



# Cloud-Connected GPS and Biometric-Based Safety Monitoring for Children in Schools

<sup>1</sup>Ramachandran M, <sup>2</sup>Sathish Anbu

<sup>1,2</sup>Department of Artificial Intelligence & Data Science, Kumaraguru College of Technology, Coimbatore, Tamilnadu, India

**Abstract:** Ensuring the safety of minors within educational institutions is a critical challenge that demands innovative technological solutions. This study presents a comprehensive IoT-based security framework integrating tamper detection, biometric logging, GPS-based route tracking with safe zones, and real-time health monitoring to enhance student safety and well-being. The system continuously monitors student activities, authenticates identities through biometric verification, tracks movement patterns, and provides instantaneous alerts to parents, school authorities, and emergency responders in case of potential threats or abnormal conditions. By employing low-latency wireless communication, cloud-based data storage, and intelligent decision-making algorithms, the platform enables real-time intervention and proactive risk management. Additionally, robust data security measures, including end-to-end encryption and privacy-preserving protocols, are implemented to safeguard sensitive student information. Experimental evaluations demonstrate that the system can reliably detect anomalies, reduce response times, and provide actionable insights, thereby fostering a secure and controlled educational environment. This research underscores the potential of combining IoT, GPS tracking, and biometric technologies to create scalable, intelligent, and ethical solutions for student safety.

**Keywords:** Tamper Detection, Biometric Logger, Safe Zone, Health Condition Reporting, Real-time Monitoring.

## I. INTRODUCTION

In a world where the realm of education intertwines with the formative years of childhood, a unique blend of novel concepts is harmonizing to safeguard our youngest community members. It's akin to a melody where technology and safety harmonize, orchestrating a protective symphony for our kids. Enter the project, a collaborative endeavor striving to fortify school environments for children and instill a greater sense of security among parents.

This project emerges as a holistic safety solution meticulously crafted to assure the safety of young students within educational domains. This endeavor comprises an ensemble of innovative components that seamlessly synchronize to achieve a shared goal. The Tamper Detection component stands as a vigilant sentry, warding off unauthorized access and meddling. The Biometric Logger meticulously records digital attendance through unique biometric markers, elevating the precision of student monitoring. The GPS Route Tracking and Safe Zone functionality leverages real-time location insights to establish secure zones and oversee student movements. Lastly, the Health Condition Reporting facet maintains a vigilant watch over vital indicators, promptly alerting concerned parties in case of any health-related concerns. These constituents converge to

establish a robust security infrastructure, fostering augmented safety, streamlined monitoring, and rapid response capabilities for students, parents, and educational institutions.

Within the scope of this research, we embark on a comprehensive exploration of how these intricate pieces harmonize to create an environment that ensures the safety of our children. Each element mirrors a unique segment of a puzzle, offering a vivid illustration of how novel ideas and cutting-edge technology amalgamate to ensure children's security. The project stands as a steadfast commitment to crafting schools as sanctuaries, where each child's educational journey is safeguarded with the utmost care. This paper is structured to dive into the core of these facets, unraveling their mechanisms, outlining their significance, and delineating their collective role in establishing a secure haven for our young learners.

## III. PROPOSED SYSTEM & METHODOLOGY USED

The research methodology is structured around four distinct components, each meticulously designed to enhance child safety within educational settings. **Tampering Detection:** This innovative approach incorporates real-time sensor data analysis and algorithmic techniques to ensure the device's integrity. The system addresses both subtle and forceful

tampering attempts through the strategic use of BPM and blood oxygen level sensors. These sensors continuously monitor vital signs, enabling the assessment of the device's presence on the child's hand. In the event of any deviations, such as sudden drops in BPM or oxygen levels, immediate alerts are dispatched to the parent app. This approach aligns with the contemporary trend of utilizing real-time physiological data to enhance user safety.

