International Journal of Advanced Research in Computer Science & Technology (IJARCST)

| ISSN: 2347-8446 | www.ijarcst.org | editor@ijarcst.org |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 9, Issue 3, May-June 2026||

DOI:10.15662/IJARCST.2026.0903005

Darkshield: Mobile Intrusion Detection using Post-Authentication Failure Analysis and Android Security APIS

Dr.V. Seedha Devi[1], M. Parvinraj[2], J. Dinesh[3], M. Venkatramana[4], P. Suryaprakash Raj[5]

Associate Professor, Department of Information Technology, Jaya Engineering College, Anna University, Chennai, Tamil Nadu, India[1]

UG Student, Department of Information Technology, Jaya Engineering College, Anna University, Chennai, Tamil Nadu, India[2,3,4,5]

Publication History: Received: 25.04.2026; Revised: 01.05.2026; Accepted: 03.05. 2026; Published: 09.05.2026.

ABSTRACT: Smartphones store sensitive personal, financial, and confidential data, making them frequent targets for theft and unauthorized access. Traditional security methods such as PINs, passwords, and biometrics mainly prevent entry but offer limited protection after repeated intrusion attempts. This paper presents DarkShield, an Android-based intrusion detection and anti-theft system that proactively detects suspicious unlock attempts and alerts the rightful owner. When multiple incorrect PIN or password entries are detected, the system captures the intruder's image, retrieves the current GPS location, uploads the evidence to cloud storage, and sends alerts through SMS and email. SMS notifications include the location and image link, while emails contain location details and the captured image as an attachment. The system also supports offline SMS alerts, online email notifications, and SIM change detection for unauthorized SIM replacement. To reduce false alerts, a machine learning-based face recognition module verifies whether the captured face matches the authorized user. By integrating evidence capture, location tracking, dual alert mechanisms, SIM monitoring, and intelligent face verification, DarkShield provides an effective solution for smartphone theft detection and unauthorized access prevention.

KEYWORDS: Smartphone security, mobile theft detection, intrusion detection, offline SMS alert, face recognition, SIM change detection, GPS tracking, Cloudinary, Android security.

I. INTRODUCTION

Smartphones have become an integral part of modern life, serving as primary devices for communication, banking, education, business, and storage of personal information. They contain sensitive data such as passwords, financial records, private messages, photographs, and access credentials to online services. As smartphone dependency continues to grow, device theft and unauthorized access have emerged as serious security concerns. Losing control of a smartphone can result not only in hardware loss but also in privacy breaches, identity theft, and misuse of confidential information.

Most smartphones rely on conventional authentication mechanisms such as PINs, passwords, pattern locks, fingerprints, and facial recognition to restrict unauthorized access. Although these methods provide an initial layer of protection, they mainly focus on preventing entry rather than responding intelligently to suspicious repeated access attempts. If an intruder repeatedly enters incorrect credentials, many existing systems simply lock the device temporarily without collecting evidence or notifying the legitimate owner. This limitation reduces the chances of timely action and device recovery. To address these challenges, this paper presents DarkShield, an advanced Android-based mobile intrusion detection and anti-theft system designed to proactively monitor suspicious unlock attempts and generate real-time alerts. When repeated incorrect PIN or password entries are detected, the system automatically captures the intruder's image using the device camera, retrieves the current GPS location, and uploads the captured evidence to Cloudinary to generate a secure image URL. The system then sends notifications to trusted contacts through SMS and email. SMS alerts contain the location and image link, while email alerts include detailed information with the captured image attached.

| ISSN: 2347-8446 | www.ijarcst.org | editor@ijarcst.org |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 9, Issue 3, May-June 2026||

DOI:10.15662/IJARCST.2026.0903005

DarkShield is further enhanced with an offline SMS alert mechanism to ensure notifications can still be delivered when internet connectivity is unavailable. In addition, the system provides SIM change detection, where unauthorized replacement of the device SIM card is identified and the new carrier details are sent to the registered trusted contact. This feature improves the chances of tracing the device after theft. Another major challenge in intrusion detection systems is false alerts. In some situations, the legitimate owner may accidentally enter an incorrect PIN, which could unnecessarily trigger notifications. To overcome this issue, DarkShield integrates a machine learning-based face recognition module. After a failed unlock attempt, the captured face image is compared with the pre-registered authorized user's face data. If the face matches the legitimate owner, alerts are suppressed; otherwise, the system confirms unauthorized access and triggers notifications.

By combining intrusion image capture, location tracking, cloud-based evidence storage, offline and online alerts, SIM monitoring, and intelligent face verification, DarkShield provides a comprehensive smartphone security framework. The proposed system aims to improve theft detection, reduce false alarms, support rapid response, and enhance the overall security of Android mobile devices.

II. LITERATURE REVIEW

Mrs. E. Shalini and Dr. V. Shanthi [1] introduced a location-based anti-theft image capture application with culprit identification for smartphones. The system combines GPS tracking with intruder image capture to help owners trace stolen devices and identify unauthorized users. It improves evidence collection during theft incidents and enhances the chances of device recovery.

