INTERNATIONAL JOURNAL OF INNOVATIVE STUDIES
A MONTHLY, INDEXED, REFEREED AND PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
VOL.8. ISSUE.1, 2026 (SEPTEMBER)

RESEARCH ARTICLE

ISSN: 3027-2173

DESIGN AND EVALUATION OF A MULTIMODAL ANDROID ANTI-THEFT SYSTEM INTEGRATING GPS, VISUAL AND BIOMETRIC EVIDENCE

Virginia E. Ejiofor[1] & Izuchukwu Nwankpa[2]
Department of Computer Science, Nnamdi Azikiwe University, Awka, Nigeria

EMAIL: iv.nwankpa@unizik.edu.ng[1], ve.ejiofor@unizik.edu.ng[2]

DOI: https://doi.org/10.5281/zenodo.22956204

ARTICLE INFORMATION

Received: 24th July, 2026

Accepted: 19th August, 2026

Published: 14th Sept., 2026

KEYWORDS: Android anti-theft system; GPS tracking; digital evidence; fingerprint acquisition; biometric evidence; mobile security

Publisher: Empirical Studies and Communication (A Research Center)
Website: www.cescd.com.ng

ABSTRACT

Smartphone anti-theft systems commonly provide device location, remote control, SIM-change monitoring, or camera-based evidence, but rarely combine these with biometric evidence. This study designed and evaluated a multimodal Android anti-theft system that combines Global Positioning System (GPS) tracking with photographic and fingerprint evidence acquisition and cloud-based remote monitoring. The system uses a three-layer architecture comprising an Android mobile layer, a Firebase cloud layer, and a React-based web layer. The Android application was developed in Kotlin using foreground services for location, camera and fingerprint operations. An external DigitalPersona U.are.U 4500 fingerprint scanner, connected via USB-OTG, acquired fingerprint samples and generated PNG images and Fingerprint Minutiae Data (FMD) templates in ANSI-378-2004 format. The front-facing camera and the GPS module captured and synchronised evidence with Firebase Realtime Database at five-second intervals. Firebase Storage held the photographic and fingerprint evidence, while a React/Leaflet web dashboard gave authorised users remote access to device location, captured evidence and tracking controls. Functional and performance testing confirmed successful operation of all major components under the defined test conditions. Observed response times were approximately 3 s for registration, 1.5 s for login, 3.5 s for scanner detection, 3 s for fingerprint capture response, 2 s for template extraction, 5–8 s for image upload, 5-s intervals for camera capture and GPS synchronisation, 10 s for dashboard loading, and 1 s for remote tracking control, with all services operating concurrently. These results demonstrate the technical feasibility of integrating location, visual and biometric evidence acquisition within a single Android anti-theft framework. However, the prototype remains dependent on external fingerprint hardware, Internet connectivity, device power, USB permissions and Android-device compatibility, and provides evidence representation rather than forensic-grade suspect identification. The system therefore offers a proof-of-concept for multimodal evidence collection rather than a complete forensic or law-enforcement solution.

This work is licensed under a Creative Commons Attribution 4.0 License

INTRODUCTION

Smartphones have become important personal computing and communication devices that commonly hold information of financial, personal and private value. Their portability and extensive use make loss or theft a significant security concern, and the consequences extend beyond the replacement cost of the hardware because a stolen device may expose stored information and complicate the owner's efforts to recover the device or investigate its unauthorised use. This study therefore identifies the need for technological mechanisms that can support both device monitoring and evidence collection following theft-related events. Regulatory bodies have likewise recognised the problem's scale, with the United States Federal Communications Commission convening a public workshop on mobile-device-theft prevention (Federal Communications Commission, 2014).

A range of anti-theft approaches has been developed over time. Earlier systems relied mainly on SMS commands, SIM-card monitoring, GPS tracking, camera activation, remote alarms and cloud-based storage (Khan et al., 2014; Sonia & Aswatha, 2013; Vasudevareddy et al., 2020). More recent work has extended this base toward geofencing, sensor-based detection, blockchain-secured responses, image capture and collaborative location technologies (Zhao & Yu, 2021; Grob et al., 2017; Jin et al., 2018; Papadakis et al., 2021; Rajkumar et al., 2021; Shober & Sadhkan, 2019). Agbonifo et al. (2021) investigated a mobile smartphone anti-theft system, and Kumar et al. (2023) and Nikure et al. (2023) each combined SIM monitoring, GPS tracking and camera-based evidence with remote access or alerting. Malsa et al. (2024) and Dubey et al. (2023) explored blockchain-secured and privacy-preserving responses to theft detection, while Awad (2024) combined SIM monitoring, GPS tracking and multimedia evidence, and Shalini and Shanthi (2025) investigated location-based image capture with culprit identification.

