite, Firebase Firestore, and Google ML Kit to create a real-time attendancemanagementframework.

A. Android Application and Technology Stack

The Smart Attendance System (SAS) framework is materialized as a native mobile application programmed in Kotlin within the Android Studio environment. The graphical user interface is constructed utilizing Jetpack Compose to deliveraresponsiveandmodernuserexperience.Thesystem's underlyingarchitectureishighlymodular,compartmentalizing core functions such as secure data syncing (Firebase), local visualprocessing(CameraXandGoogleMLKit),andartificial intelligence operations (TensorFlow Lite). By keeping these operationalmodulesfunctionallydistinct,theplatformensures long-term maintainability and allows for the straightforward integration of future upgrades without requiring system-wideoverhauls.

B. BLE Proximity Verification and DistanceEstimation

For classroom localization, the platform heavily utilizes Android's native Bluetooth Low Energy (BLE) Application Programming Interfaces (APIs). The instructor's module utilizes the BluetoothLeAdvertiser class to transmit a session-specific Universally Unique Identifier (UUID). Thistransmission is configured withADVERTISE_MODE_BALANCED and ADVERTISE_TX_POWER_MEDIUM parameters to deliberately confine the signal radius to 5–10 meters. Conversely, the student module employs theBluetoothLeScanner class with a SCAN_MODE_LOW_LATENCY configuration to actively seek this exact UUID. Upon packet interception, the system evaluates the Received Signal Strength Indicator (RSSI). The spatial distance between the devices is mathematicallyestimated using Eq. 1:
Distance=10^[(TxPower-RSSI)/(10×n)]

C. Camera Processing and Liveness Detection

Following successful spatial validation, the application automaticallytriggersthefront-facingcameraviatheCameraX pipeline. To maintain real-time analysis speeds and avoid processing bottlenecks, the frame buffer is explicitly set to STRATEGY_KEEP_ONLY_LATEST. Liveness verification issubsequentlyexecutedusingtheGoogleMLKitframework. The application prompts the user to perform randomized physical actions—such as lateral head rotations, ocular blinking, or smiling—while analyzing facial landmarks and Euler angles in real time. To further safeguard against presentation attacks utilizing miniature digital displays or distant printed photographs, the dimensional proportion of the faceiscalculatedasshowninEq.2: Face Area Ratio = [Face Bounding Box Area] / [Total FrameArea]An abnormally low ratio instantly flags the interaction as apotential spoofing attempt.

D. TensorFlowLiteFaceRecognitionIntegration-

Once liveness is verified, the captured frame undergoes morphological preprocessing, including facial cropping, dimensional resizing, and pixel normalization. A lightweight FaceNet model executed via TensorFlow Lite (TFLite) processesthisnormalizedinputtoextracta128-dimensional biometric embedding vector. This newly generated vector is computationally compared against the student's authorized baseline embedding retrieved from the cloud database. The comparative analysis utilizes the Cosine Similarity metricdefined in Eq. 3:
CosineSimilarity=(A·B)/(||A||×||B||)
whereAistheliveembeddingvector and Bisthe registered enrollment vector. As outlined previouslyinSec.2.2.1,the validationstrictlyrequires asimilarityscore of≥0.85 toofficiallymark the student as present.

E. Firebase Database Integration and SecurityRules -

The entire backend infrastructure is hosted on Firebase Firestore, a highly scalable NoSQL cloud environment. The database schema is logically divided into three primary collections: Students, Sessions, and Attendance Records. The Students collection retains enrollment data and biometric embedding arrays, the Sessions collection tracks live and historical lecture metadata, and the Attendance Records collection immutably logs temporal stamps, spatial RSSI values,andvalidationoutcomes.

Toensurestrictdataprivacy, Firebase Authentication is paired with customized Firestore Security Rules, completely preventing unauthorized endpoint access. Furthermore, because the heavy biometric computations detailed in Sec. 2.4.4 occur locally on the edge device, sensitive facial imagery is never transmitted to the cloud, significantly reinforcing user privacy compliance. Finally,theapplicationdynamicallymanagesAndroidruntime permissions, gracefully handling user denials withouttriggering application crashes.

