AI Based Attendance System Using GeoFencing

Mr. Danish Idrisi[1], Mr. Kaustubh Patil[2], Mr. Sabir Shaikh[3], Mr. Kundan Bhagat[4], Mr.Sarfaraz Tazak[5], Mr. Ali Karim Sayed[6]

[1,2,3,4]*Student AIML, Anjuman-I-Islam's A. R. Kalsekar Polytechnic, New Panvel*

[5]*Lecturer AIML, Anjuman-I-Islam's A. R. Kalsekar Polytechnic, New Panvel*

[6]*Head of the Department Anjuman-I-Islam's A. R. Kalsekar Polytechnic, New Panvel*

***Abstract* - The proposed approach is to secure attendance monitoring in educational institutions by using artificial Intelligence (AI) system that uses context-awareness. This system combines a probabilistic trust score engine and HMAC-SHA256 cryptographically fingerprinting devices to accurately verify a student's identity and prevent proxy attendance from being attempted. It also protects against GPS spoofing and falsifying the location of a student. Through experiments on our system demonstrated that it provides for a smooth experience for students, reduces attendance fraud, allows for faster attendance session setups, and supports the effective management of attendance in an institutional environment.**

***Keywords*--- Device Fingerprinting, GPS Geofencing, Trust Score Engine, Proxy Attendance Detection, Multi-Factor Verification, Secure Attendance Management.**

I. INTRODUCTION

In educational institutions, attendance management is a critical administrative task. Traditional methods of taking attendance such as paper roll calls are often time-consuming, prone to errors, and can be easily manipulated with "proxy" attendance (have someone else mark you present).

As mobile phones and mobile internet access become more universally available, digital attendance systems are likewise becoming more feasible. However, many existing digital attendance systems continue to utilize a single verification factor (i.e., a QR code or PIN) that can be easily exchanged among students, thus defeating the purpose of a system with a single verification factor.

We developed an AI-powered secure attendance system to address these concerns at A.R. Kalsekar Polytechnic (New Panvel). The innovative attendance system uses a multi-factor verification architecture consisting of four independent signals: (1) HMAC-SHA256 Cryptographic Device Fingerprinting, (2) Three-Tier GPS Geofencing, (3) IP Geolocation Cross-Verification, and (4) Network Anomaly Detection. The four independent validation signals are assessed in parallel and collectively contribute to an aggregated trust score, which autonomously determines whether to approve, flag for verification, or reject an attendance attempt.

An important part of an educational institution's administration is managing their attendance.

Traditional means of capturing attendance such as paper roll calls are time-consuming, susceptible to human error, and easily manipulated through "proxy" attendance. With the growing ubiquity of mobile phones and mobile internet access, digital attendance systems are becoming more common. However, the majority of digital attendance solutions use only one verification factor (QR code or PIN) which are easily exchanged between students, therefore defeating the purpose of a solution with only one verification factor.

A.R. Kalsekar Polytechnic (New Panvel) has adapted an AI-based secure attendance solution to address these aforementioned issues. This attendance system employs four independent signals for capturing attendance: (1) HMAC-SHA256 Cryptographic Device Fingerprint, (2) Three-Tier GPS Geofencing, (3) IP Geolocation Cross-Verification, and (4) Network Anomaly Detection. These four signals are evaluated simultaneously and contribute to an accumulated trust score that independently determines if an attendance attempt is accepted, flagged for verification, or rejected.

II. SYSTEM ARCHITECTURE

The system architecture has been constructed utilizing a multi-layered approach, which integrates device

fingerprinting, GPS validation, and network activity measurement for identifying and validating student attendance attempts. All attendance information is stored in a centralised database comprising six tables: teachers, students, device_fingerprints, lectures, attendances, and security_audit_log. The primary methodology used to ascertain an ongoing cumulative trust score is to determine which signal most strongly indicates fraudulent activity, enabling accurate attendance records even where an individual signal is not conclusive.

A dynamic request handler divides the workload between the FastAPI backend and the React frontend, utilizing asynchronous request processing to allow the dashboard to remain responsive in real-time without being delayed by backend verification computations.

A temporal consistency filter reduces noise generated through repeated and automated submissions, and handles edge cases whereby students lose GPS signal during an attendance attempt, via rate limiting and duplicate attempt detection. This feedback loop smooths the verification process, balancing security strictness with usability.