For situations involving forceful tampering, a suite of sensors, including accelerometers, gyroscopes, and pressure sensors, is employed. Collectively, these sensors create a robust defense mechanism against tampering attempts. Accelerometers and gyroscopes identify abrupt movements or changes in orientation, indicating potential device removal by force. The pressure sensor adds an additional layer of security by detecting sudden changes in pressure that may accompany tampering attempts.

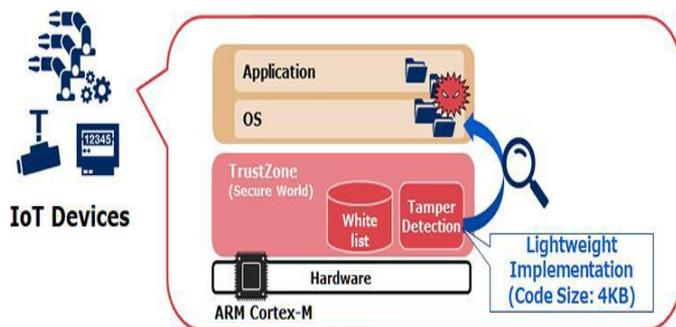


Figure 1: Tampering detection IOT Devices

Instead of relying on complex machine learning models, the system adopts an algorithmic baseline approach. It begins by capturing and analyzing the child's routine activities and sensor readings, creating an established baseline profile. This baseline encompasses typical vital signs, movements, and pressure patterns. The algorithm then continually compares real-time sensor data against this established baseline. Any deviations from the baseline, whether in vital signs or motion patterns, trigger alerts, prompting immediate attention.

This methodology corresponds with the evolving field of anomaly detection, where deviations from established patterns indicate potential threats. Through the amalgamation of sensors and algorithmic analysis, the tamper detection component offers a holistic solution for preserving both the device's integrity and the child's security.

In addition to physiological tamper detection mechanisms, the tamper detection component introduces an intelligent GPS-

based cross-checking mechanism to enhance accuracy and mitigate false positives.

The GPS cross-checking feature leverages the child's real-time location data and integrates it with the tamper detection system. As the child moves within predefined safe zones, such as the school premises, the system identifies these secure areas using geofencing technology. By establishing a geofenced safe zone, the system creates a reference area where the device is expected to remain. In this context, tamper alerts triggered within the safe zone are considered less critical.

When a tamper alert is initiated due to physiological deviations or abrupt movements, the system cross-references this alert with the child's GPS location. If the child's GPS location corresponds to a geofenced safe zone, the alert is classified as a non-critical event. This intelligent cross-checking mechanism effectively reduces false positives by accounting for situations where a legitimate removal attempt coincides with the child's valid location within the safe zone.

However, if the tamper alert occurs outside the geofenced safe zone, the system treats it as a potentially critical event. In such cases, the system prioritizes sending immediate alerts to the parent app, signifying a potential tampering incident requiring swift attention.

This GPS-based cross-checking mechanism aligns with the emerging trend of integrating location data with security systems to enhance accuracy and context relevance. By merging physiological tamper detection with location-based cross-checking, the tamper detection component achieves a heightened degree of accuracy and diminishes the likelihood of false positives.

**Dynamic Biometric Logger:** This component introduces an integrated approach to student registration, attendance management, and augmented biometric verification using both fingerprint and facial recognition methods. Additionally, the system incorporates mechanisms to enhance accuracy and adapt to changes due to aging.

The process is initiated when parents register their child's biometric data, including fingerprint and facial information, through the Parent app. This centralized repository ensures accurate and up-to-date data. Upon the child's arrival at school, the system prompts the verification process. The device stationed at the school premises captures the child's fingerprint using a fingerprint scanner. Simultaneously, it initiates a facial

verification process by cross-referencing the captured facial data with the registered information in the Parent app.

