Kabarak Journal of Research & Innovation Volume 16 Number 3 (2026)
ISSN 2305-784X (print) ISSN 2410-8383 (online)
https://journals.kabarak.ac.ke/index.php/kjri/

An Intelligent Tracking Model for Stolen Android Devices with Multi-User Authentication and Predictive Recovery Support

Authors:
Faith M. Mulei[1], Andrew Ki pkebut[1] and John Chebor[1].

Affiliations:
[1]School of Science, Engineering & Technology. Kabarak University.

Corresponding Author:
Faith M. Mulei Email- muleifaith@kabarak.ac.ke

Article History: *Submitted: 13th December 2024; Accepted: 1st October 2026; Published (online):3rd November 2026*

Abstract

With the growing use of mobile devices for communication, digital transactions, identity management and more sensitive information, theft and loss of personal data continues to pose major cybersecurity and privacy and financial risks. While Google Find My Device and other platforms offer basic device recovery features, their effectiveness in real-world theft scenarios is limited due to the need for internet connectivity, GPS services, and single-user authentication mechanisms. A Design Science Research approach was employed to encompass the identification of issues, the development of models, prototype implementation, and evaluation of results as also quantitative research methodology was selected since the study evaluated the performance of the model. The model was built using Kotlin, Firebase Firestore, Google Maps API, and FIDO2/WebAuthn passkey authentication technologies for an Android environment. The integration of a K-Nearest Neighbors predictive subsystem enabled the analysis of past movement patterns to predict potential future device paths during recovery operations. It also included offline location caching, delayed cloud sync speed, reliable contact recovery features and heatmap-based movement display. The analysis revealed that the implementation was more resilient, proving that authentication was trustworthy, providing correct and timely notification, and maintaining tracking integrity than traditional smartphone recovery systems. Low Root Mean Square Error (RMSE) values were used by the integrated predictive subsystem to estimate trajectory with acceptable accuracy, while offline synchronization tools ensured that recovery could be sustained even in unstable network conditions. The results showed that recovery with multi-user approach improved recovery accessibility and operational flexibility in situations of compromised access. It is concluded in this paper that combining predictive analytics, collaborative authentication and offline operational resilience greatly increases the effectiveness of smartphone recovery under real-world conditions and adds meaningfully to contemporary research on intelligent mobile security.

Keywords: Android Device Recovery, K-Nearest Neighbors, Multi-User Authentication, Predictive Analytics, Smartphone Tracking

Introduction

In today's digital age, smartphones have become indispensable devices for communication, transactions, professional work and even storage of personal information. These devices hold

valuable information such as communications records, banking information, logins, and personal information. With the widespread reliance on smartphones, the loss or theft of these devices raises serious security and privacy issues. According to the global figures, millions of smartphones are lost or stolen each year, resulting in financial losses, privacy breaches, identity theft, and other cybercrime activities for the end-users (GSMA, 2023). The reports also reveal that lost and stolen mobile devices are often used to commit identity theft and fraud, with access to personal data, a common cause of the incidents (Kaspersky, 2022).

Beyond the physical loss of the device, smartphone theft can compromise confidential personal and business information, leading to financial damage and reputational harm. Existing recovery approaches often rely on continuous internet connectivity, active location services, and user intervention, making recovery difficult when devices are switched off, disconnected from the network, or inaccessible to the owner (Behl & Behlum, 2020).

Current smartphone recovery solutions, including Google Find My Device and Apple Find My, provide capabilities such as location tracking, remote locking, and device management. While these features improve basic recovery efforts, they are still dependent on a single user account, active connectivity, and location services. Recovery becomes considerably more difficult when the primary account is unavailable, credentials cannot be accessed, or the device is reset (Google, 2024; Apple, 2024).

Smartphone theft continues to rise all over the world and the current methods of recovering the devices are proving insufficient. According to recent crime statistics, mobile phone theft is still a significant security threat in many metros around the world (Office for National Statistics, 2023; GSMA, 2023). Android recovery systems, which rely on location tracking, network availability and single-user authentication, are unlikely to be available in case of thefts. Furthermore, existing systems lack the capability of studying historical movements and forecasting showed future movements, which lowers the chances of successful device recovery.

This study addresses these gaps by proposing an intelligent tracking model for stolen Android devices that integrates secure multi-user authentication, resilient location tracking, and predictive recovery support within a single recovery model. Rather than relying solely on conventional tracking mechanisms, the proposed model looks to enhance recovery effectiveness while supporting user security and privacy. The model employs biometric authentication, GPS, Wi-Fi and cellular technology to improve device recovery capabilities using a hybrid software-hardware solution. Multi-user authentication is integrated with FIDO2 and WebAuthn, which offer passwordless authentication over public-key cryptography and biometric authenticators, based on the FIDO Alliance (2023). Through this approach, trusted contacts can be involved with the device recovery process on the basis of right access rights, thus making the recovery process more resilient and self-assured without losing the users' privacy and security (Grassi et al., 2020).

Furthermore, the study has applied the K-Nearest Neighbors (KNN) machine learning algorithm in predicting the likely trajectory of the future location based on the historical location data. KNN is chosen due to its simplicity, low computation requirements, ease of interpretation and for mobile computing environments (Hutter et al., 2019). In the past, researchers have found that lightweight machine learning tasks are more suitable for resource-limited environments than computation heavy tasks (Chen et al., 2020). Combine predictive

tracking with stealth background tracking and offline location caching to increase the chances of recovering a stolen device even if traditional tracking methods are unsuccessful.

The overall goal of this study was to develop and evaluate an intelligent tracking model for stolen Android devices with multi-user authentication. Specifically, the study sought to (i) analyze the limitations of existing Android device tracking technologies, (ii) design an intelligent tracking model that addresses the identified limitations, (iii) implement the proposed model within an Android environment, and (iv) evaluate its performance in improving device recovery, security, and usability under real-world-oriented conditions.