Location tracking remains one of the most common components of anti-theft systems. GPS and related technologies can indicate where a lost or stolen device is located, and geofencing can additionally detect movement beyond predefined boundaries, while Bluetooth-based and collaborative finding approaches have been investigated as alternatives or complements to conventional GPS. Nevertheless, location information primarily answers the question of where a device is located and does not necessarily indicate who is handling it.

Camera-based evidence collection provides another dimension. Several anti-theft systems have attempted to capture photographs or video of an unauthorised user following events such as SIM-card replacement, remote activation or other suspicious activity. Visual information can provide useful contextual evidence, but its usefulness may depend on lighting, camera orientation, image quality and obstruction, so it may not always be sufficient as the only source of information about an unauthorised user.

Biometric evidence provides a different form of information. Previous smartphone anti-theft research has investigated behavioural biometrics, including motion and gait, but such approaches generally focus on detecting an unusual user or behaviour rather than producing a physical fingerprint record. The comparative review above indicates that the reviewed systems generally lacked fingerprint acquisition in combination with GPS and visual evidence.

Recent studies reinforce this gap. Kumar et al. (2023) combined SIM monitoring, GPS, camera capture and remote access but did not include fingerprint acquisition; Nikure et al. (2023) similarly integrated GPS and image-based monitoring without biometric fingerprint evidence; and Malsa et al. (2024) concentrated on sensor-based detection and blockchain-secured responses rather than biometric capture. Awad (2024) and Shalini and Shanthi (2025)

focused on SIM-triggered or location-triggered image collection. This comparative review consequently points to limited integration of fingerprint acquisition with location tracking and visual evidence within a single Android anti-theft system.

The problem addressed in this study is therefore not simply the inability to locate a stolen smartphone, but the limited availability of an integrated mechanism that can collect complementary evidence about a theft-related event. This motivates the need for an Android system that combines GPS tracking, image capture, external fingerprint acquisition and secure evidence management through an authorised remote interface.

The aim of this study was to develop an Android-based anti-theft application that combines stolen-device location tracking with contextual digital evidence collection to support subsequent investigation of mobile phone theft. Specifically, the study implemented GPS tracking, photographic and fingerprint evidence acquisition, secure data transmission and remote monitoring.

The main contribution of the study is a multimodal Android anti-theft architecture in which location information, photographic evidence and fingerprint evidence are acquired and managed through interconnected mobile, cloud and web components. The system also demonstrates the practical integration of the DigitalPersona U.are.U 4500 scanner with Android foreground services and the generation of both visual and machine-readable fingerprint representations.

MATERIALS AND METHODS

SYSTEM DEVELOPMENT APPROACH

The study adopted Structured Systems Analysis and Design Methodology (SSADM) together with Rapid Application Development (RAD): SSADM structured the system requirements and processes, while RAD supported iterative development and rapid refinement of the prototype, appropriate given a small-to-medium system with multiple interacting components requiring iterative testing during implementation.

The resulting system was implemented as a prototype and evaluated in a controlled environment. The evaluation focused on whether the principal functions of the system operated according to their defined requirements and on measuring selected response and synchronisation times.

MATERIALS

The implementation used an Android smartphone, a development computer, Android Studio and the software libraries required for the mobile, biometric, cloud and web components. The prototype was tested on a supported Android smartphone and used a DigitalPersona U.are.U 4500 fingerprint scanner connected to the device through USB-OTG. The development environment included Kotlin-based Android development, CameraX for camera acquisition, Firebase Authentication, Firebase Realtime Database and Firebase Storage for backend functions, and React and Leaflet for the web dashboard.

The fingerprint acquisition subsystem used the DigitalPersona Software Development Kit (SDK) and required native library initialisation, USB device enumeration and permission handling. The implementation also used native biometric components for fingerprint capture and template extraction. The external scanner was selected because the research specifically sought to demonstrate acquisition of fingerprint evidence rather than relying only on the smartphone's built-in biometric authentication sensor.