Godavarthy Sri Padma Praneeth et al. [2] developed an intruder detection and email alerting system that automatically captures images during suspicious access attempts and sends alerts to the owner through email notifications. The proposed system enables remote monitoring and provides quick evidence sharing to the rightful user. It also improves user awareness by instantly reporting unauthorized access attempts. The captured evidence can assist in identifying the intruder and support further investigation. However, the system mainly depends on internet connectivity for timely email delivery.

Mrs. Priyanka Gupta et al. [3] proposed an anti-theft device tracking system focused on monitoring smartphone location and assisting users in recovering lost or stolen devices through tracking mechanisms. The system increases recovery possibilities by continuously updating device coordinates and movement status.

Mattipelli Sandeep Kumar et al. [4] presented a forensics activity logger to extract user activity from devices. The system records smartphone activities and provides digital evidence useful for post-incident investigation and forensic analysis. It supports investigators in identifying suspicious actions performed on compromised devices.

P. Preethi et al. [5] introduced a theft alert call and SMS system that sends immediate notifications through calls and text messages during theft incidents, especially when internet connectivity is unavailable. The system ensures faster communication with the owner and improves response time during emergencies.

III. PROBLEM STATEMENT

The widespread use of smartphones for digital payments, personal communication, academic work, and access to online services has made them valuable targets for theft and misuse. A stolen or compromised smartphone can expose sensitive information such as banking data, private files, saved credentials, and personal contacts. Protecting mobile devices has therefore become a critical security requirement. Existing smartphone protection methods are largely limited to screen-lock authentication such as PINs, passwords, patterns, or biometrics. While these mechanisms attempt to block unauthorized access, they do not actively respond when suspicious attempts occur. If multiple wrong unlock attempts are made, many devices simply delay further access attempts without collecting evidence or informing the owner. Another challenge is the lack of dependable alert mechanisms during theft situations.

Internet connectivity may be unavailable, disabled, or restricted, causing cloud-based notifications to fail. Similarly, unauthorized SIM replacement is a common tactic used after theft, yet many systems do not monitor SIM changes or notify trusted contacts about the new network details. False alarms are also a practical concern. The legitimate owner may occasionally enter an incorrect PIN, which can trigger unnecessary alerts in conventional systems. Without intelligent verification, repeated false notifications reduce user confidence and system usefulness.

International Journal of Advanced Research in Computer Science & Technology (IJARCST)

| ISSN: 2347-8446 | www.ijarcst.org | editor@ijarcst.org |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 9, Issue 3, May-June 2026||

DOI:10.15662/IJARCST.2026.0903005

Hence, there is a need for a smart mobile security system that can identify suspicious failed unlock attempts, capture evidence of the person attempting access, share location details, deliver alerts through multiple communication channels, detect SIM replacement, and intelligently distinguish the legitimate owner from an intruder. Such a system should improve theft response time, reduce false alerts, and strengthen overall smartphone security.

IV. RESEARCH METHODOLOGY

The proposed DarkShield system follows a modular Android-based security architecture designed to detect unauthorized access attempts, collect evidence, verify user identity, and notify trusted contacts in real time. The methodology combines mobile sensing, cloud integration, communication services, and machine learning techniques to provide a complete anti-theft solution.