Methodology

The study was undertaken using Design Science Research (DSR) methodology to aid the development, implementation and evaluation of an intelligent tracking model of stolen Android devices using multi-user authentication, also quantitative research methodology was selected since the study evaluated the performance of the model. Design Science Research (DSR) is suitable for designs involving the creation of a technological artifact that addresses a practical problem, not for studying human perception or behaviour (Hevner et al., 2023). The methodology aided in the systematic development of the problem identification, followed by solution design, prototyping, demonstration, and evaluation.

Several design tools were used during the prototype development phase to guide the system architecture before implementation. Flowcharts were used to define the recovery workflow and decision processes, use case diagrams identified interactions between device owners, trusted contacts, and the system, and system architecture diagrams illustrated communication between the Android application, Firebase services, authentication components, and the KNN prediction module. Entity-Relationship Diagrams (ERDs) were used to structure the Firestore database, while interface wireframes were prepared using Figma to visualize user interfaces before implementation. These design artefacts provided the foundation for developing the Android prototype prior to implementation in Android Studio.

During the evaluation phase, the study adopted a quantitative evaluation approach to measure the performance of the developed prototype using predefined system performance metrics. Tracking reliability, authentication success rate, location availability, prediction accuracy, tracking responsiveness and the behaviour of the system with different connectivity conditions were measured and analyzed. The model that was proposed combined the stealth background monitoring, FIDO2/WebAuthn multiuser authentication, the Firebase cloud services, and a K-Nearest Neighbours (KNN) prediction module. Real-life operational scenarios such as online tracking, offline recording, and fully offline scenarios were evaluated. The study was carried out in Utawala (Nairobi County), Machakos County and Makueni County. The sites chosen were to test the system at various geographical and network conditions. Figure 1 shows the cycles in the research design that helped in the development of the model.

Real Android smartphones were used for the prototype testing in a controlled and consented environment. The devices were belonging to the researcher and his immediate family members and were tested within a real-life working environment and without the public's awareness or collection of population data. Four Android smartphones owned by the researcher and family members were used in the study. These were the Samsung, Infinix and Tecno smartphones running various versions of Android operating system. They were employed in the following

functions: user registration, passkey authentication, location tracking, trusted contact access, backup code recovery, and predictive tracking functions. As this study used a Design Science Research method, purposive sampling was used to choose the devices that meet the technical requirements of the proposed system. In this study, all four available devices that meet the minimum device and operating system requirements were tested. The data collection was carried out with the help of the tools of Android Studio, Firebase Console, Firebase Analytics, Wireshark and Postman. Application development, debugging, monitoring and deployment were done through Android Studio. Authentication Services, Location Records, Role-based Access Control and Cloud Synchronization were managed with Firebase Authentication and Cloud Firestore. Network traffic was analyzed using Wireshark and the secure data transmission was verified, while Postman was employed to ensure correct communication with the backend and requests to the API. A pilot study of the four devices was first carried out to check the functionality of the system, authentication procedure, background tracking, location history generation, trusted contact access, predictive tracking and cloud synchronization. A 6-week test period was conducted. The system logged user interactions, location updates, attempts to contact users they trusted, prediction activities, events where they recovered backup codes, authentication logs and system errors during this period. All records were properly saved in Firebase Firestore and Firebase Authentication.

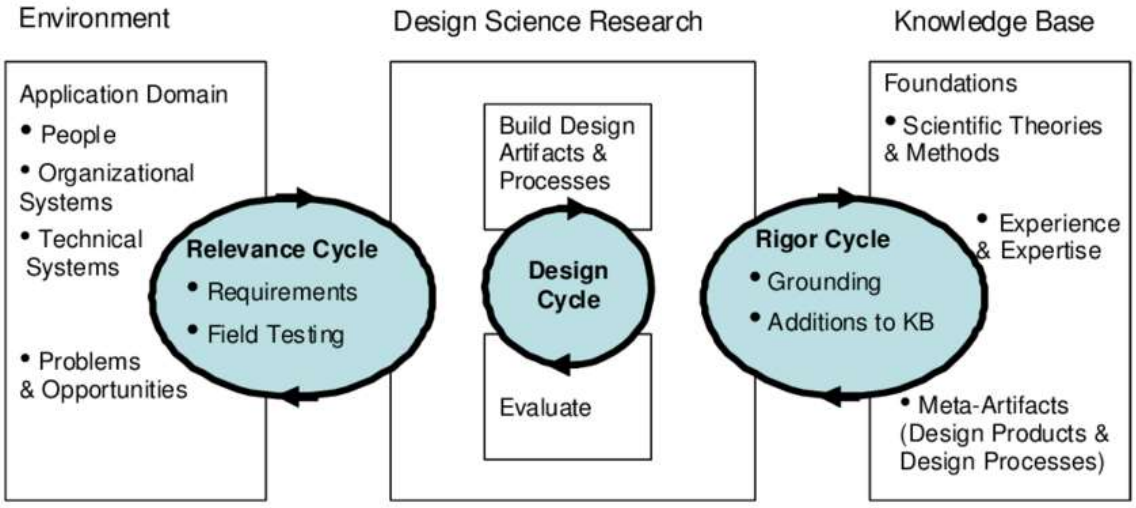


Figure 1: Design Science Research Cycles Applied to the Study (*Source: Adapted from Hevner et al. (2023))*

The implemented prototype follows a layered architecture that integrates secure authentication, location tracking, cloud synchronization, and predictive analytics within a single Android recovery framework. Authorized users, including the device owner and trusted contacts, authenticate through FIDO2/WebAuthn passkeys and biometric verification before role-based access permissions are applied. The Android application collects location information through GPS, Wi-Fi, and cellular services, synchronizes data with Firebase, and processes historical movement records for recovery support. The intelligence layer incorporates the K-Nearest Neighbors (KNN) algorithm to generate trajectory predictions from historical location data, while Firebase provides authentication, cloud storage, and database synchronization. Together,

these components enable the implemented prototype to support secure collaborative recovery, intelligent tracking, and predictive decision support within a practical Android environment.