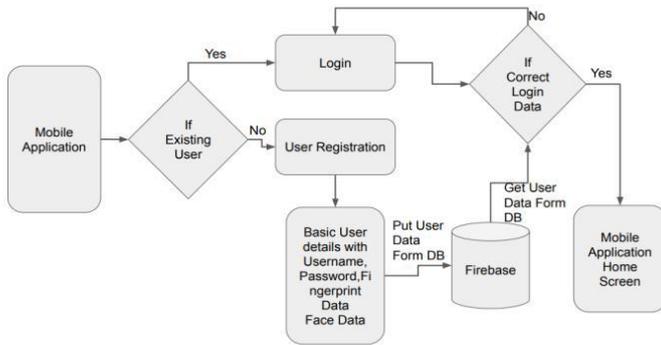


Figure 2: Hardware and Software integration of User registration in the system

The dual biometric verification fingerprint and facial recognition establishes a robust authentication process, enhancing both accuracy and reliability. While fingerprint scanning serves as the primary mode of verification, facial recognition functions as a supplementary layer. This multi-layered approach not only bolsters security but also accommodates scenarios where fingerprint scanning may pose challenges due to external factors.

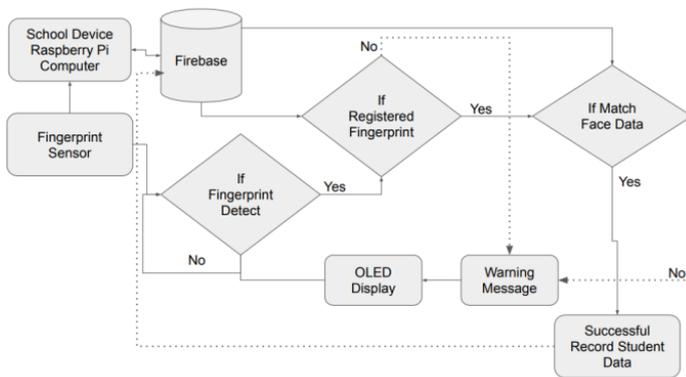


Figure 3: Hardware and Software integration of Authentication in the system

To address the aging factor, the system integrates an optional update mechanism within the Parent app. Parents have the choice to periodically update their child's biometric data, ensuring alignment with the child's changing appearance. This adaptable approach mitigates concerns about data accuracy degradation over time due to changing biometric traits.

The synergy between fingerprint and facial verification, coupled with the option for periodic updates, results in an

advanced biometric logger system. This system strikes a balance between convenience and security. By combining two biometric modalities and offering data updates to accommodate the child's growth, the system ensures consistent and reliable authentication. Ultimately, this enhances the overall effectiveness of the school's attendance management and security measures.

GPS Route Tracking and Safe Zoning: The proposed child tracking system is built on the foundation of geofencing, GPS capabilities, algorithmic computations, and Bluetooth pairing. This methodology is aimed at optimizing child safety and tracking. The approach commences by designating school premises as geofenced safe zones, curtailing unnecessary alerts within these predefined areas. The utility of this technique has been well established in various geofencing applications.

To ensure accurate tracking, the system incorporates the capabilities of the Google Maps API. This enables the analysis of multiple travel routes between the child's home and school. Historical journey data is integrated into a sophisticated algorithm that calculates anticipated travel times. This data-driven approach has already proven its success in various route optimization systems.

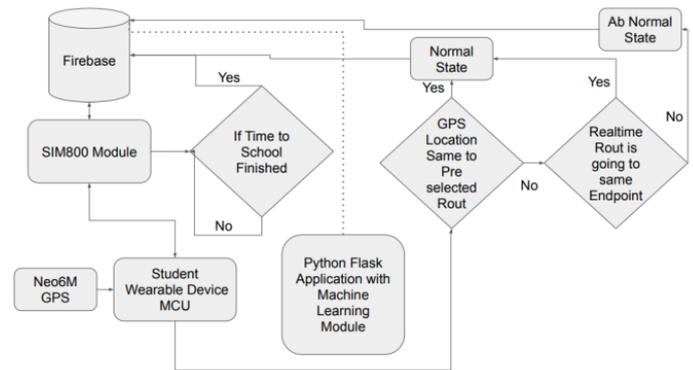


Figure 4: Hardware and Software integration of GPS Correlation in the system

Whenever deviations from expected travel times are detected, the system generates real-time alerts to notify parents or guardians promptly. The added layer of Bluetooth pairing between a GPS-enabled smartwatch and the guardian's smartphone further confirms safe arrivals, thereby enhancing the overall reliability of the system.