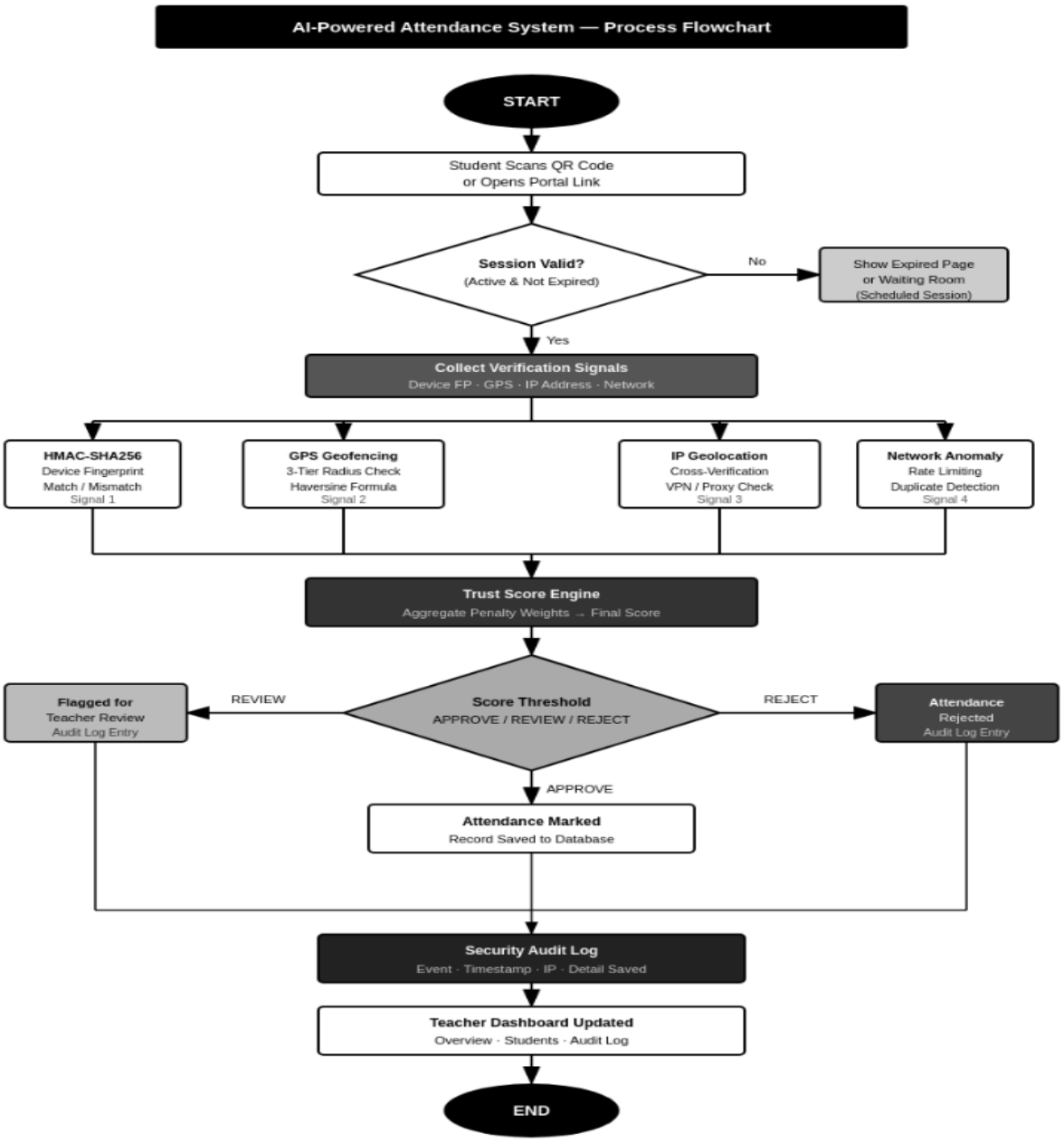

Fig.1. System Flowchart of the AI Based Attendance System Using GeoFencing

III. SECURITY MECHANISMS

A Four-Signal Security Architecture for Attendance Management is established by the collective efforts of four independent verification signals to determine the authenticity of student attendance. The first verification signal is an HMAC-SHA256 device fingerprinting (i.e., hash-based message authentication code), which produces a unique Permanent Device Binding for each student by requiring five browser/hardware attributes (i.e., the user agent string, screen resolution, timezone, WebGL renderer string, and browser language) that must be captured during each attendance attempt. The server-side hash is generated using a unique secret key and is then associated with the student's Permanent Device Binding. An impending FINGERPRINT_MISMATCH penalty will be triggered when there is a mismatch during the subsequent attendance attempts. The second verification signal relies on a 3-Tier GPS geofencing system for verifying the physical presence of students. A student's reported geolocation coordinates will be compared to the teacher's previously registered classroom geolocation coordinates using the Haversine formula (i.e., calculated distance).