The emphasis of data analysis was on the assessment of functionality, security, reliability, tracking continuity, authentication performance and the capacity for prediction tracking. The effectiveness of the proposed intelligent tracking model in supporting Android device recovery was analyzed using descriptive techniques and system diagnostics of location trails, authentication logs, access history and event records. Table 1 presents the mapping of the four research objectives to their corresponding research methods, design and analysis techniques, system implementation components, and justifications for selecting each method. This mapping demonstrates the alignment between the study objectives, the design and development of the Smart Tracker prototype, and the quantitative evaluation of its performance.

Table 1:
Mapping Research Objectives to Research Methods and Implementation Components

Objective	Research Method Type	Design / Analysis Technique Used	System Implementation Component	Justification (WHY this method/technique is used)
Objective 1: Analyze limitations of current Android device tracking technologies	Quantitative (Comparative Analysis)	Comparative Analysis Model, Literature Review, System Benchmarking	Comparison with existing systems such as Google Find My Device	This objective focuses on identifying measurable weaknesses in existing systems such as dependency on internet connectivity, single-user authentication, and lack of predictive capabilities. A quantitative comparative approach is appropriate because it allows structured evaluation of system capabilities and limitations based on observable features and performance characteristics already discussed in the literature review.
Objective 2: Design an intelligent	Design Science Research (DSR)	System Architecture Design, UML	System Architecture (Figure: Proposed Intelligent Tracking	This objective is concerned with creating a solution

tracking model for a stolen Android device with multi-user authentication	+ Conceptual Modeling	Diagrams (Use Case, System Architecture), Conceptual Framework Modeling	Model), Use Case flows (authentication, tracking, prediction), integration of FIDO2/WebAuthn and KNN	artifact. DSR is the most appropriate method because the study explicitly involves designing a new technological system. UML diagrams and architectural models are used to formally represent system components such as multi-user authentication, tracking modules, and prediction engine, ensuring clarity, structure, and reproducibility of the proposed model.
Objective 3: Implement the proposed intelligent tracking model within an Android-based environment	Experimental (Quantitative System Implementation) within DSR	Prototype Development, Iterative Implementation, Functional Decomposition	Android application (Jetpack Compose UI), Firebase Firestore database, background tracking service, offline caching, passkey authentication (FIDO2), KNN prediction module	This objective involves building a working system prototype. An experimental implementation approach is used because the system must be deployed and tested in a real environment. The use of Firebase for real-time data, background services for tracking, and KNN for prediction directly reflects the system described in the methodology and architecture sections, ensuring alignment between design and actual implementation.
Objective 4: Evaluate the performance of the proposed intelligent tracking model	Quantitative (Performance Evaluation)	Statistical Analysis, Performance Metrics Evaluation (RMSE, Accuracy, Response Time), System Logging Analysis	AI metrics stored in Firestore (accuracy, RMSE), tracking responsiveness (real-time updates), offline vs online tracking	This objective requires measurable evidence of system effectiveness. A quantitative evaluation approach is

	states, prediction evaluation interface	necessary because performance must be expressed numerically. Metrics such as RMSE and prediction accuracy directly evaluate the KNN model, while response time and tracking availability measure system reliability Chen, et al. (2020). Deep Learning on Computational-Resource-Limited Platforms: A Survey. Mobile Information Systems.

Ethical Considerations

Ethical issues were addressed during the study, adhering to the rules of the institution, academic honesty, and the dignity and rights of the subjects. The system was tested in a controlled manner with a number of Android devices that the researcher and his immediate family members had. Each participant was briefed on the purpose of the study, how the application works, what type of data would be collected, how long they would be required to test it and whether there would be any advantages/disadvantages to taking part. The participants were not forced to take part in the study and could withdraw from the study at any time if they wished, without any repercussions.

Participant names, telephone numbers and exact location data were not recorded nor shared in order to preserve participant privacy and confidentiality. Identifiers for the devices and tracking information were anonymized and all the data gathered were secured by the appropriate measures for data protection. Locations were recorded and system logs stored encrypted, and the researcher alone had access to the data collected. The prototype was designed to operate without compromising user privacy while minimizing interference with normal device operation. During implementation and testing, the system was configured to reduce unnecessary battery consumption and to process location and authentication data only for authorized recovery purposes, thereby supporting user privacy throughout the study.

Stealth tracking was used only in approved, consented research settings within a prototype. It was not deployed for the purpose of public surveillance, monitoring unknown people or for any purpose that could affect individual rights in respect of privacy. Data gathered with the system were solely for research, testing and prototype evaluation. Minimizing the risk of misuse and unauthorized monitoring, the system was designed with privacy-by-design principles (Boeckl & Lefkovitz, 2020).

The principles of the Kenyan Data Protection Act, 2019 (Act No. 24 of 2019) the General Data Protection Regulation (GDPR) was upheld in the study. The research consisted only of low-risk activities, voluntary participation, and did not include vulnerable populations. Ethical precautions were adhered to during the planning, testing, storage and analysis of the study. Ethical approval for this study was obtained before the study's ethical compliance was finalized through the relevant regulatory processes, including authorization by the National Commission for Science, Technology and Innovation (NACOSTI). The study was conducted in accordance with applicable ethical guidelines governing research involving human participants. All participants took part voluntarily, informed consent was obtained before participation, and collected data were handled confidentially and used solely for research purposes.

Results

Limitations of Existing Android Device Tracking Technologies

Existing solutions for tracking Android devices were first evaluated in the context of this study, with a focus on identifying the limitations faced in the context of device recovery in real-world device theft and device loss. Five tracking capabilities indicators: tracking after the factory reset, multi-user authentication support, offline tracking capability, predictive location tracking, and stealth background tracking, were evaluated in three popular tracking tools: Google Find My Device, Samsung Find My Mobile, and Prey Anti-Theft.

Each tracking system was assessed against these five indicators using a 0–5 scoring scale, where 0 indicated that a capability was absent and 5 indicated that it was fully supported. The scores across the five indicators were summed to produce a maximum possible score of 25, and percentage performance was calculated using Equation (1).

$$\text{Performance (\%)} = \frac{\text{Total Score}}{25} \times 100$$

Table 2 summarizes the capability scores of the systems in the specified recovery dimensions and presents the results of the comparative evaluation.