SYSTEM ARCHITECTURE

The proposed architecture consists of three principal layers: Mobile, Cloud and Web, illustrated in Figure 1.

The Mobile Layer contains the Android application and its background services. Authentication is handled through the application interface, while the Main Activity provides the primary user interface and location information. The Fake Shutdown Activity presents a shutdown-like interface during the defined evidence-collection scenario. The Camera Foreground Service acquires photographs, while the Fingerprint Service interfaces with the external scanner. Android Location Services obtain geographical coordinates from the device.

The Cloud Layer is implemented using Firebase. Firebase Authentication manages user identity and authenticated access. Firebase Realtime Database stores device metadata, GPS coordinates, tracking status and associated timestamps, while Firebase Storage stores photographs, fingerprint images and FMD templates. The cloud layer consequently acts as the central data exchange and storage point between the Android application and the web interface.

The Web Layer is implemented using React and JavaScript. It provides an authenticated monitoring dashboard through which an authorised user can view the device location on a Leaflet map, access captured photographs and fingerprint images, and change the available tracking status. As shown in Figure 1, communication between the mobile, cloud and web layers is bidirectional: device data is transmitted to the cloud, while authorised remote-control information is retrieved by the Android application.

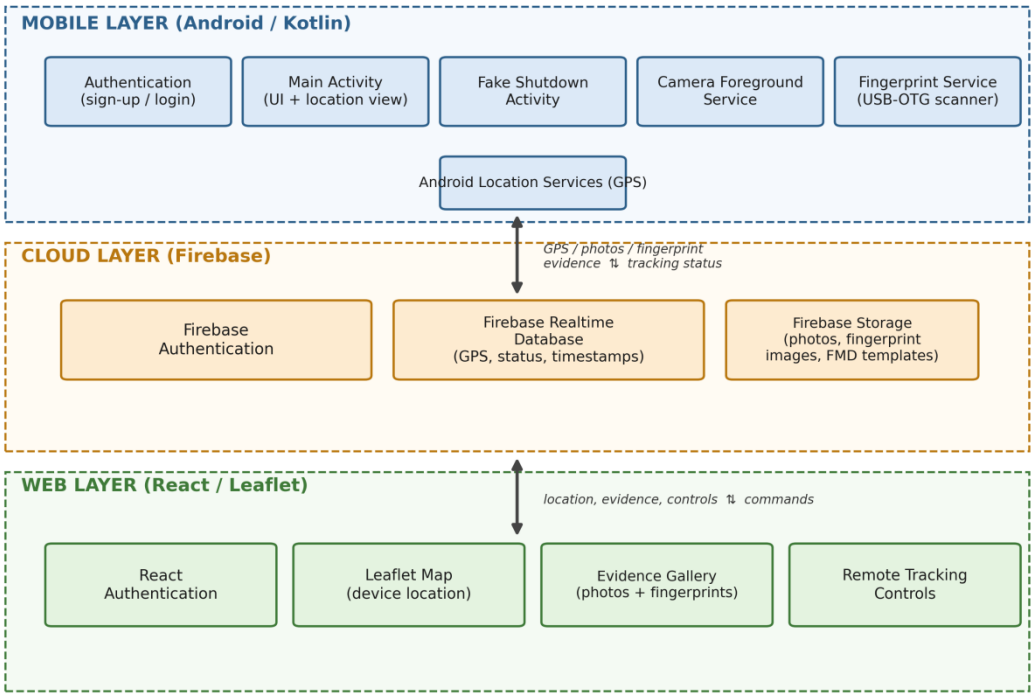

Figure 1. System architecture of the proposed multimodal Android anti-theft system, showing the Mobile, Cloud and Web layers and the bidirectional flow of location, photographic and fingerprint evidence between them.

SYSTEM OPERATION

The overall operating sequence, summarised in Figure 2, begins with registration and authentication of the device owner. The application associates the registered account and device with the cloud backend. During an activated theft-related evidence collection scenario, location information is periodically obtained and synchronised with Firebase.

The photograph acquisition component uses the front-facing smartphone camera through CameraX. The Camera Foreground Service operates independently of the main user interface and captures photographs at configured intervals. In the implemented prototype, photographs were obtained at approximately five-second intervals and uploaded to Firebase Storage.