A. SYSTEM ARCHITECTURE

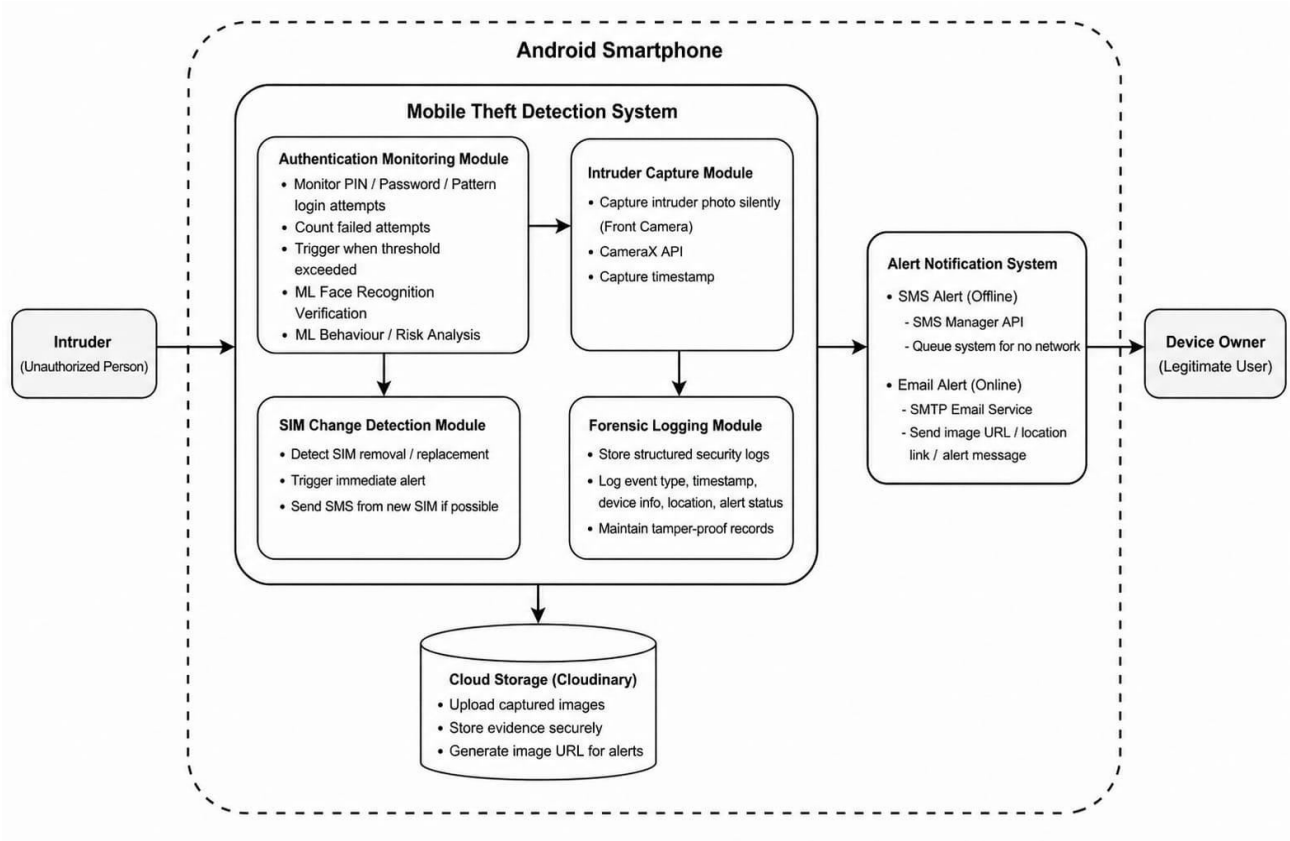

Fig.1. Architecture of the DarkShield Smartphone Intrusion Detection Framework

The proposed DarkShield system adopts modular Android-based architecture for real-time detection of unauthorized access attempts, evidence collection, alert generation, and secure event management. The system operates automatically with minimal user intervention and consists of five functional modules: Authentication Monitoring Module, Evidence Collection Module, Alert Notification Module, SIM Change Detection Module, and Forensic Logging Module.

The workflow begins with the Authentication Monitoring Module, which continuously monitors device unlock attempts such as PIN, password, or pattern inputs. When repeated incorrect attempts exceed the predefined threshold, the intrusion response process is triggered. The Evidence Collection Module captures the current user image using the front camera and retrieves the real-time device location through Android location services. The captured image is securely uploaded to Cloudinary, where a unique evidence URL is generated.

International Journal of Advanced Research in Computer Science & Technology (IJARCST)

| ISSN: 2347-8446 | www.ijarcst.org | editor@ijarcst.org |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 9, Issue 3, May-June 2026||

DOI:10.15662/IJARCST.2026.0903005

The evidence is forwarded to the Alert Notification Module, which sends notifications through SMS and email. SMS works offline, while email is sent when internet is available. Simultaneously, the SIM Change Detection Module compares the current SIM with the registered details. If a mismatch is detected, an immediate alert is generated.

Thus, DarkShield provides an integrated workflow of authentication monitoring, evidence capture, alert communication, SIM monitoring, and secure logging for smartphone anti-theft protection.

AUTHENTICATION MONITORING MODULE

This module continuously monitors device unlock attempts such as PIN, password, or pattern entries. Failed attempts are counted and compared with a predefined threshold. When the limit is exceeded, suspicious activity is detected and the intrusion detection workflow is triggered. To reduce false alerts, the captured face is compared with the registered authorized user.

Trigger condition:

$$Trigger = \begin{cases} Yes, & W \geq 2 \\ No, & W < 2 \end{cases}$$

Where **W** represents the number of wrong unlock attempts.

Face verification decision:

$$Access = \begin{cases} Authorized, & M \geq T \\ Intruder, & M < T \end{cases}$$

Where **M** is the face similarity score and **T** is the matching threshold.

The module achieved an accuracy of 98%, with an average trigger response time of less than 1 second. The threshold used for intrusion detection was 2 wrong attempts.

EVIDENCE COLLECTION MODULE

Once suspicious activity is detected, this module gathers real-time evidence from the device. It silently activates the front camera to capture the current user image and retrieves the real-time geographical location using Android location services.

The captured image is then uploaded securely to Cloudinary, where a unique evidence URL is generated for remote access and alert sharing.