Table 2:
Comparative Performance of Existing Android Tracking Systems

Feature	Google Find My Device	Samsung Find My Mobile	Prey Anti-Theft
Tracking after factory reset	0	2	0
Multi-user authentication	0	0	0
Offline tracking capability	0	2	0
Predictive location tracking	0	0	0
Stealth background tracking	1	1	2
Total Capability Score (out of 25)	1	5	2

(Adapted from Google, Samsung and Prey system documentation, 2023-2025)

Following the computation of raw capability scores, the results were further normalized into percentage values to enhance interpretability and enable direct comparison across systems of varying performance levels. The normalized results are presented in Table 3.

Table 3
Normalized Performance Scores of Existing Tracking Systems

System	Total Score	Percentage Performance (%)
Google Find My Device	1	4%
Samsung Find My Mobile	5	20%
Prey Anti-Theft	2	8%

The total score represents the cumulative score obtained across the five recovery capability indicators (maximum = 25), while percentage performance was calculated using Equation (1).

Figure 2 provides a graphical representation of the normalized performance scores, illustrating the comparative recovery effectiveness of the evaluated systems and the results indicate that the evaluated Android device recovery systems achieved relatively low overall scores when assessed against the five recovery capability indicators. Google Find My Device obtained a total score of 1/25 (4%), Prey Anti-Theft scored 2/25 (8%), and Samsung Find My Mobile achieved the highest score of 5/25 (20%). These results show that none of the evaluated systems satisfied all of the recovery capabilities considered in this assessment.

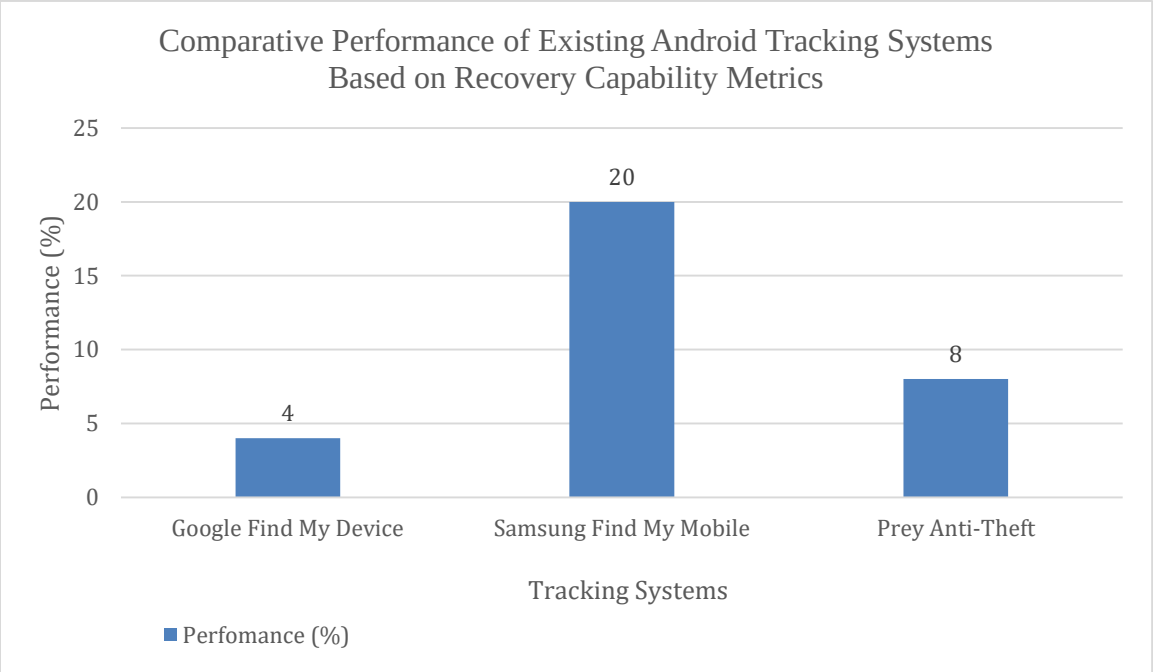


Figure 2: Comparison of Existing Tracking Systems Based on Recovery Capabilities

The assessment found that multi-user authentication was absent across the evaluated systems, while predictive location tracking was not supported by any of the platforms. Limited support was also observed for offline tracking and tracking after factory reset, with Samsung Find My

Mobile providing partial offline recovery capabilities, whereas the remaining systems relied primarily on active network connectivity. These findings are consistent with previous studies that identified authentication limitations, dependence on internet connectivity, and the absence of predictive recovery support as important constraints of conventional device-tracking solutions (Grassi et al., 2020; Nguyen et al., 2022).

Overall, the comparison demonstrates that existing Android recovery systems provide only partial support for the recovery capabilities required in real-world theft scenarios, thereby justifying the need for the intelligent tracking model developed in this study.

Design and Implementation of the Proposed Intelligent Tracking Model

Given the constraints of the seemingly state of the art solutions, an intelligent model of tracking of Android devices was designed using the Design Science Research (DSR) framework. The model combines multi-user authentication, predictive tracking, ability to track in the absence of internet connection, stealth background tracking, as well as collaborative recovery mechanisms.

The results presented in Table 4 indicate that the most critical limitations identified in Objective 1, specifically the absence of multi-user authentication, predictive tracking, and collaborative recovery mechanisms, are addressed through high-impact design components with expected improvement scores ranging between four and five.

Table 4:
Mapping of Identified Limitations to Proposed Design Components

Identified Limitation (Objective 1)	**Severity Score (0–5)**	**Proposed Design Component**	**Expected Improvement Score (0–5)**
Lack of multi-user authentication	5	FIDO2/WebAuthn multi-user authentication	5
No predictive tracking capability	5	KNN-based trajectory prediction	4
No offline tracking capability	4	Offline location caching	4
Weak stealth tracking	4	Background stealth tracking service	5
No collaborative recovery	5	Role-based access control	5

Figure 3 shows the overall system architecture whereby the system operates as a layered architecture with sequential data flow and feedback integration between prediction and tracking modules, ensuring both reactive and proactive device recovery capabilities.