Full confidence in the student's attendance status (i.e., TRUSTED attendance) is granted when the distance between the student and classroom geolocation coordinates is less than or equal to 15 meters (Tier 1). The student is then assigned a moderate penalty for distances between 15 meters and 50 meters (Tier 2) and assigned a severe penalty for distances between 50 meters and 100 meters (Tier 3). Any attendance attempts submitted by the student that exceed the maximum geolocation radius of 100 meters will be automatically rejected. IP geolocation cross-verification serves as the third verification signal for determining the student's attendance status. Specifically, the IP-derived location of the student will be cross-verified against the expected campus location. If a VPN is detected, the attendance attempt will be flagged as an IP_GPS_MISMATCH. Proxy or datacenter IP addresses will be flagged as a PROXY_ATTEMPT. Network anomaly detection establishes a fourth verification signal for attendance management by establishing a limiting parameter.

IV. COMPUTATIONAL ARCHITECTURE AND DATA PROCESSING

In Client-Server Architecture, FastAPI does the heavy lifting (back-end) and React does the heavy lifting (front-end). Truly sensitive actions (HMAC-SHA256, trust scoring, geolocation, and database transactions) are completed by the back-end to ensure the integrity of the verification logic and to minimize the risk of being tampered with or reverse engineered.

Once a student submits an attendance request, the verification process for that submission begins. Upon submission, all four verification signals from the student will be sent to the back-end simultaneously, and the back-end will process the verification signals in parallel. A hash will be generated using HMAC SHA 256 based on the submitted browser/hardware info, and it will be compared to the Permanent Device Binding for that student. The physical distance from the student to the registered classroom will be calculated using the Haversine formula to compare the submitted GPS coordinates to the teacher's registered classroom coordinates, and the actual geolocation of the student will be determined using the X-Forwarded-For HTTP request header to extract the student's true IP address and send it to the geolocation service provider.

V. DEPLOYMENT AND INTEGRATION STRATEGIES

The first stage establishes a baseline performance metric (the time it takes for a student to submit a signal and receive a verdict regarding attendance) which will then be used as a reference to measure how different design choices impact this baseline performance metric. The second stage involves a passive validation process whereby the trust score engine is operating in a monitoring mode with respect to flagging events and comparing the results to confirmed records of attendance through an external validation process without requiring any approvals or denials. The third stage introduces active integration in a controlled environment with low volume of traffic.

This will allow the complete four-signal

verification pipeline and asynchronous request processing to occur while preventing the backend verification of attendance calculations from interfering with frontend response times. The fourth stage implements dynamic resource management. The verification pipeline produces consistent response times regardless of how high the load is throughout the entire five phases of stress testing and performing security checks on the pipeline. The fifth phase of the testing process involves performing stress testing on the pipeline and performing security checks, including spoofing GPS coordinates, connecting using a VPN, entering incorrect device fingerprint information and flooding the pipeline with multiple submissions at the same time to ensure that the trust score engine and rate limiting mechanisms function correctly for each of those flows through the system.

In order to maintain consistent performance throughout the life of the system; there is a continuous feedback loop established between the telemetry gathered from the field deployment to the development environment. The majority of the information used by the performance log associated with the back end deployments is used to identify environmental variables that can lead to receiving false positives or extended delays in the verification process.

Therefore, to aid with keeping the penalty weightings balanced, and the tier separation for geofences, you will need to modify these parameters as the conditions in the environment change.

Ultimately, the level of security you have in place during deployment is no less significant than the level of accuracy you have with the kinematic model of the system. As such, it is essential to ensure the stability and responsiveness of your autonomous system through cryptography by verifying the integrity of all sensor data as it is received by your system and maintained within the system for use in estimating the state of the system.

VI. DEPLOYMENT CHALLENGES

The system's introduction to the market brought on various practical challenges across both technical and institutionalized dimensions. Arguably the most significant challenge was the reliability of GPS in indoor environments. The use of classroom environments with thick concrete walls, combined with limited view of the sky, often resulted in the loss of GPS accuracy to more than 100 metres in distance, resulting in students being flagged as displaying GPS_ACCURACY_SUSPICIOUS flags for being legitimate. These challenges required the possible heavy calibration of geofencing tier thresholds and accuracies of the products to create a balance between security strictness and usability under indoor conditions.

Another challenge of usage was the stability of the device fingerprint. Browser updates and operating system changes, as well as the use of privacy policy browsers such as Firefox with an increased focus on Tracking Protection are proven to change 1 or more of 5 of the five device fingerprinting attributes that are utilized on a per-fingerprinting session basis; therefore, legitimate students will frequently trigger FINGERPRINT_MISMATCH penalties. Consequently, a teacher-accessible device reset function was determined to be necessary, to allow historically flagged student(s) to update and re-register their device binding to be able to successfully complete the registration and attendance process without relying on back-end intervention.