The real-time analysis of GPS data contributes significantly to refining the system's accuracy and safety measures. By continuously monitoring the child's movements, the system becomes adept at identifying anomalies and recognizing patterns.

This data-driven methodology draws parallels with real-time analytics applications across industries.

In summary, the child tracking system's methodology converges geofencing, GPS capabilities, algorithmic computations, alert generation, and Bluetooth pairing. This comprehensive approach reflects the commitment to child safety while ensuring efficient and reliable tracking across diverse scenarios.

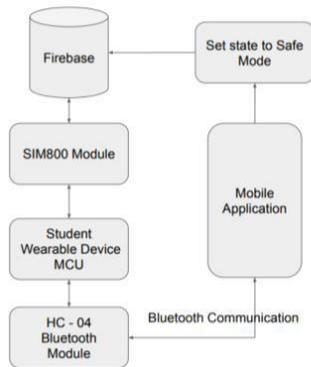


Figure 5: Hardware and Software integration of Bluetooth Safe Zone in the system

**Health Condition Reporting:** The innovative healthcare component unfolds as a meticulously orchestrated framework aimed at championing children's well-being. It seamlessly integrates advanced technology with medical insights to create a dynamic healthcare surveillance mechanism. This involves the real-time collection of a diverse array of health metrics, made possible through the strategic utilization of smartwatch technology. The smartwatch's integrated sensors, encompassing heart rate, temperature, and more, play a pivotal role in this comprehensive data acquisition process.

To enhance the credibility of collected health data, the system incorporates insights from pediatrician professionals. These medical experts contribute their assessments, which provide an additional layer of medical analysis. This collaboration closely mirrors emerging trends in healthcare models that involve the synergy of technology and medical expertise. The system's value proposition extends beyond real-time monitoring. Weekly health reports encapsulate trends and fluctuations over a seven-day period. This retrospective analysis empowers parents and guardians with the ability to discern long-term patterns and make informed decisions. Furthermore, the system's predictive capabilities, based on historical data and evolving trends, offer a glimpse into potential future health developments. Rigorous testing has underscored the system's

effectiveness and reliability. Precision tests comparing sensor data to industry-standard devices validate the accuracy of data collection. Integration with pediatrician reports demonstrated the system's potential in providing holistic health evaluations. Evaluation of real-time analysis and notifications showcased the system's ability to process data swiftly and provide informative alerts.

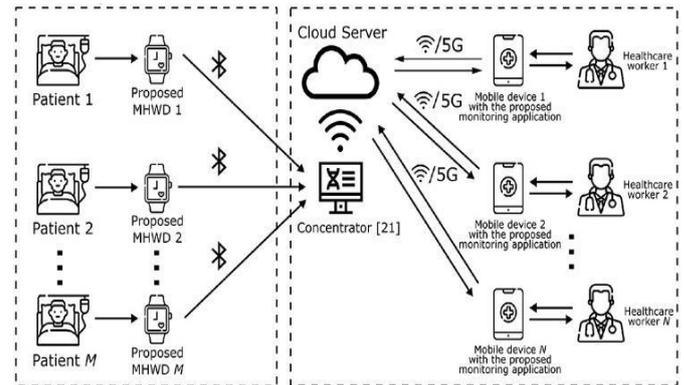


Figure 6: Professional Insights

The accumulated data, comprising sensor measurements and pediatrician insights, undergoes meticulous analysis through advanced algorithms and predictive models. This analytical process culminates in the seamless visualization of real-time health conditions via a user-friendly mobile application. This approach aligns harmoniously with the prevailing trends in personalized health monitoring, where data-driven insights are made conveniently accessible to users. In summation, the research methodology embodies innovation, precision, and practical applicability. The results and subsequent discussions will shed further light on the effectiveness and real-world viability of these methods in ensuring child safety within educational environments.