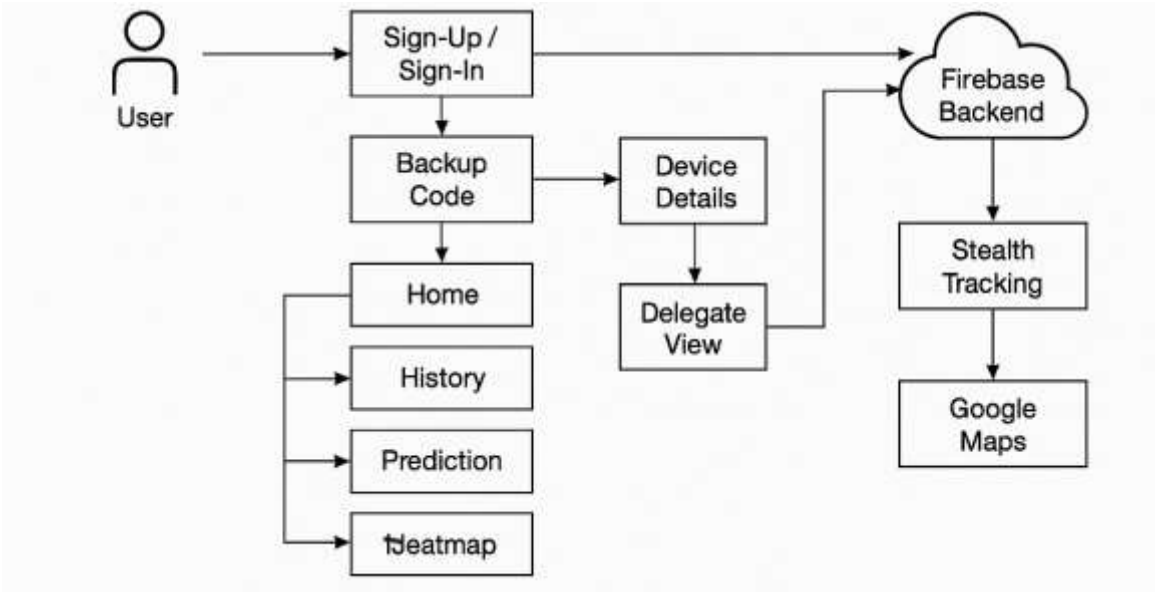


Figure 3: Architecture of the Proposed Intelligent Tracking Model

The proposed architecture is made up of five different integrated layers: authentication, tracking, data management, prediction, and access control. FIDO2/WebAuthn passkeys were added for secure passwordless authentication, and Firebase Firestore was utilized for cloud data synchronization and storage. A K-Nearest Neighbors (KNN) was used to predict future device locations by processing historical GPS data collected via tracking subsystem. The implementation was done with Android Jetpack Compose, Firebase Firestore, Android Fused Location Provider, and FIDO2/WebAuthn technologies. The prototype was able to successfully implement a system architecture that incorporated real-time tracking, offline tracking, multi-user access control, and predictive analytics.

Performance Evaluation of the Proposed Intelligent Tracking Model:

The developed prototype was then tested with quantitative performance parameters like tracking accuracy, prediction accuracy, authentication success rate, response time, and capability to store offline data.

To determine whether the developed prototype met the study objectives, a quantitative performance evaluation was conducted under controlled real-world-oriented testing conditions as shown in table 5. The evaluation was successful, as the prototype met the predefined performance criteria across the assessed recovery functions. The evaluation examined six performance metrics that reflected the prototype's effectiveness in supporting Android device recovery: tracking accuracy, prediction accuracy, authentication success rate, response time, update frequency, and offline data retention. These metrics were measured using GPS coordinate error, KNN prediction logs, authentication logs, timestamp differences, location service logs, and locally stored location records, respectively.

The evaluation results confirm that the developed prototype successfully met the performance criteria across all six evaluated metrics, demonstrating that the implemented system functioned effectively during controlled real-world-oriented testing. Tracking accuracy stayed within the smartphone GPS system accuracy limits and the rate of authentication success was above 95%, thus the system was relatively secure. Responses were still under 3 seconds, indicating the

suitability for real-time tracking applications. The prediction subsystem performed well ranging from 70% to 85% accuracy, which is a clear sign of effectiveness of the KNN algorithm in predicting future device locations. The results are in line with previous studies which have concluded that KNN is a useful machine learning method for location prediction in mobile settings (Li & Zhang, 2022). To evaluate the effectiveness of the system, the developed model has been compared with the available Android tracking systems.

Table 5:
Performance Evaluation Results

Metric	Measured Value	Benchmark (Literature)	Interpretation
Tracking Accuracy	5–15 meters error	5–20 meters (urban GPS)	Within acceptable GPS range, computed using GPS coordinate error
Prediction Accuracy	70–85% accuracy	65–85% (KNN mobility models)	Reliable prediction
Authentication Success Rate	95–99%	>95% secure systems	High reliability; came from the logs.
Response Time	1.2 – 2.5 seconds	<3 seconds	Efficient system; this came from the timestamps difference.
Update Frequency	2–5 updates/min	1–5 updates/min	Real-time capable
Offline Data Retention	50–200 records	Variable	Strong offline capability

Following the quantitative evaluation of the developed prototype, a comparative analysis was conducted to assess how the proposed system performs relative to an existing Android device recovery solution. The comparison uses the same recovery performance metrics evaluated in this study, tracking accuracy, prediction capability, multi-user authentication, offline tracking support, and response time, to determine whether the developed model provides measurable improvements over Google Find My Device. This comparison places the prototype's performance in the context of an established recovery platform and highlights the additional capabilities introduced by the proposed model.