Fingerprint acquisition is performed through the DigitalPersona U.are.U 4500 scanner connected through USB-OTG. The fingerprint service enumerates and initialises the scanner, monitors for finger placement, captures the fingerprint and processes the acquired data. The resulting fingerprint is represented as a PNG image and as an FMD template in ANSI-378-2004 format, at a resolution of 320 × 360 pixels and 508 DPI.

The fingerprint acquisition process incorporates error handling for the URU_E_MORE_DATA buffer condition: when the required buffer size was not initially sufficient, the implementation retried the acquisition using the required buffer size. This mechanism addressed an observed capture problem and enabled successful fingerprint records to be obtained.

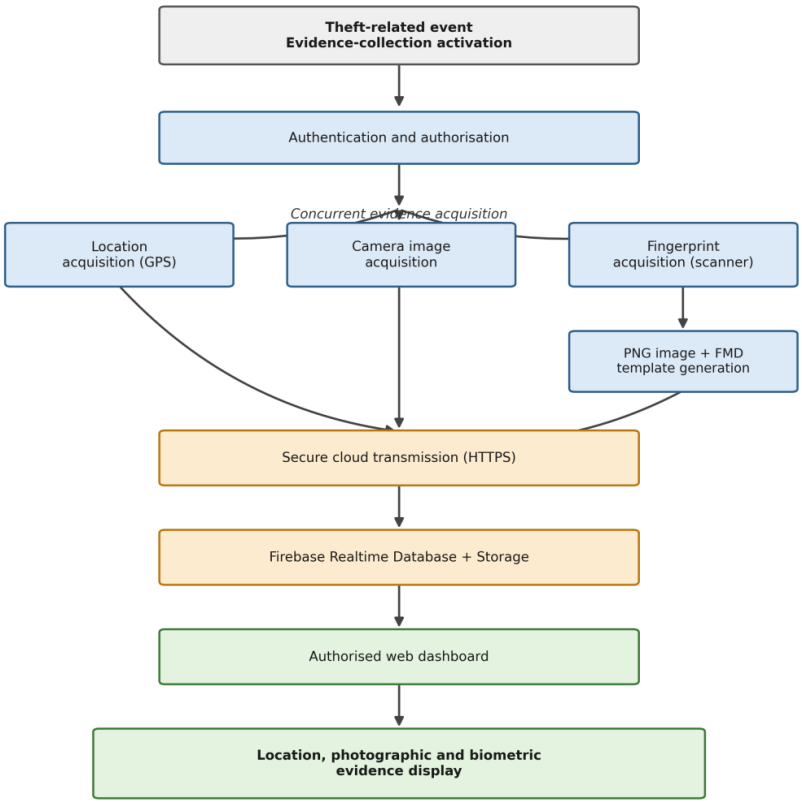

Figure 2. Multimodal evidence-acquisition workflow, from theft-related activation through concurrent location, camera and fingerprint acquisition to secure cloud transmission and dashboard display.

The web dashboard, shown schematically in Figure 3, provides the remote monitoring component. After authentication, the authorised user can view the most recent device location on an interactive map, browse captured photographs and fingerprint images, and control the available tracking services.