Capture success rate:

$$Capture\ Rate = \frac{Successful\ Captures}{Triggered\ Events} \times 100$$

Location retrieval formula:

$$Location = (Latitude, Longitude)$$

International Journal of Advanced Research in Computer Science & Technology (IJARCST)

| ISSN: 2347-8446 | www.ijarcst.org | editor@ijarcst.org |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 9, Issue 3, May-June 2026||

DOI:10.15662/IJARCST.2026.0903005

Where **Latitude** and **Longitude** represent the current GPS coordinates of the device. The module achieved an accuracy of 95%. The average image capture time was 1–2 seconds, while the cloud upload time was 6.22 seconds.The generated outputs include the captured image, GPS location, cloud evidence URL, and forensic log.

ALERT NOTIFICATION MODULE

This module sends notifications to trusted contacts through SMS and email whenever an intrusion is detected. SMS alerts operate in offline conditions through the cellular network and include location details with the evidence link.
Email alerts are sent when internet connectivity is available and contain detailed intrusion information with the captured image.

Alert delivery rate:

$$Delivery\ Rate = \frac{Delivered\ Alerts}{Sent\ Alerts} \times 100$$

Response time formula:

$$T_{alert} = T_{received} - T_{triggered}$$

The module achieved an accuracy of 97%. The average SMS delivery time was 0.12 seconds, while the email delivery time was 12.26 seconds. The generated outputs include SMS alerts, email notifications, and the evidence link.

SIM CHANGE DETECTION MODULE

This module monitors the currently inserted SIM card and compares it with the registered SIM information stored during setup. If the registered SIM is inserted, no alert is generated. If a new or unauthorized SIM is detected, the system immediately sends an alert containing the current carrier or network details. It helps users quickly identify unauthorized SIM replacement attempts after theft. The module operates automatically in the background without requiring user intervention.

Detection rule:

$$Status = \begin{cases} No\ Alert, & SIM_{current} = SIM_{registered} \\ Alert, & SIM_{current} \neq SIM_{registered} \end{cases}$$

The module achieved an accuracy of 99%. The response time was instant and event based. The generated output includes a SIM change alert with carrier or network details.

.FORENSIC LOGGING MODULE

This module stores all security-related events in the Android **Room Database** for future reference and investigation. Logged records include failed unlock attempts, timestamps, GPS coordinates, SIM change events, alert status, and evidence image URLs. The stored data enables efficient retrieval of past incidents and supports forensic analysis.

Logging formula:

$$Records_{new} = Records_{old} + 1$$

Where **Records_old** is the existing number of stored logs and **Records_new** is the updated count after a new event is recorded. The module achieved 100% successful local log storage during testing. The average logging time was less than 500 milliseconds. The storage method used was Room Database.

International Journal of Advanced Research in Computer Science & Technology (IJARCST)

| ISSN: 2347-8446 | www.ijarcst.org | editor@ijarcst.org |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 9, Issue 3, May-June 2026||

DOI:10.15662/IJARCST.2026.0903005

V. RESULTS

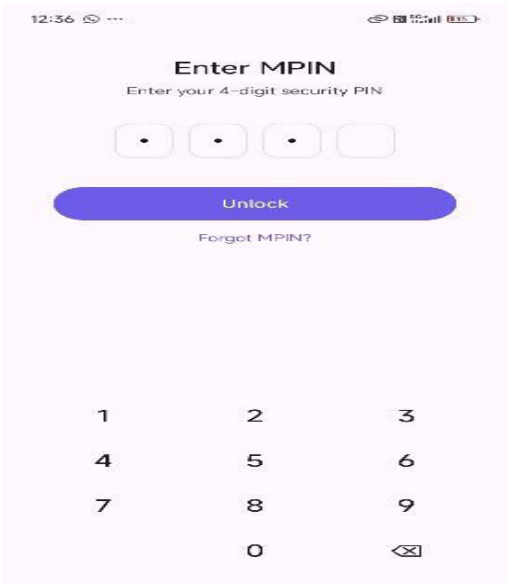

Fig.2. Enter MPIN Authentication Screen

Users enter a 4-digit MPIN to access DarkShield.
Wrong attempts trigger intrusion monitoring.

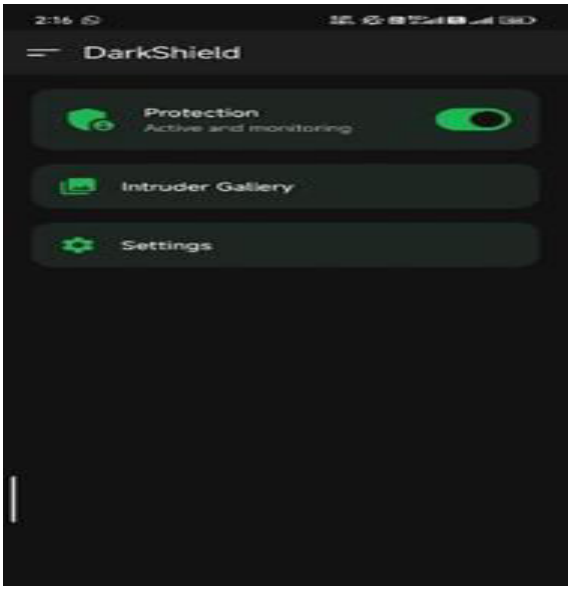

Fig.3. DarkShield Home Dashboard

The DarkShield dashboard provides protection monitoring, intruder gallery access, and settings control with a real-time security toggle.