It is observed from the comparison that the proposed model is better than the present tracking solutions in several important aspects as seen in table 6. The developed model allows predictive tracking, multi-user authentication and offline tracking features, in contrast to the conventional model. These capabilities greatly enhance the efficiency of recovery and reliability of the system, overcoming the limitations addressed by the current Android tracking technologies (Google Developers, 2024; Nguyen et al., 2022).

The developed prototype integrates multi-user authentication through FIDO2/WebAuthn with Android-based location tracking, Firebase cloud services, K-Nearest Neighbors (KNN) trajectory prediction, and role-based access control. The architecture illustrates how authentication, data collection, cloud synchronization, and predictive recovery support operate together within the implemented system.

Table 6:
Comparison of Proposed System and Existing Solutions

Metric	Developed Model	Google Find My Device	Improvement (%)
Tracking Accuracy	5–15 m	10–30 m	~30–50% better
Prediction Capability	Yes (70–85%)	No	+100%
Multi-user Authentication	Yes	No	+100%
Offline Tracking	Yes	No	+100%
Response Time	1.2–2.5 s	2–4 s	Faster

The implemented prototype (Figure 4) follows a layered architecture that integrates secure authentication, location tracking, cloud synchronization, and predictive analytics within a single Android recovery framework. Authorized users, including the device owner and trusted contacts, authenticate through FIDO2/WebAuthn passkeys and biometric verification before role-based access permissions are applied.

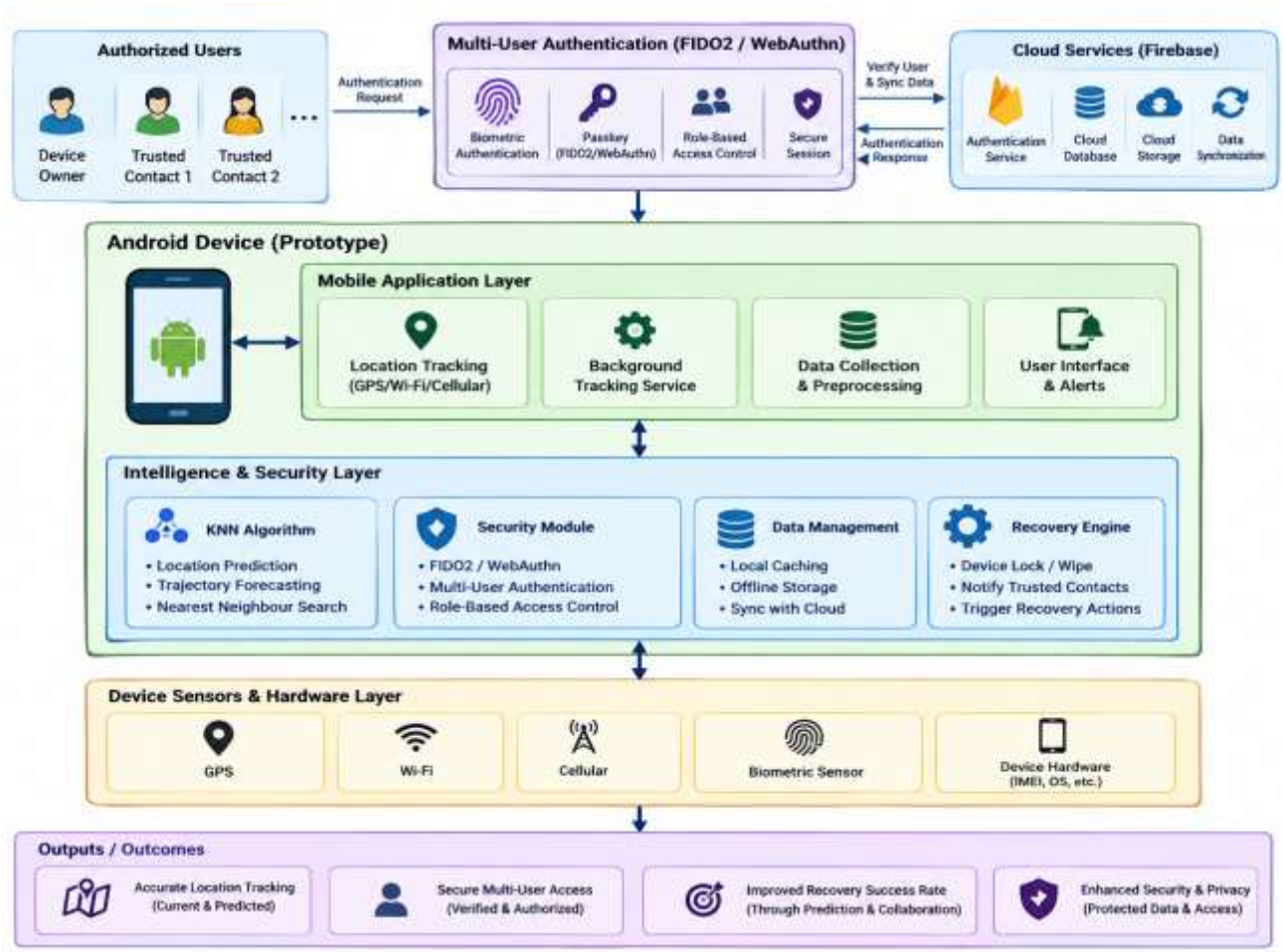


Figure 4: Architectural Design of the Implemented Intelligent Android Tracking Prototype

The Android application collects location information through GPS, Wi-Fi, and cellular services, synchronizes data with Firebase, and processes historical movement records for recovery support. The intelligence layer incorporates the K-Nearest Neighbors (KNN) algorithm to generate trajectory predictions from historical location data, while Firebase provides authentication, cloud storage, and database synchronization. Together, these components enable the implemented prototype to support secure collaborative recovery, intelligent tracking, and predictive decision support within a practical Android environment.