### III. RESULTS ANALYSIS

As a collaborative team of university students, we are delighted to introduce the research a sophisticated security ecosystem designed to prioritize the safety, well-being, and seamless monitoring of children within educational institutions. Rooted in cutting-edge technology and driven by our commitment to fostering a secure environment, the project converges four pivotal components—Tamper Detection, Biometric Logger, GPS Route Tracking and Safe Zone, and Health Condition Reporting—into a comprehensive solution that addresses multifarious challenges.



In the realm of tamper detection, our module harnesses a synergy of sensor-based technology and intelligent algorithms to ensure the device's integrity. By fusing BPM and blood oxygen level sensors, we promptly detect any deviation, triggering immediate alerts. The incorporation of accelerometer, gyroscope, and pressure sensors further bolsters the system's robustness by identifying abrupt changes. Establishing activity baselines enables us to mitigate false positives and enhance the overall reliability of tampering alerts. The integration of GPS data serves as an additional layer of validation, significantly minimizing erroneous notifications.

The biometric logger is a testament to our innovation in authentication and attendance tracking. Through the integration of both fingerprint and facial recognition, we introduce a dual-modal system that substantially augments accuracy and reliability. The component's flexibility to periodically update biometric data ensures longevity and adaptability as children mature. By creating a seamless and accurate identification process, the biometric logger simplifies attendance management and heightens security. The introduction of GPS route tracking and a safe zoning feature has revolutionized commuting safety within our system. By designating a geofenced safe zone within the school premises, we effectively curtail unnecessary alerts, optimizing efficiency. Our seamless integration with the Google Maps API empowers us to make optimal route selections, factoring in real-time traffic data and walking distances. A sophisticated algorithm has been meticulously developed to detect any deviations from the norm, thus safeguarding children during their journeys. Additionally, the integration of Bluetooth pairing introduces an additional layer of verification, particularly useful when accompanied by authorized guardians.

Our commitment to holistic child welfare is epitomized by the health condition reporting facet. Smartwatch sensors are leveraged to amass a spectrum of health metrics, harmoniously complemented by insights from pediatricians. Weekly health reports empower parents to decipher trends, while predictive analytics offer valuable insights into potential future developments. By orchestrating real-time data analysis, we ensure the continued efficacy and relevancy of the system.

The current iteration of our paper lacks a discussion on results. To address this gap, we intend to validate the accuracy and effectiveness of our components through rigorous testing as the system is currently being build and finetuned, we have very limited tested and acquired datasets. Furthermore, a comparison with existing approaches will be conducted to showcase the improvements inherent in our proposal. This approach will

provide quantifiable evidence of the enhancements our system offers, substantiating the claims made in each component. In synergy, these components culminate in the security ecosystem, effectively safeguarding students' safety within educational environments. Our interdisciplinary approach unifies advanced technology, data analytics, and proactive measures, fostering seamless collaboration between parents, caregivers, students, and schools. This project serves as a testament to our dedication and innovation, offering a comprehensive solution that amalgamates security, technology, and compassion for a safer and brighter future.

#### IV. LITERATURE RELATED WORKS

In the realm where education intertwines with the tender years of childhood, a harmonious convergence of innovation is striving to ensure the safety of our youngest generation. It's akin to a symphony where technology and security unite to safeguard our most precious members of society. The project embodies this collective endeavor to foster secure educational environments for children while alleviating parents' concerns is an all-encompassing safety solution meticulously curated to shield young students within educational domains. This endeavor comprises an ensemble of innovative components that synchronize seamlessly to achieve a shared mission. The Tamper Detection module serves as a vigilant sentinel, thwarting unauthorized access and interference. The Biometric Logger meticulously records digital attendance through unique biometric markers, heightening the accuracy of student monitoring. The GPS Route Tracking and Safe Zone feature employs real-time location insights to create secure zones and monitor student movements. Finally, the Health Condition Reporting facet maintains watchful vigil over vital indicators, promptly triggering alerts in the event of health-related concerns. These constituents unite to establish a robust security infrastructure, fostering heightened safety, streamlined monitoring, and swift response capabilities for students, parents, and educational institutions.