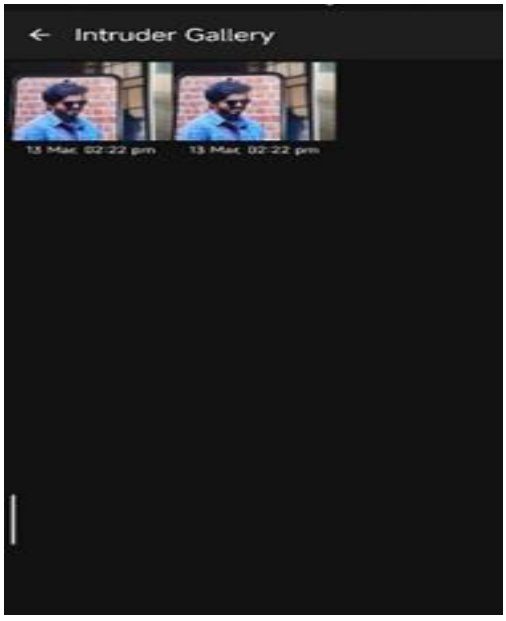

Fig. 4. Intruder Gallery

The Intruder Gallery stores captured intruder images with timestamps for review and evidence tracking.

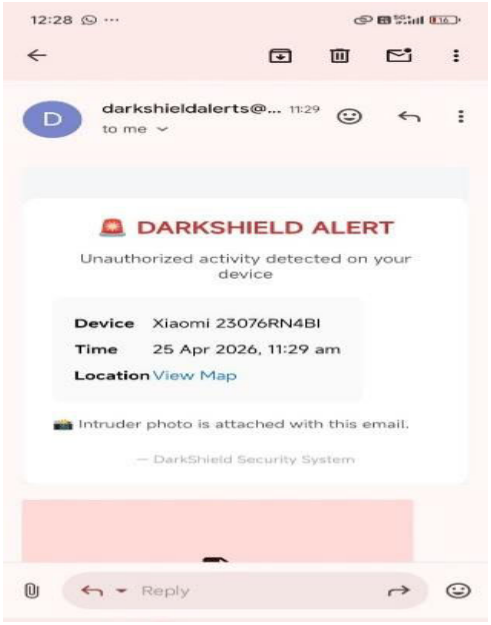

Fig.5. Email Alert Notification

An email alert is sent to the user with device details, time, location link, and intruder image.

International Journal of Advanced Research in Computer Science & Technology (IJARCST)

| ISSN: 2347-8446 | www.ijarcst.org | editor@ijarcst.org |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 9, Issue 3, May-June 2026||

DOI:10.15662/IJARCST.2026.0903005

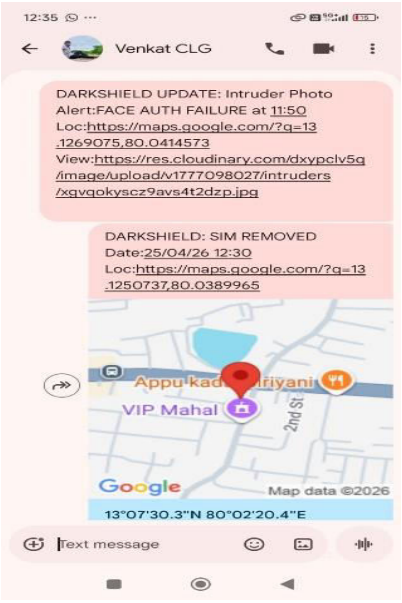

Fig.6. SMS Alert Notification

The SMS Notification sends instant alerts of unauthorized access attempts with device details, time, and location for quick user response.

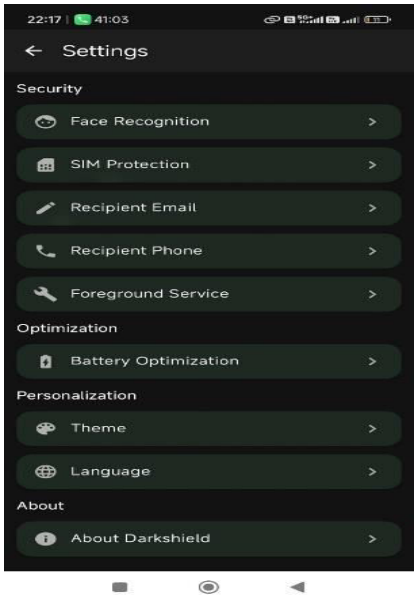

Fig.7. Settings Module

The SMS Notification sends instant alerts with device details, time, and location.