A third challenge of concern is network variability issues. Students connecting via mobile data on heavily-congested networks are routinely timed out in their requests intermittently; therefore, students frequently resubmit their request for attendance due to multiple failed attempts and timeouts and submitting duplicate records when performing so. This presented a need to fine-tune current rate-limiting and/or duplicate detection methods to be able to differentiate between legitimate duplicate fraud attempts versus attempts that are generated as a result of network latency issues.

VII. CONCLUSION

This system provides a high-performance base for validating student attendance, by using four independent verification sources that are processed independently through a trust engine so that they are all able to achieve consistent result times and accurate results even when there are chaotic events happening, such as loss of GPS signal or network timeouts. The combination of

location-based awareness, behavioral analysis, and cryptographic security in an entirely software-based system will ensure reliability in overcoming real world problems such as loss of indoor GPS and instabilities in device fingerprints without requiring any additional hardware. In total, this creates a strong foundation for an attendance infrastructure that will actively validate, not just record, attendance, and sets the stage for the adoption of AI-based administrative systems across educational institutions.

ACKNOWLEDGMENT

The authors would like to express their gratitude to Anjuman- I-Islam A.R. Kalsekar Polytechnic, New Panvel, for providing the necessary resources and support for this project. Special thanks to our project guide, Mr. Sarfaraz Tazak, for his invaluable guidance and insights throughout the development of the AI Based Attendance System Using GeoFencing. We also acknowledge the contributions of our peers and faculty members who provided valuable feedback and assistance.

REFERENCES

[1] A. K. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 14, no. 1, pp. 4–20, Jan. 2004. [Online]. Available: https://ieeexplore.ieee. org/ document/1262027

[2] P. Eckersley, "How unique is your web browser?" in *Proc. 10th Int. Conf. Privacy Enhancing Technologies (PETS)*, Berlin, Germany, 2010, pp. 1–18. [Online]. Available: https://coveryourtracks.eff.org/static/browser-uniqueness.pdf

[3] R. Harle, "A survey of indoor inertial positioning systems for pedestrians," *IEEE Communications Surveys and Tutorials*, vol. 15, no. 3, pp. 1281–1293, 2013. [Online]. Available: https://ieeexplore.ieee.org/document/6399492

[4] D. Dasgupta, A. Roy, and A. Nag, "Multi-factor authentication," in *Advances in User Authentication*, Springer, Cham, 2017, pp. 185–233. [Online]. Available: https://link.springer.com /chapter/10.1007/978-3-319-58808-7_5

[5] S. Kiyomoto, T. Fukushima, and T. Tanaka, "A security and privacy analysis of attendance management systems," in *Proc. IEEE Int. Conf. Trust, Security and Privacy in Computing and Communications*, 2011, pp. 1–8. [Online]. Available: https:// ieeexplore.ieee.org/document/6120843

[6] A. K. Awasthi and S. Lal, "A Remote User Authentication Scheme Using Smart Cards with Forward Secrecy," *IEEE Transactions on Consumer Electronics*, vol. 49, no. 4, pp. 1246–1248, Nov. 2003. [Online]. Available: https://ieeexplore.ieee.org/document/1261228

[7] R. Fielding and J. Reschke, "Hypertext Transfer Protocol (HTTP/1.1): Authentication," *Internet Engineering Task Force (IETF)*, RFC 7235, Jun. 2014. [Online]. Available: https:// datatracker. ietf.org/doc/html/rfc7235

[8] N. Sakimura, J. Bradley, M. Jones, B. de Medeiros, and C. Mortimore, "OpenID Connect Core 1.0," *OpenID Foundation*, Nov. 2014. [Online]. Available: https:// openid.net/specs/openid-connect-core-1_0.html

[9] T. Ylonen and C. Lonvick, "The Secure Shell (SSH) Authentication Protocol," *Internet Engineering Task Force (IETF)*, RFC 4252, Jan. 2006. [Online]. Available: https://datatracker.ietf.org/doc/html/rfc4252

[10] S. Thakur, P. Itankar, P. Gujar, A. K. Sayed, V. Pandey and S. Agrawal, "ER-ADENN:Design and Implementation of EEG-based Emotion Recognition using Adaptive Dropout Enabled Neural Network," 2025 3rd International Conference on Advancement in Computation & Computer Technologies (InCACCT), Gharuan, India, 2025, pp. 320-325. https://ieeexplore. ieee.org/document/11011425