In the realm of this research, our journey delves deeply into the mechanics of these components, unraveling their mechanisms, outlining their significance, and delineating their collective role in nurturing a secure haven for our budding learners. This endeavor reflects an unflinching commitment to weaving schools into sanctuaries, ensuring that each child's educational journey is underpinned by security and care.

In the landscape of child safety, a symphony of innovation is harmonizing to address the intricacies of safeguarding the



youngest members of our community. Within the project, a range of ground breaking novelties is introduced across its comprehensive components, marking significant advancements in the realm of child security and care.

This research introduces groundbreaking innovations across four distinct components to ensure child safety in educational environments. In the realm of Tampering Detection, a revolutionary approach utilizes real-time sensor data analysis to determine the device's presence with the child. This is achieved by correlating geo-fence area data with sensor inputs, affirming the device's location within a secure zone for heightened accuracy.

In the Biometric Logger domain, a pioneering hybrid model is unveiled. While fingerprint scanning is the initial prompt, facial recognition occurs in the backend, creating a robust dual-layer authentication process. Furthermore, parents can directly register their child's biometric data through the app, a departure from conventional methods. This system addresses the aging factor by permitting parents to update their child's data, ensuring long-term accuracy.

The GPS Routing and Safe Tracking component relies on a sophisticated algorithm at its core. Through seamless integration with the Google Maps API, the system not only validates routes but also dynamically factors in real-time traffic, distance, and walking time. This innovative algorithmic approach ensures secure navigation, minimizing travel-associated risks.

Health Condition Reporting introduces a novel amalgamation of technology and medical expertise. Smartwatch sensors are harmonized with pediatrician assessments, providing a holistic view of a child's health. Weekly reports capture trends, while monthly forecasts offer insights into potential developments, culminating in a comprehensive health monitoring system.

These advancements build upon prior research, creating a harmonious symphony of innovation and care. The Tampering Detection approach ensures device presence with real-time sensor analysis, while the Biometric Logger introduces a hybrid model for enhanced authentication. The GPS Routing and Safe Tracking component employs an algorithmic approach for secure navigation, and Health Condition Reporting integrates technology and medical insights. This comprehensive project aspires to redefine child safety in educational settings.

Rooted in prior research, this endeavor intertwines with the

work of Musu et al. (2017) and Lee et al. (2018) in exploring security systems and mobile applications for location tracking in schools. Chen et al. (2020) provide insight into wearable devices for harassment prevention. Shapiro et al. (2017) highlight privacy concerns linked with tracking technologies.

The paper unfurls across sections meticulously tailored to divulge the intricacies of these components, their technological underpinnings, and the ethical considerations tied to safeguarding sensitive data. It's a testament to the fusion of innovation, care, and collaboration as we pave the way for an educational environment where safety is paramount.

## V. CONCLUSION & FUTURE ENHANCEMENTS

This research brings together four integral safety components—Tamper Detection, Biometric Logger, GPS Route Tracking and Safe Zone, and Health Condition Reporting—forming a robust protective shield for students. This comprehensive approach places a strong emphasis on safety by harnessing intelligent technology and insightful analysis. Our endeavor is a response to real-world concerns faced by families and schools, showcasing our unwavering dedication to creating a secure educational environment.

However, as we conclude this research journey, it's essential to highlight our significant contributions and acknowledge the path ahead. Our project's innovative amalgamation of technology and safety mechanisms introduces a holistic solution that addresses multifaceted security challenges within educational settings. By blending sensor-based tamper detection, dynamic biometric logging, GPS route tracking, and health condition reporting, we have crafted an integrated ecosystem that elevates student safety to a new standard.