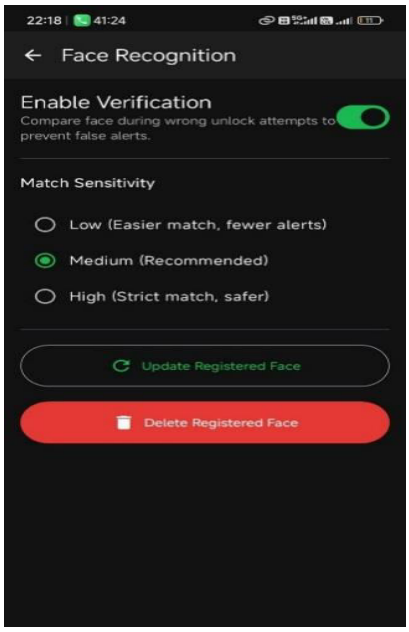

Fig.8. Face Recognition Settings

This module allows users to enable face verification, adjust match sensitivity, update the registered face, an manage authentication preferences.

Fig.9. SIM Protection Module

The SIM Protection module shows trusted SIM details, fetches current SIM info, and lets users register authorized SIMs for change detection.

International Journal of Advanced Research in Computer Science & Technology (IJARCST)

| ISSN: 2347-8446 | www.ijarcst.org | editor@ijarcst.org |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 9, Issue 3, May-June 2026||

DOI:10.15662/IJARCST.2026.0903005

GRAPH ANALYSIS

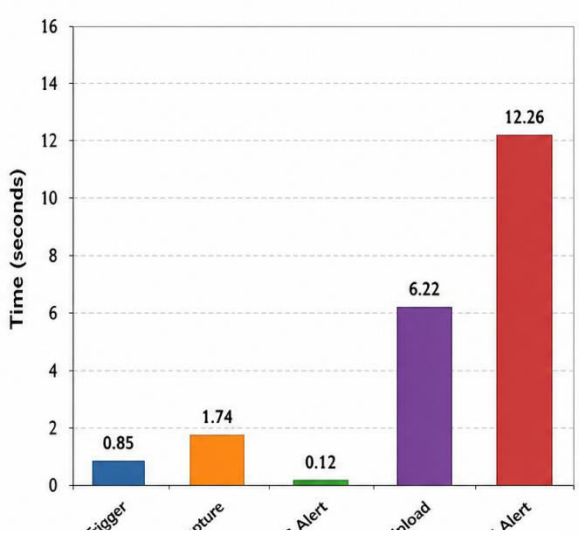

Fig.10. Response Time Performance Analysis

The graph compares DarkShield operation times, showing fast intrusion detection and SMS alerts, with higher delay for cloud upload and email notifications.

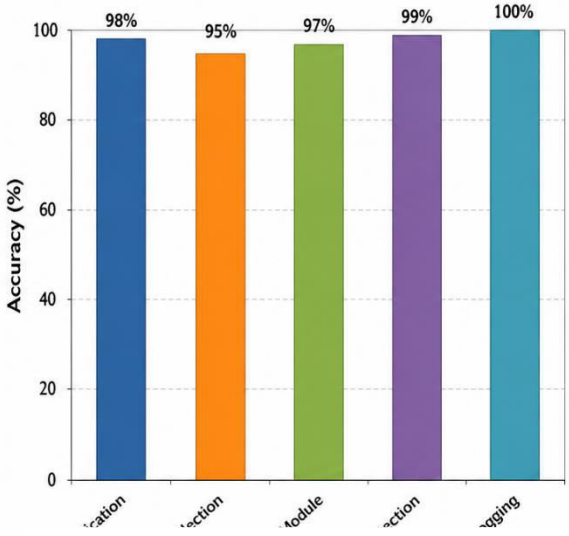

Fig.11. Module Accuracy Performance Analysis

The graph shows DarkShield module accuracy, highlighting high reliability in authentication, evidence collection, alerts, SIM detection, and forensic logging.

VI. CONCLUSION AND FUTURE ENHANCEMENTS

The proposed DarkShield system successfully demonstrates an effective solution for smartphone theft detection and unauthorized access prevention. By integrating custom authentication, wrong PIN detection, intruder image capture, GPS location tracking, cloud evidence storage, SMS and email alerts, SIM change detection, face verification, and forensic logging, the system provides multi-layered mobile security. Experimental results confirmed reliable performance, fast response time, and high accuracy across all major modules. The developed system offers practical real-time protection and enables users to respond quickly during theft or intrusion incidents.

Future versions of DarkShield can include improved machine learning models for more accurate face recognition under different lighting conditions and face angles. Live location tracking can be added for continuous device movement monitoring. A secure user account login system can enable cloud synchronization and remote access to alerts and evidence. Fake shutdown or crash screen mechanisms can be introduced to mislead intruders while background monitoring continues silently. Additional enhancements such as remote lock, remote wipe, smartwatch alerts, web dashboard monitoring, multilingual support, and battery optimization can further strengthen the overall system.