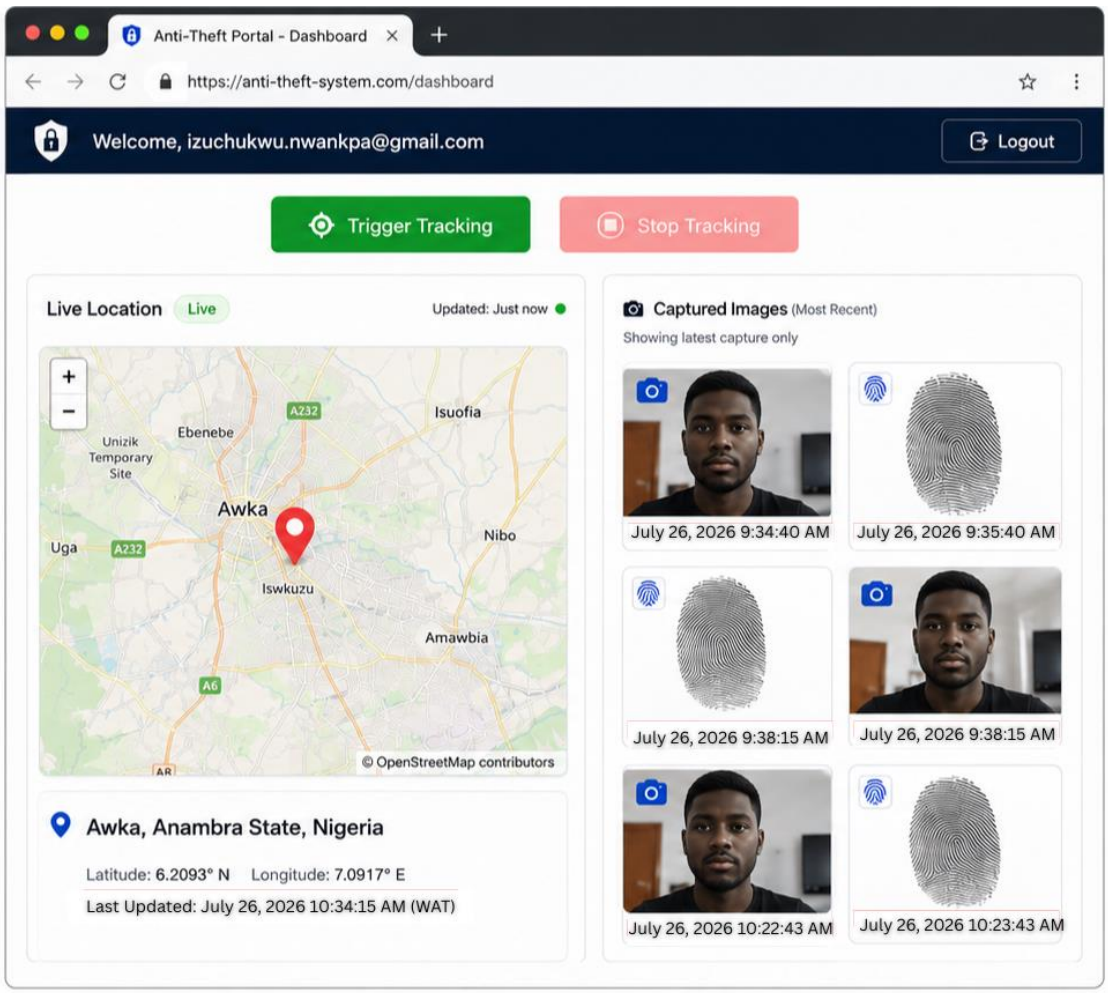

Figure 3. web dashboard for remote monitoring and evidence management, showing the location map, evidence gallery, fingerprint evidence panel and tracking controls.

DATA FLOW AND EVIDENCE MANAGEMENT

The system receives five principal categories of input: user registration details, fingerprint data, photographs, GPS coordinates and remote commands. As Figure 2 shows, these data pass through authentication, evidence acquisition, biometric processing and cloud-upload operations. Fingerprint acquisition generates both image and template representations, while the GPS component writes device coordinates and status information to Firebase Realtime Database. Captured photographic and fingerprint files are stored in Firebase Storage.

This arrangement separates structured metadata from multimedia evidence. Location and tracking information are maintained in the Realtime Database, whereas photographs, fingerprint images and FMD templates are stored as files. The web interface retrieves the corresponding information after successful authentication, creating a centralised evidence-management mechanism rather than distributing evidence across separate email, SMS or local-storage channels.

SECURITY AND ACCESS CONTROL

The prototype incorporates several security mechanisms. Firebase Authentication is used for authenticated access to the mobile application and web dashboard. Firebase Security Rules restrict access to data associated with the authenticated user, while communications between application components and Firebase use encrypted network transport. The system design also relies on authenticated sessions and controlled access to stored evidence.

The fingerprint templates are stored as FMD binary representations rather than as ordinary image files, and the system separately stores the fingerprint image for visual examination. These two representations provide different forms of evidence while supporting subsequent compatible biometric processing.

EXPERIMENTAL TESTING

The prototype was evaluated using functional and performance testing. Functional testing checked whether major operations, such as registration, authentication, scanner detection, fingerprint capture, image upload, GPS synchronisation, dashboard display and remote control, behaved according to their defined requirements.

Performance evaluation measured selected response times and synchronisation intervals, including registration time, login time, scanner detection time, fingerprint capture response, image upload latency, template extraction time, camera capture interval, GPS synchronisation interval, dashboard loading time and remote-toggle latency. Concurrent operation of camera capture, fingerprint capture, upload and GPS synchronisation was also evaluated.