VI. ADVANTAGES,LIMITATIONS,ANDFUTURESCOPE -

The Smart Attendance System (SAS) offers substantial advantages over traditional and existing digital attendance methods by integrating BLE-based proximity tracking with AI-powered facial authentication. This dual-factor approach significantly enhances attendance security, reduces administrative burdens, and optimizes operational efficiency withineducationalinstitutions.However,despitethesecritical advancements in automation, the proposed framework possesses several practical and technical limitations that must becarefullyevaluatedpriortoreal-worlddeployment.

A. System Advantages and Security Benefits

The integration of these dual verification stages provides substantial operational and security improvements over traditional methods. Primarily, the architecture successfully eradicates proxy attendance by strictly enforcing physical proximitythroughBLElocalization.Furthermore,itinherently resistsbothGPSspoofingandadvancedbiometricpresentation attacks. Because the validation sequence executes entirely on edge devices, the platform operates without requiring expensive, dedicated external hardware. This local execution ofAImodelsalsofortifiesuserprivacy,asrawbiologicaldata never leaves the handset. Finally, as established in Sec. 2.2.2, the entire verification transaction is consistently completed in under 15 seconds, ensuring high execution efficiency duringlecture hours.

B. HardwareandEnvironmentalLimitations-

Despiteitsrobustsecurityprofile,theframeworkissusceptible tospecificenvironmentalandhardware-centricconstraints.

BLE signal propagation can experience significant variability due to structural obstructions, such as thick concrete walls, or signal absorption from dense human crowds, occasionally resulting in false proximity rejections. Additionally, the system's operational consistency is heavily reliant on the hardware specifications of the student's smartphone. Devices with inferior camera optics or limited processing units may struggletoexecutetheTFLitemodelsrapidly.Lastly,although biometric computations occur entirely offline, the current architecture still requires a stable internet connection to synchronizethefinalattendancelogswiththecloudbackend.

C. Future Enhancements

To mitigate the aforementioned limitations and broaden the system's applicability, several developmental enhancements are proposed. Future iterations will focus on transitioning the native Android codebase to a cross-platform framework, specifically Flutter, to provide native support for iOS devices. To address classroom connectivity issues, the implementation of localized offline caching with asynchronous cloud synchronization is planned. Furthermore, integrating adaptive signal calibration algorithms could dynamically adjust the proximity thresholds based on real-time environmental interference. Finally, establishing API bridges to directly synchronize the authenticated data with broader university Enterprise Resource Planning (ERP) databases will significantlystreamlineadministrativeworkflows.

VII. CONCLUSIONS

This research presented a unified Smart Attendance System (SAS) engineered to resolve the persistent vulnerabilities of proxy reporting, location spoofing, and administrative inefficiency prevalent in modern educational institutions. By abandoning legacy singular-validation methods—such as vulnerable QR codes, inaccurate indoor GPS, and cost-prohibitive RFID infrastructure—this study successfully introduced a decentralized, Two-Factor Attendance Protocol(TFAP).

The proposed architecture effectively bridges spatial and biological verification through edge-computing mobile devices. Utilizing native Bluetooth Low Energy (BLE) Application Programming Interfaces, the framework establishes a localized, hardware-independent classroom perimeter, enforcing a strict presence threshold of RSSI > -80 dBm. Following this spatial validation, the integration of TensorFlow Lite and Google ML Kit facilitates advanced liveness detection and local facial embedding extraction. By mathematically confirming student identities against cloud-registeredtemplatesusingCosineSimilarity(where$A \cdot B / \|A\| \times \|B\| \geq 0.85$), the system practically eliminates biometricpresentation attacks.