REFERENCES

1. Mrs. E. Shalini and Dr. V. Shanthi, “A Novel Location-Based Anti-Theft Image Capture Application with Culprit Identification for Smartphones,” Testing, Psychometrics, Methodology in Applied Psychology, ISSN: 1972-6325, Volume 32, Special Issue S5, May 2025.
2. Godavarthy Sri Padma Praneeth, Chadarasi Bhavana Sai, Chakka Sravya, and Chinthalapudi Bala Padmaja Praveena, “Intruder Detection and Email Alerting System,” International Journal of Progressive Research in Engineering Management and Science, ISSN: 2583-1062, Volume 04, Issue 05, May 2024.
3. Mrs. Priyanka Gupta, Sahebrao Waghmare, Sham Gavane, and Aditya Dhurv, “Anti-Theft Device Tracking System,” International Journal for Multidisciplinary Research, E-ISSN: 2582-2160, Volume 6, Issue 2, March–April 2024.

| ISSN: 2347-8446 | www.ijarcst.org | editor@ijarcst.org |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 9, Issue 3, May-June 2026||

DOI:10.15662/IJARCST.2026.0903005

4. Mattipelli Sandeep Kumar, Mohammad Iliyas, Pottimuttu Saiteja, Mohammad Aslam, and K. Sathiyapriya, "A Forensics Activity Logger to Extract User Activity from Devices," International Journal of Innovative Research in Science, Engineering and Technology, ISSN (O): 2319-8753, ISSN (P): 2347-6710, Volume 14, Issue 4, April 2025.
5. P. Preethi et al., "Theft Alert Call and SMS," International Journal of Current Science, ISSN: 2250-1770, Volume 15, Issue 3, July 2025.
6. F. M. David, E. M. Chan, J. C. Carlyle, and R. H. Campbell, "Android Security: A Survey of Issues and Solutions," IEEE Communications Surveys & Tutorials, vol. 15, no. 4, pp. 1–23, 2013.
7. W. Enck, P. Gilbert, B. Chun, L. Cox, J. Jung, P. McDaniel, and A. Sheth, "TaintDroid: An Information-Flow Tracking System for Real-Time Privacy Monitoring on Smartphones," in Proceedings of the USENIX OSDI, 2010.
8. Shabtai, U. Kanonov, Y. Elovici, C. Glezer, and Y. Weiss, "Andromaly: A Behavioral Malware Detection Framework for Android Devices," Journal of Intelligent Information Systems, vol. 38, no. 1, pp. 161–190, 2012.
9. Y. Zhou and X. Jiang, "Dissecting Android Malware: Characterization and Evolution," in Proceedings of the IEEE Symposium on Security and Privacy, pp. 95–109, 2012.
10. N. Peiravian and X. Zhu, "Machine Learning for Android Malware Detection Using Permission and API Calls," in Proceedings of the IEEE International Conference on Tools with Artificial Intelligence (ICTAI), pp. 300–305, 2013.
11. Howard, M. Sandler, G. Chu, et al., "Searching for MobileNetV3," in Proceedings of the IEEE International Conference on Computer Vision (ICCV), pp. 1314–1324, 2019.
12. F. Schroff, D. Kalenichenko, and J. Philbin, "FaceNet: A Unified Embedding for Face Recognition and Clustering," in Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR), pp. 815–823, 2015.
13. S. Nath, B. Priyantha, D. Kotz, and C. Cornelius, "Smartphone-Based Intrusion Detection Systems Using Sensor Data," IEEE Sensors Journal, vol. 14, no. 6, pp. 123–130, 2014.
14. Android Developers, "Fused Location Provider API Guide," Google LLC, 2024.
15. Android Developers, "SmsManager API Reference," Google LLC, 2024.
16. Seedha Devi, V., Mahalakshimi, P. V., & Anitha, A. (2026). Automated skin disease analysis and detection using AI-powered mobile application. International Journal of Research and Applied Innovations (IJRAI), 9(3), 531–539. https://doi.org/10.15662/IJRAI.2026.0903004
17. Pandi Prabha, S., & Rengarajan, A. (2025, February). Decentralized Resource Allocation Model Using Multi-agent Reinforcement Learning for Cloud Environment. In International Conference on Universal Threats in Expert Applications and Solutions (pp. 71-82). Singapore: Springer Nature Singapore.
18. Alangaram, S., Udaykiran, M., Rajkumar, K., & Yogeeswaran, T. (2026). Enhancing customer churn prediction and retention for e-commerce. International Journal of Advanced Research in Computer Science & Technology (IJARCST), 9(3), 803–813. https://doi.org/10.15662/IJARCST.2026.0903003
19. Saravanan, M., Sivaganesan, S., & Rajamani, V. Performance analysis of Very Sparse Matrix Converter fed Three Phase cage Induction Drive using Conventional Space Vector Modulation.
20. Socrates, S., Shanmugapriya, M., Murugeshwari, B., & Angalaeswari, S. (2024). Efficient Design for Implantable Device Constant Current Induction Doubly Fed Generating Incorporating Grid Connectivity. In Intelligent Solutions for Sustainable Power Grids (pp. 382-392). IGI Global Scientific Publishing.
21. MATHEW, A. (2025). BEYOND THE BURNER: THE SYSTEMIC RISKS OF DISPOSABLE EMAIL ECOSYSTEMS.
22. Santhoshini, G., & Anbazhagan, K. (2014, February). An object based software tool for software measurement. In International Conference on Information Communication and Embedded Systems (ICICES2014) (pp. 1-5). IEEE.
23. Alangaram, S., Kiswar, M., Ajay, B., & Ezhilkumaran, P. (2026). Socialflow AI: Voice to social media scheduler. International Journal of Research and Applied Innovations (IJRAI), 9(3), 540–547. https://doi.org/10.15662/IJRAI.2026.0903005
24. Rajasekar, M., Nahar, G., Jagatheeswaran, S., Chinthamani, S. A. M., Mohammed, S. H., & Al-Hilali, A. (2024, May). The Roadmap to Classify Malware Using ML Algo Through IOT Based SN. In 2024 4th International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE) (pp. 127-130). IEEE.
25. Raghul, K., Rajasolan, P., Rohinth, S., & Tharun, P. (2026). AI knowledge sharing web portal. International Journal of Advanced Research in Computer Science & Technology (IJARCST), 9(3), 814–823. https://doi.org/10.15662/IJARCST.2026.0903004
26. Narayanan, L. K., Loganayagi, S., Hemavathi, R., Jayalakshmi, D., & Vimal, V. R. (2024, March). Machine learning-based predictive maintenance for industrial equipment optimization. In 2024 International Conference on Trends in Quantum Computing and Emerging Business Technologies (pp. 1-5). IEEE.