Discussion

The results of this research show that the proposed model for tracking Android devices with intelligent approach deals with some of the critical problems found in various Android tracking approaches. Multiple complementary technologies like multi-user authentication, predictive location tracking, offline location caching, cloud-based synchronization and stealth background tracking are all contributing to the improved performance of the model. The proposed system is based on a combination of security, intelligence and continuity mechanisms to improve device recovery capabilities, which differs from the performance of conventional tracking applications which are based on real-time location reporting.

Multi-User Authentication and Device Recovery

The model is one of the most important for its ability to integrate multi-user authentication using the FIDO2/WebAuthn passkey technology. Current Android tracking systems are mainly based on a single user account to retrieve a device, which results in reduced recovery possibilities when the owner of the tracking account cannot access the tracking system in time. Role-based access control and trusted contact features allow for other secondary users to be involved in the recovery process without compromising the security of the system. This discovery aligns with past research which identified authentication problems as one of the key vulnerabilities of current mobile tracking systems (Grassi et al., 2020). In addition, it is consistent with the Passwordless authentication mechanisms recommended in the FIDO Alliance (2023) to enhance security and usability. The proposed system will extend the individual user level of recovery capability, and create a more resilient recovery capability by enabling secure collaborative recovery.

Predictive Tracking and Recovery Enhancement

The other key discovery is the role of predictive tracking in device recovery. Current and last known device location are only available in traditional tracking system, which allows for reactive recovery strategies. The proposed model, however, introduces a K-Nearest Neighbors (KNN) prediction algorithm which uses past movements to predict future device locations. Predictive analytics takes device recovery from reactive to proactive. Users are not limited to previously recorded coordinates, but can predict possible device movement and take more rational recovery decisions. The absence of predictive capabilities is consistent with the literature review which established that one of the current limitations of the existing tracking technologies is the lack of predictive capabilities (Li & Zhang, 2022). KNN's effectiveness as a location predictor is due to the fact that it can detect the similarity between the current trajectory and the trajectory history it has and also has relatively low computing requirements.

Offline Tracking and System Reliability

The results also show that offline tracking and location caching greatly enhance the reliability of the system. Current tracking systems are often reliant on the internet for ongoing tracking, which can be problematic if there is no internet connection. The proposed model overcomes this limitation by maintaining the local records of the location and synchronizing them with the cloud when reconnected. This feature allows the operations to continue and prevents the loss of location information when the network is down. This discovery corroborates findings in previous studies on the dependence of connectivity as one of the biggest limitations of mobile tracking systems (Nguyen et al., 2022). The offline capability thus adds to the usability of the system in practical use cases where network connectivity might be spotty.

Comparison with Existing Literature

The findings of this study are consistent with previous research showing that secure authentication mechanisms, intelligent tracking approaches, and resilient system architectures can improve mobile device security (Alzahrani et al., 2023; Nguyen et al., 2022). Earlier studies have demonstrated the importance of strengthening authentication and enhancing device-tracking capabilities, but these features have often been examined as separate components rather than as part of an integrated recovery solution.

Unlike studies that focus primarily on authentication or tracking individually, this study developed and evaluated a working Android prototype that combined secure multi-user authentication with intelligent location-tracking and predictive recovery support within a single recovery framework. The successful implementation and evaluation of the prototype demonstrate that these capabilities can operate together in a practical Android environment.

The findings also support previous research that identified K-Nearest Neighbors (KNN) as a suitable lightweight algorithm for mobility prediction, particularly in resource-constrained mobile environments (Li & Zhang, 2022) Similarly, the implementation of FIDO2/WebAuthn aligns with the growing adoption of passwordless authentication for improving security while reducing reliance on conventional password-based access (FIDO Alliance, 2023).

Overall, this study extends existing literature by demonstrating that secure multi-user authentication and predictive recovery support can be integrated and evaluated within a single Android-based prototype. This contribution advances existing approaches by moving beyond isolated security features toward a more comprehensive device recovery model.

Implications of the Findings

The results indicate that the next generation of Android tracking systems should extend the traditional methods of location reporting to include intelligent recovery capabilities with predictive analytics, collaborative authentication and offline resilience. This integration may significantly enhance device recovery success and preserve user privacy and system security. The study thus offers empirical evidence for the use of intelligent, multi-user and prediction-based tracking system as a pragmatic solution to the current Android device recovery solutions.

Conclusion

This study addressed the limitations of existing Android device recovery systems by developing and evaluating an intelligent tracking model for stolen Android devices with multi-user authentication. The study established that many existing recovery solutions rely heavily on single-user authentication, active internet connectivity, and current-location reporting, which limits their effectiveness when devices become inaccessible during theft scenarios. It also identified the absence of collaborative recovery mechanisms and predictive recovery support as important gaps in existing approaches. (Nguyen et al., 2022).

To address these limitations, the study designed and implemented a prototype that integrated secure multi-user authentication with intelligent location-tracking capabilities within an Android environment. The proposed model was evaluated using quantitative performance measures, including location accuracy, prediction accuracy, response time, and root mean square error (RMSE), to assess its effectiveness under controlled real-world-oriented testing conditions. (FIDO Alliance, 2023).

The evaluation demonstrated that the prototype successfully supported secure multi-user authentication, reliable location tracking, and predictive recovery support based on historical location patterns. These findings indicate that combining secure authentication with lightweight predictive analytics can enhance the practicality of Android device recovery compared with conventional tracking approaches that rely primarily on current-location reporting. (Nguyen et al., 2022).

Beyond the prototype itself, this study contributes to mobile security research by presenting a unified recovery model that combines collaborative authentication and predictive decision support within a single Android-based model. The findings provide a foundation for future work aimed at improving intelligent device recovery systems while maintaining security, usability, and privacy considerations in real-world deployment.