Implemented natively on Android with a secure Firebase Firestore backend, the SAS provides a highly scalable and cost-effective alternative to traditional attendance systems. While minor operational constraints exist regarding environmental BLE signal variability and mobile hardware dependencies, the foundational architecture demonstrates profoundimprovementsindataintegrityandprocessingspeed (consistentlyoperatingunder15seconds). Ultimately, this dual-layer verification framework illustrates the significant potential of merging short-range network telemetry with localized artificial intelligence. It delivers a robust, transparent, and privacy-compliant solution that minimizes administrative overhead while rigorously securingacademic integrity.

{ online version of the volume will be available in LNCS Online.MembersofinstitutessubscribingtotheLectureNotes inComputerScienceserieshaveaccesstoallthepdfsofallthe online publications. Non-subscribers can only read as far as the abstracts. If they try to go beyond this point, they are automatically asked, whether they would like to order the pdf, and are given instructions as to how to do so.

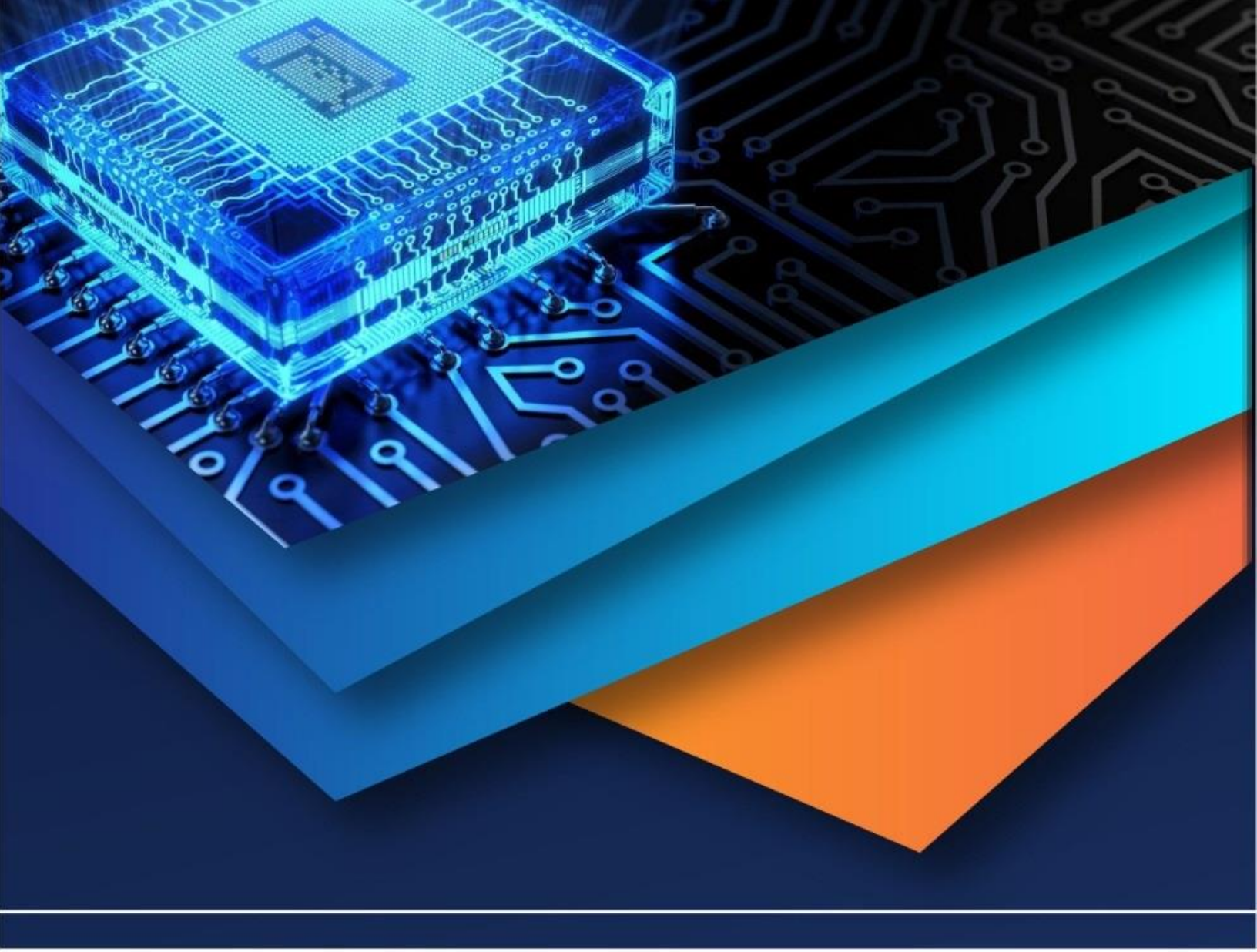
VIII. ACKNOWLEDGEMENT

We would like to express our profound gratitude to the Department of Computer Science & Engineering at Shree SantkrupaInstituteofEngineeringandTechnology,Ghogaon, for providing the essential resources, laboratory facilities, and academic environment required to successfully complete this research. We are deeply thankful to our faculty mentors and project guides for their continuous encouragement, technical insights, and valuable feedback throughout the development and testing of the Smart Attendance System. Furthermore, we extend our sincere appreciation to the college administration for their unyielding support. Finally, we would like to thank our peers and families for their constant motivation during the course of this project.

REFERENCES

[1] M. A. Raza, M. Akhtar, S. Akhtar, and M. A. Khan, "A review of intelligent attendance systems using machine learning and deep learning,"Int.J.Adv.Comput.Sci.Appl.,vol.13,no.4,pp.1–12,2022.
[2] S. B. Kotsiantis, C. Pierrakeas, and P. E. Pintelas, "Predicting students' performance in distance learning using machine learning techniques,"Appl.Artif.Intell.,vol.18,no.5,pp.411–426,2004.
[3] V. S. Dhaka and S. Sinhal, "Biometric attendance system to preventproxyattendanceineducationalinstitutions,"inProc.2nd Int.Conf.Comput.Commun.Technol.(ICCCT),Allahabad,India, 2011, pp. 756–759.
[4] N. P. Patidar, R. Agrawal, and P. Sharma, "Smart attendance management using biometric system and internet of things,"in Proc. Int. Conf. Emerg. Technol. (ICET), Jaipur, India, 2020, pp.1–5.