| ISSN: 2347-8446 | www.ijarcst.org | editor@ijarcst.org |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 9, Issue 3, May-June 2026||

DOI:10.15662/IJARCST.2026.0903005

27. Sangeetha, D., Dharan, K. D., Krishna, A. C., & Karthikeyan, C. (2026). Speech and text conversion system for sign language using ML. International Journal of Computer Technology and Electronics Communication (IJCTEC), 9(3), 1000–1007. https://doi.org/10.15680/IJCTECE.2026.0903003
28. Rajasekar, M. (2024). Real-Time Predictive DevOps Intelligence for Risk-Aware Digital Business Processes in Cloud and SAP Ecosystems. International Journal of Advanced Research in Computer Science & Technology (IJARCST), 7(4), 10713-10718.
29. Anbazhagan, K., SUGUMAR, D., Mahendran, M., & Natarajan, R. (2012). An efficient approach for statistical anonymization techniques for privacy preserving data mining. International Journal of Advanced Research in Computer and Communication Engineering, 1(7), 482-485.
30. Chowdary, P. B. K., Udayakumar, R., Jadhav, C., Mohanraj, B., & Vimal, V. R. (2024). An Efficient Intrusion Detection Solution for Cloud Computing Environments Using Integrated Machine Learning Methodologies. J. Wirel. Mob. Networks Ubiquitous Comput. Dependable Appl., 15(2), 14-26.
31. Seedha Devi, V., Kaavya, S., Deepika, B., Jayashree, D., & Nithikaa, L. (2026). AI-driven voter authentication and fraud detection system. International Journal of Computer Technology and Electronics Communication (IJCTEC), 9(3), 1008–1017. https://doi.org/10.15680/IJCTECE.2026.0903004
32. Mathew, A. (2021). Obfuscation Techniques for Magecart Detection and Prevention. International Journal of Computer Science and Mobile Computing, 10(2), 39-44.
33. Alangaram, S., Yuvaraj, G., Srivatsan, M. J., & Sathish, R. (2026). An IoT-based smart helmet for real-time rider safety monitoring and emergency response system. International Journal of Research in Production Engineering, Technology and Management (IJRPETM), 9(3), 1021–1030. https://doi.org/10.15662/IJRPETM.2026.0903003
34. Kaliappan, S., Ragunthar, T., Ali, M., & Murugeshwari, B. (2024). Implementation of Virtual High Speed Data Transfer in Satellite Communication Systems Using PLC and Cloud Computing. In AI Approaches to Smart and Sustainable Power Systems (pp. 274-286). IGI Global Scientific Publishing.
35. Naresh, D., Anand, P., Harish, M., Vamshi, A., Kethan, A., Nirmala, B., & Saravanan, M. (2026). Face Recognition Door Lock System with IoT &AI. International Journal of Computer Technology and Electronics Communication, 9(2), 526-534.
36. Prabha, S. P., & Rengarajan, A. (2025). ENHANCING CLOUD RESOURCE ALLOCATION WITH VISION TRANSFORMER, DEEP REINFORCEMENT LEARNING, AND IMPROVED SHRIKE OPTIMIZATION ALGORITHM. Corrosion Management ISSN: 1355-5243, 35(2), 233-245.
37. Raghul, K., Thamaraikannan, R., Sunil Kumar, S., & Siva, B. (2026). Plastitrack: A community-driven plastic waste collection and redemption platform. International Journal of Research and Applied Innovations (IJRAI), 9(3), 548–557. https://doi.org/10.15662/IJRAI.2026.0903006