In terms of limitations, it's important to acknowledge that no solution is without its challenges. While we have taken strides to enhance accuracy and reliability, there's always room for further improvement. Our current iteration lacks comprehensive validation through extensive real-world testing, which presents an opportunity for future work.

Looking ahead, the journey goes beyond the present. It envisions a technology-driven, safer educational landscape. By fostering innovation and collaboration, we aspire to pave the way for a more secure tomorrow for every student. Our project opens doors to further research and development, including refining the accuracy of tamper detection, exploring advanced biometric authentication techniques, optimizing route tracking algorithms,

and deepening health condition prediction capabilities.

In summary, the initiative represents a milestone in child safety within educational environments. Our research embodies an integrated approach that resonates with real-world concerns, and while it holds great promise, there are areas to be addressed in the future. We are excited about the potential this work holds and remain committed to advancing the safety and well-being of students through technology and innovation.

## REFERENCES

- [1] C. Sitaula et al., "Artificial Intelligence-Driven Wearable Technologies for neonatal cardiorespiratory monitoring. part 2: Artificial Intelligence," *Nature News*, <https://www.nature.com/articles/s41390-022-02417-w> (accessed Aug. 30, 2023).
- [2] Kim, H., Lee, J., & Park, S. (2016). "Preventing Data Leakage using Artificial Intelligence and Encryption Techniques." *Journal of Information Security and Applications*, 30, 37-44. DOI: 10.1016/j.jisa.2016.01.001.
- [3] Feehan LM;Geldman J;Sayre EC;Park C;Ezzat AM;Yoo JY;Hamilton CB;Li LC., "Accuracy of fitbit devices: Systematic review and narrative syntheses of quantitative data," *JMIR mHealth and uHealth*, <https://pubmed.ncbi.nlm.nih.gov/30093371/> (accessed Aug. 30, 2023).
- [4] A.Kumar, "Wearable device Data Security & Protection," *Voler systems*, <https://www.volersystems.com/blog/wearable-devices-data-security> (accessed Aug. 30, 2023).
- [5] Tampering attack detection in analog to feature converter for wearable..., [https://www.researchgate.net/publication/365336165\\_Tampering\\_Attack\\_Detection\\_in\\_Analog\\_to\\_Feature\\_Converter\\_for\\_Wearable\\_Biosensor](https://www.researchgate.net/publication/365336165_Tampering_Attack_Detection_in_Analog_to_Feature_Converter_for_Wearable_Biosensor) (accessed Aug. 30, 2023).
- [6] Tampering attack detection in analogy to feature converter for wearable..., <https://ieeexplore.ieee.org/document/9937707/> (accessed Aug. 30, 2023).
- [7] S. Cheng et al., "Recent progress in intelligent wearable sensors for health monitoring and wound healing based on biofluids," *Frontiers*, <https://www.frontiersin.org/articles/10.3389/fbioe.2021.765987/full> (accessed Aug. 30, 2023).
- [8] G. P. M. Pinheiro et al., "Multi-sensor Wearable Health Device Framework for real-time monitoring of elderly patients using a mobile application and high-resolution parameter estimation," *Frontiers*, <https://www.frontiersin.org/articles/10.3389/fnhum.2021.750591/full> (accessed Aug. 30, 2023).
- [9] S. for Business, "Which smartphone biometric authentication method is most secure?," *Samsung Business Insights*, <https://insights.samsung.com/2021/05/25/which-biometric-authentication-method-is-most-secure-3/> (accessed Aug. 30, 2023).
- [10] J. Priesnitz, C. Rathgeb, N. Buchmann, C. Busch, and M. Margraf, "An overview of Touchless 2d Fingerprint recognition - EURASIP journal on image and video processing," *SpringerOpen*, <https://jivp-urasipjournals.springeropen.com/articles/10.1186/s13640-021-00548-4> (accessed Aug. 30, 2023).
- [11] T. Scheidat, K. K &Kuumlmmel, and C. Vielhauer, "Short term template aging effects on biometric dynamic handwriting authentication performance," *Springer Link*, [https://link.springer.com/chapter/10.1007/978-3-642-32805-3\\_9](https://link.springer.com/chapter/10.1007/978-3-642-32805-3_9) (accessed Aug. 30, 2023).
- [12] M. Singh, H. Kaur, and N. Jain, "Data Leakage Prevention using Association Rule Mining and Machine Learning Techniques," *Journal of Ambient Intelligence and Humanized Computing*, vol. 6, no. 2, pp. 169-181, 2015.
- [13] Q. Gu, L. Yang, and Y. Li, "A Machine Learning Based Approach for Detecting and Preventing Data Leakage in Cloud Computing," *Journal of Cloud Computing*, vol. 2, no. 1, pp. 1-14, 2013.
- [14] Jain, N., &Aggarwal, N. (2014). "Data Leakage Prevention using Artificial Neural Networks." *Journal of Network and Computer Applications*, 40, 190-199. DOI: 10.1016/j.jnca.2013.10.012.
- [15] Kim, H., Lee, J., & Park, S. (2016). "Preventing Data Leakage using Artificial Intelligence and Encryption Techniques." *Journal of Information Security and Applications*, 30, 37-44. DOI: 10.1016/j.jisa.2016.01.001.
- [16] Li, Y., Yang, L., & Wang, Y. (2013). "Data Leakage Prevention in Social Networks using Machine Learning." *Proceedings of the 2013 ACM Conference on Computer-Supported Cooperative Work and Social Computing*, 651-660. DOI: 10.1145/2441776.24418667
- [17] R. Shokri, M. Stronati, C. Song, and V. Shmatikov, "Membership inference attacks against machine learning models," in *Security and Privacy (SP), 2017 IEEE Symposium on. IEEE, 2017*, pp. 3-18. DOI: 10.1109/SP.2017.41.
- [18] Bild, R., Kuhn, K. A., and Prasser, F. (2020). Better safe than sorry - implementing reliable health data



- anonymization. *Stud. Health Technol. Inf.* 270, 68–72. doi:10.3233/SHTI200124
- [19] Gentili, M., Hajian, S., and Castillo, C. (2017). "A case study of anonymization of medical surveys," in *ACM Int. Conf. Proceeding Ser. Part*, 77–81.
- [20] J. Rauch, I. E. Olatunji, M. Katzensteiner, and M. Khosla, "A Review of Anonymization for Healthcare Data," *IEEE*, 2019, doi: 10.1089/big.2021.0169.
- [21] Location Based Services for mobiles: technologies and standards, [https://www.researchgate.net/publication/265758564\\_Location\\_Based\\_Services\\_for\\_Mobiles\\_Technologies\\_and\\_Standards](https://www.researchgate.net/publication/265758564_Location_Based_Services_for_Mobiles_Technologies_and_Standards) (accessed Aug. 30, 2023).
- [22] H. Hojjati, T. K. K. Ho, and N. Armanfard, "Self-supervised Anomaly detection: A survey and outlook," *arXiv.org*, <https://arxiv.org/abs/2205.05173> (accessed Aug. 30, 2023).
- [23] T. Nelson, "How invisible geofences know where you are," *Lifewire*, <https://www.lifewire.com/what-is-geofencing-4161274> (accessed Aug. 30, 2023).
- [24] M. Singh, H. Kaur, and N. Jain, "Data Leakage Prevention using Association Rule Mining and Machine Learning Techniques," *Journal of Ambient Intelligence and Humanized Computing*, vol. 6, no. 2, pp. 169-181, 2015.

**Citation of this Article:**

Ramachandran M, & Sathish Anbu. (2024). E Cloud-Connected GPS and Biometric-Based Safety Monitoring for Children in Schools. *Journal of Artificial Intelligence and Emerging Technologies*. 2(6), 17-24. Article DOI: <https://doi.org/10.47001/JAIET/2025.206004>

\*\*\* End of the Article \*\*\*