[5] A. El-Rabbany, Introduction to GPS: The Global Positioning System, 2nd ed. Norwood, MA, USA: Artech House, 2006.
[6] K.Jain,A.Ross,andS.Prabhakar,"Anintroductiontobiometric recognition," IEEE Trans. Circuits Syst. Video Technol., vol. 14, no. 1, pp. 4–20, Jan. 2004.
[7] K. Nambiar, "RFID technology: A review of its applications," in Proc. World Congr. Eng. Comput. Sci. (WCECS), San Francisco, CA, USA, 2009, vol. 2, pp. 1–5.
[8] G.A.Akintola,O.A.Akinde,andA.S.Alatishe,"Aweb-based students' attendance management system," Int. J. Sci. Technol. Res., vol. 2, no. 7, pp. 164–168, Jul. 2013.
[9] H. F. Lin, "Attendance management system using QR code,"in Proc. IEEE Int. Conf. Consum. Electron.-Taiwan (ICCE-TW), Nantou, Taiwan, 2017, pp. 193–194.
[10] Y.JavedandM.Khan,"GPSbasedstudentattendancesystem," in Proc. 10th Int. Conf. Digit. Inf. Manage. (ICDIM), Jeju, South Korea, 2015, pp. 100–103.
[11] P. Davidson and R. Piché, "A survey of selected indoor positioning methods for smartphones," IEEE Commun. Surv. Tutor., vol. 19, no. 2, pp. 1347–1370, 2nd quart. 2017.
[12] H.Liu,H.Darabi,P.Banerjee,andJ.Liu,"Surveyofwireless indoor positioning techniques and systems," IEEE Trans. Syst. Man Cybern. C Appl. Rev., vol. 37, no. 6, pp. 1067–1080, Nov.2007.
[13] R. Harle, "A survey of indoor inertial positioning systems for pedestrians," IEEE Commun. Surv. Tutor., vol. 15, no. 3, pp. 1281–1293, 3rd quart. 2013.
[14] F. Zafari, A. Gkelias, and K. K. Leung, "A survey of indoor localization systems and technologies," IEEE Commun. Surv. Tutor., vol. 21, no. 3, pp. 2568–2599, 3rd quart. 2019.
[15] R. Faragher and R. Harle, "Location fingerprinting with Bluetoothlowenergybeacons,"IEEEJ.Sel.AreasCommun.,vol. 33, no. 11, pp. 2418–2428, Nov. 2015.
[16] P. Spachos and K. N. Plataniotis, "BLE beacons for indoor positioningataninteractiveIoT-basedsmartmuseum,"IEEESyst. J., vol. 14, no. 3, pp. 3483–3493, Sep. 2020.
[17] F. Schroff, D. Kalenichenko, and J. Philbin, "FaceNet: A unified embedding for face recognition and clustering," in Proc. IEEE Conf. Comput. Vision Pattern Recognit. (CVPR), Boston, MA, USA, 2015, pp. 815–823.
[18] A. G. Howard et al., "MobileNets: Efficient convolutional neural networks for mobile vision applications," arXiv preprint arXiv:1704.04861, 2017.
[19] TensorFlowLite,"TensorFlowLite:On-deviceMLformobile and edge devices," Google LLC. [Online]. Available:https://www.tensorflow.org/lite. [Accessed: Apr. 2026].
[20] Z. Boulkenafet, J. Komulainen, and A. Hadid, "Face anti-spoofing using speeded-up robust features and fisher vector encoding,"IEEESignalProcess.Lett.,vol.24,no.2,pp.141–145, Feb. 2017.
[21] A. Jourabloo, Y. Liu, and X. Liu, "Face de-spoofing: Anti-spoofingvianoisemodeling,"inProc.Eur.Conf.Comput.Vision (ECCV), Munich, Germany, 2018, pp. 290–306.