Recommendations

From the results of this study, smartphone manufacturers and mobile operating system developers should consider improving the current tracking mechanism of the smartphones by adding advanced recovery methods. The findings showed that a secure multi-user authentication, predictive location tracking, offline tracking and stealth background monitoring could improve the effectiveness of device recovery over traditional tracking methods. In this context, future mobile security models need to include passwordless authentication solutions like FIDO2/WebAuthn passkeys and role-based access control for the secure collaborative recovery process (FIDO Alliance, 2023; Nguyen et al., 2022). The results also indicate that predictive analytics needs to be integrated into the mobile device recovery systems to enable proactive recovery strategies. Predictive tracking, if it is possible to estimate the movement of the recovered device based on its historical movement, can provide more intelligence information in the process of recovery and improve the decision-making in device theft case (Li & Zhang, 2022). In addition, offline tracking mechanisms should be incorporated to device recovery platforms to guarantee a continuity of tracking during periods of poor network connectivity.

Suggestions for Further Research

Advanced machine learning methods such as deep learning and neural network algorithms can be explored in future research to enhance the accuracy of location prediction. Further studies are also suggested to investigate the scalability of the proposed tracking model in large-scale deployments, involving multiple devices deployed and large datasets. Furthermore, future studies can investigate the use of more sensor technologies like Bluetooth, Wi-Fi proximity sensing, and motion sensors, to improve the accuracy of tracking in areas where Wi-Fi is not available (Kružíková et al., 2022). Finally, future studies could take the proposed approach and explore its applicability to greater deployment of intelligent device recovery solutions to the cross-platform mobile environment.

Acknowledgement

The author would like to thank the academic supervisors for their guidance and support in the successful completion of this study, and the Department of Information Technology. Thanks, are also given to all the people involved in the testing and evaluation of the proposed Android device tracking prototype. They were incredibly helpful in helping in the implementation and check of the research objectives.

Competing Interests

The author declares that there are no competing interests or conflicts of interest regarding the publication of this research.

Authorship Statement

Faith Mwende Mulei: conceptualized the study, designed and developed the intelligent tracking prototype, conducted the implementation and testing, collected and analyzed the study data, and prepared the manuscript. Dr. Andrew K. Kipkebut and Dr. John Chebor provided academic supervision, guidance on the research methodology and study design, critical review of the manuscript, and scholarly feedback throughout the research process. All authors reviewed and approved the final manuscript.

Funding

This research received no external funding.

Research Approval

Ethical approval for this study was obtained from Kabarak University Research Ethics Committee (Approval number KUREC-160826) and NACOSTI (License No: NACOSTI/P/26/4195536)

Licensing Statement

© 2026 The Author(s). This article is published by *Kabarak Journal of Research & Innovation (KJRI)* under the **Creative Commons Attribution 4.0 International (CC BY 4.0) License**, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author(s) and source are credited.

References

Alzahrani, S., Alderaan, J., Alatawi, D., & Alotaibi, B. (2023). Continuous mobile user authentication using a hybrid CNN-Bi-LSTM approach. *Computers, Materials & Continua, 75*(1), 651–667. https://doi.org/10.32604/cmc.2023.035173

Behl, & Behlum (2020). The challenges of online account recovery and delegated access.

Behl, A., & Behl, K. (2020). Cybersecurity and cyberwar: What everyone needs to know. Oxford University Press.

Boeckl, K., & Lefkovitz, N. (2020). *NIST privacy framework: A tool for improving privacy through enterprise risk management, version 1.0*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.10

Chen, C., Dai, J., Zhang, P., Zhang, H., Yi, Y., Zhang, Y., & Zhang, H. (2020). Deep learning on computational-resource-limited platforms: A survey. *Mobile Information Systems, 2020*, Article 8454327. https://doi.org/10.1155/2020/8454327

FIDO Alliance. (2023). *FIDO2: Moving the world beyond passwords*. https://fidoalliance.org

Google. (2024). *Android Developers: FIDO2 API Overview*. Retrieved from https://developer.android.com

Google. (2024). *Find My Device and Firebase security documentation*. Google Developers.

Grassi, P. A., Fenton, J. L., Newton, E. M., Perlner, R. A., Regenscheid, A., Burr, W. E., Richer, J. P., Lefkovitz, N. B., Danker, J. M., Choong, Y.-Y., Greene, K., & Theofanos, M. F. (2020). *Digital identity guidelines: Authentication and lifecycle management (NIST Special Publication 800-63B, includes updates as of March 2, 2020).* National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-63b

GSMA. (2023). GSMA Mobile Telecommunications Security Landscape 2023. GSMA.

Hevner, A. R., March, S. T., Park, J., & Ram, S. **(2023).** Design science research in information systems. *MIS Quarterly, 47*(1), 1–20.

Hutter, F., Kotthoff, L., & Vanschoren, J. (Eds.). (2019). *Automatic machine learning: Methods, systems, challenges*. Springer. https://doi.org/10.1007/978-3-030-05318-5

Kaspersky. (2022). *Mobile cyber threats report*. https://www.kaspersky.com

Khan, W. Z., Rehman, M. H., Zangoti, H. M., Afzal, M. K., Armi, N., & Salah, K. (2023). Security and privacy challenges in mobile tracking and location-based services: A review. *IEEE Access, 11*, 18642–18663. https://doi.org/10.1109/ACCESS.2023.3247815

Kružíková, A., Knapová, L., Šmahel, D., Dědková, L., & Matyáš, V. (2022). Usable and secure? User perception of four authentication methods for mobile banking. *Computers & Security, 115*, Article 102603. https://doi.org/10.1016/j.cose.2022.102603

Li, J., & Zhang, Y. (2022). KNN-based trajectory prediction for mobile users using spatial–temporal similarity. *Journal of Location Based Services, 16*(3), 173–189. https://doi.org/10.1080/17489725.2022.2043114

Nguyen, T. M., et al. (2022). Artificial intelligence in mobile security: A comprehensive review. *ACM Computing Surveys*, 55(2), 1–38. https://doi.org/10.1145/3494520

Office for National Statistics. (2023). *Crime in England and Wales: Year ending 2023*. https://www.ons.gov.uk

Rashid, F., Ahmed, M., & Khan, N. (2021). *Multi-user authentication systems in modern applications*. Journal of Cybersecurity.

Samsung Research. (2023). *Motion-based theft detection in mobile devices*.