RESULTS

FUNCTIONAL RESULTS

The functional tests showed that the principal components of the prototype operated successfully under the defined test conditions. User registration and authentication were successful. The DigitalPersona scanner was detected, finger placement was recognised, fingerprints were acquired, and the resulting image and template files were generated and uploaded. The web dashboard successfully authenticated the user, displayed location information and provided access to captured evidence, and remote tracking control was correctly reflected between the dashboard and the Android device.

Testing also confirmed concurrent operation of the camera and fingerprint services: simultaneous camera capture, fingerprint acquisition, evidence upload and GPS synchronisation (Figure 2) were maintained without interference under the tested conditions.

The fingerprint component successfully produced 508 DPI fingerprint captures, PNG images and FMD templates. The processing pipeline therefore demonstrated that an external fingerprint device can be integrated with Android software and that the captured biometric information can be converted into both visual and structured machine-readable forms.

PERFORMANCE RESULTS

The observed performance values are summarised in Table 1.

Table 1. Performance evaluation of the developed system.

Evaluation metric	Target/threshold	Observed value	Status
User registration time	< 5 s	~3 s	Pass
User login time	< 3 s	~1.5 s	Pass
Scanner detection time	< 5 s	~3.5 s	Pass
Fingerprint capture response	< 5 s	~3 s	Pass
Image upload latency	< 10 s	~5–8 s	Pass
Template extraction time	< 3 s	~2 s	Pass
Camera capture interval	5 s	5 s	Pass
GPS synchronisation	≥ 1 update/10 s	~5 s intervals	Pass
Web dashboard load time	< 15 s	~10 s	Pass
Remote toggle latency	< 3 s	~1 s	Pass
Concurrent operation	Simultaneous operation	Successful	Pass

All ten measured metrics met their defined thresholds. Interactive operations such as login and remote-toggle control completed in under two seconds, registration and scanner detection completed in three to four seconds, and the more data-intensive operations, image upload and dashboard loading, took up to eight and ten seconds respectively. Camera capture and GPS synchronisation both operated at approximately five-second intervals, consistent with the configured evidence-collection interval. These values should be interpreted as prototype measurements obtained in the controlled testing environment rather than as general performance guarantees across all Android devices and network conditions; broader field testing remains an area for further work.

EVIDENCE ACQUISITION OUTPUTS

Three principal evidence categories were generated by the prototype. The first was location evidence, consisting of device latitude, longitude, timestamps and tracking status stored in Firebase Realtime Database. The second was visual evidence, consisting of photographs captured by the front-facing camera, uploaded to Firebase Storage and displayed through the web dashboard. The third was biometric evidence, consisting of fingerprint images and FMD templates: the fingerprint image provides a visual representation of the ridge pattern, while the FMD representation provides a structured biometric template intended for subsequent compatible biometric processing.

Together, as summarised in Figure 3, these outputs represent complementary information concerning the location of a device, visual context and biometric contact with the external scanner.

DISCUSSION

The results demonstrate the technical feasibility of integrating multiple evidence-acquisition mechanisms in one Android anti-theft application. The main distinction from many systems reviewed above is that location tracking is not treated as the sole outcome of the anti-theft process; instead, the system combines location information with photographic and fingerprint evidence and makes the resulting data remotely accessible through a single authenticated

interface (Figures 1 and 2). The performance results further confirm that these services operate concurrently without interference under test conditions (Table 1) — evidence that the study's contribution lies not merely in three separate features but in their coordination within one workflow. This is consistent with earlier research on the value of GPS, camera evidence and remote monitoring in smartphone anti-theft systems, though, as noted in the Introduction, integration of fingerprint evidence has remained limited in that body of work.

The fingerprint subsystem is an important technical contribution of the study. Conventional smartphone anti-theft applications rely mainly on SIM monitoring, GPS, behavioural detection or camera capture; this prototype instead introduces an external USB fingerprint scanner into the Android anti-theft workflow. The successful detection, acquisition, image generation and FMD-template generation demonstrate that Android foreground services can coordinate an external biometric device alongside other anti-theft functions.

The use of both a PNG fingerprint image and an FMD template provides complementary data representations: the PNG file can be inspected as an image, whereas the FMD template offers a structured biometric representation for compatible subsequent processing. The prototype, however, did not perform a complete identification or matching operation against an external criminal or biometric database. The presence of an FMD template should therefore be interpreted as an evidence-representation capability rather than demonstrated suspect identification.

The cloud architecture further differentiates the system from communication models based primarily on SMS, MMS or direct email, which previous systems commonly used for remote interaction. Cloud-based communication instead provides a central point for storing heterogeneous evidence and presenting it through an authenticated web interface (Figure 3), giving a unified location-and-evidence monitoring mechanism in which device coordinates and captured files can be accessed from one authorised dashboard.

While the reliance on a tethered DigitalPersona U.are.U 4500 scanner via USB-OTG presents a practical constraint for everyday smartphone use, this hardware configuration was necessitated by current Android operating system security protocols. Presently, Android's Biometric API strictly prohibits third-party applications from accessing raw biometric data (such as ridge patterns) from integrated on-device sensors, limiting developer access to simple boolean authentication tokens to protect user privacy. Consequently, this external scanner setup serves as a necessary and foundational proof-of-concept to validate the complete multimodal capture-to-cloud pipeline. The underlying architecture, data flow, and foreground service orchestration developed in this study establish a robust framework that can seamlessly transition to utilizing integrated device hardware should future mobile operating systems introduce secure, authorized APIs for raw biometric extraction during anti-theft scenarios. Nevertheless, the results also expose several limitations. First, fingerprint acquisition depends on the DigitalPersona U.are.U 4500 scanner connected through USB-OTG, so the prototype cannot be assumed to support other scanner models or smartphone-integrated fingerprint sensors without additional implementation. Second, cloud operations depend on active Internet connectivity, so captured information cannot be synchronised to Firebase while the device is offline. Third, continuous camera, GPS and fingerprint-service operation can increase battery consumption. Fourth, Android-device-specific security and USB restrictions may affect scanner reliability on some devices. Finally, the system was tested in a controlled environment using a limited testing configuration, so broader validation across device models, users and real-world conditions is required.

The cloud and evidence-management components should not be interpreted as establishing a complete forensic chain of custody: the prototype applies principles of secure transmission, controlled access and structured storage, but does not by itself establish legal admissibility of the resulting evidence.

The research also differs from approaches designed to continue tracking when a phone is completely offline or powered down. Li et al. (2023), for example, investigated offline finding through collaborative Bluetooth Low Energy discovery, whereas the present prototype relies on the operational Android device and network connectivity for cloud synchronisation. The proposed architecture should therefore be understood as an evidence-oriented Android prototype that complements conventional tracking approaches rather than replacing offline-finding or hardware-level tracking systems.

Overall, the results support the central proposition of this study: GPS, visual and fingerprint evidence can be integrated into one Android anti-theft workflow and exposed through a cloud-supported monitoring interface. The system's contribution is therefore architectural and implementation-oriented, supported by functional and timing evidence.

CONCLUSION

This study designed and evaluated a multimodal Android anti-theft system that integrates GPS tracking, photographic evidence capture, external fingerprint acquisition and cloud-based remote monitoring. The resulting architecture combines mobile, cloud and web components (Figure 1) to collect, transmit, store and remotely present complementary evidence associated with a theft-related event (Figure 2).

The prototype successfully demonstrated integration of the DigitalPersona U.are.U 4500 scanner with Android foreground services, producing both PNG fingerprint images and ANSI-378-2004 FMD templates. The camera service captured photographs at approximately five-second intervals, GPS coordinates were synchronised with the Firebase backend at comparable intervals, and the web dashboard (Figure 3) provided authenticated access to location information, captured images and remote tracking controls. Performance testing confirmed that all measured operations met their defined thresholds (Table 1), and concurrent operation of the camera, fingerprint and GPS services was also successful under the defined conditions.

The study therefore demonstrates the feasibility of extending smartphone anti-theft functionality beyond device location to include contextual visual and biometric evidence acquisition. The system should, however, be regarded as a proof-of-concept, since its operation remains constrained by external fingerprint hardware, USB permissions, Internet availability, battery consumption and Android-device compatibility. Further work should investigate broader device compatibility, larger-scale testing, offline evidence handling, battery optimisation, additional biometric modalities and integration with validated forensic identification workflows.

ACKNOWLEDGEMENTS

I want to thank Prof. V.E . EJIOFOR for all her tireless effort, in supporting and encouraging me to see that this work is published.

REFERENCES

Agbonifo, O. C., Afolayan, A. H., & Akinola, O. H. (2021). Design of a mobile smartphone anti-theft system. Nigerian Journal of Technology, 40(6), 1086–1095. https://doi.org/10.4314/njt.v40i6.11

Awad, F. A. (2024). Android anti-theft security system with GPS tracking [Unpublished manuscript]. ISBAT University. https://www.researchgate.net/publication/385312413_Android_Anti-Theft_Security_System_with_GPS_TrackingDubey, S., Eswari, R., & Vamshi, A. (2023). Mobile anti-theft and privacy protection framework using blockchain. Research Square. https://www.researchsquare.com/article/rs-3232202/v1

Federal Communications Commission. (2014, May 20). FCC announces workshop to focus on prevention of mobile device theft (DA 14-685) [Public notice]. https://docs.fcc.gov/public/attachments/DA-14-685A1.pdf

Grob, S., Tiwari, A., & Hammer, C. (2017). ThiefTrap—An anti-theft framework for Android. In Security and privacy in communication networks: 13th International Conference, SecureComm 2017 (pp. 164–187).

Jin, M., He, Y., Fang, D., Chen, X., Meng, X., & Xing, T. (2018). iGuard: A real-time anti-theft system for smartphones. IEEE Transactions on Mobile Computing, 17(10), 2307–2320.

Khan, A. U. S., Qureshi, M. N., & Qadeer, M. A. (2014). Anti-theft application for Android-based devices. In 2014 IEEE International Advance Computing Conference (IACC) (pp. 365–369). IEEE. https://ieeexplore.ieee.org/document/6779350

Kumar, A., Jain, S., Kurade, R., Abhinav, K., & Patil, S. V. (2023). Anti theft mobile security application. International Research Journal of Modernization in Engineering Technology and Science, 5(5), 3164–3170.

Li, T., Liang, J., Ding, Y., Zheng, K., Zhang, X., & Xu, K. (2023). On design and performance of offline finding network. In IEEE INFOCOM 2023 – IEEE Conference on Computer Communications (pp. 1–10). IEEE.

Malsa, N., Jain, R., & Goyal, S. B. (2024). Mobile device security: A two-layered approach with blockchain and sensor technology for theft prevention. Scalable Computing: Practice and Experience.

Nikure, V., Ikhar, P., Kharalkar, V., Manapure, J., Choudhari, S., & Kubade, H. (2023). Android & Firebase based anti-theft mobile application. International Research Journal of Engineering and Technology (IRJET), 10(5), 48–51. https://www.irjet.net/archives/V10/i5/IRJET-V10I506.pdf

Papadakis, N., Koukoulas, N., Christakis, I., Stavrakas, I., & Kandris, D. (2021). An IoT-based participatory antitheft system for public safety enhancement in smart cities. Smart Cities, 4(2), 919–937.

Rajkumar, M., Rani, P. S., Yasin, S. M., Rakesh, K., & Vignesh, S. (2021). Mobile anti-theft software (MATS). Revista Gestão, Inovação e Tecnologias, 11(3), 1642–1650.

Shalini, E., & Shanthi, V. (2025). A novel location-based anti-theft image capture application with culprit identification for smartphones. TPM: Testing, Psychometrics, Methodology in Applied Psychology, 32(S5), 286–293. https://tpmap.org/submission/index.php/tpm/article/view/1359

Shober, M. A., & Sadhkan, S. B. (2019). A developed method to locate a mobile phone in remote areas. In 2019 2nd International Conference on Engineering Technology and Its Applications (IICETA) (pp. 165–170). IEEE.

Sonia, C. V., & Aswatha, A. R. (2013). AALTM: An Android application to locate and track mobile phones. International Journal of Engineering Trends and Technology, 4(5), 1836–1840.

Vasudevareddy, H., Karthik, V., Karthik, T., Yashwanth, K. P., & Hande, S. (2020). Anti-theft mobile tracking system. International Journal of Innovative Science and Research Technology, 5(6), 497–501.

Zhao, L., & Yu, X. (2021). Design and development of anti-theft tracking APP based on geofence. In 2021 IEEE Asia-Pacific Conference on Image Processing, Electronics and Computers (IPEC) (pp. 738–741). IEEE. https://doi.org/10.1109/IPEC51340.2021.9421332