[22] P. Mell and T. Grance, The NIST Definition of Cloud Computing, NIST Special Publication 800-145, Gaithersburg, MD, USA: National Institute of Standards and Technology, 2011.
[23] S. Bhatt and R. Bhatt, "Multi-factor authentication for smart campusattendance:Acasestudy,"J.Comput.Educ.,vol.8,no.2,pp. 233–251, Jun. 2021.
[24] M. A. Khan, F. Algarni, and M. T. Quasim, "A decentralised IoT-based authentication system with multi-factor biometric verification for smart cities," IEEE Access, vol. 8, pp. 127298–127308, 2020.
[25] T.PadmaandT.Kanimozhiselvan,"Asurveyonmobilebased attendancemanagementsystems,"inProc.3rdInt.Conf.Commun. Electron. Syst. (ICCES), Coimbatore, India, 2018, pp. 816–821.
[26] EuropeanParliamentandCouncil,"Regulation(EU)2016/679 of the European Parliament and of the Council (General Data Protection Regulation)," Official Journal of the European Union,L 119, pp. 1–88, May 2016.
[27] A. G. Howard et al., "Searching for MobileNetV3," in Proc. IEEE/CVF Int. Conf. Comput. Vision (ICCV), Seoul, South Korea, 2019, pp. 1314–1324.
[28] Google LLC, "Firebase Firestore documentation: Security rules and data modeling," Google LLC. [Online]. Available: https://firebase.google.com/docs/firestore. [Accessed: Apr. 2026].
[29] Google LLC, "ML Kit: Face detection API documentation,"Google LLC. [Online]. Available: https://developers.google.com/ml-kit/vision/face-detection.[Accessed: Apr. 2026].
[30] Android Developers, "Bluetooth low energy overview,"Google LLC. [Online]. Available: https://developer.android.com/guide/topics/connectivity/bluetooth /ble-overview.[Accessed:Apr.2026].



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY