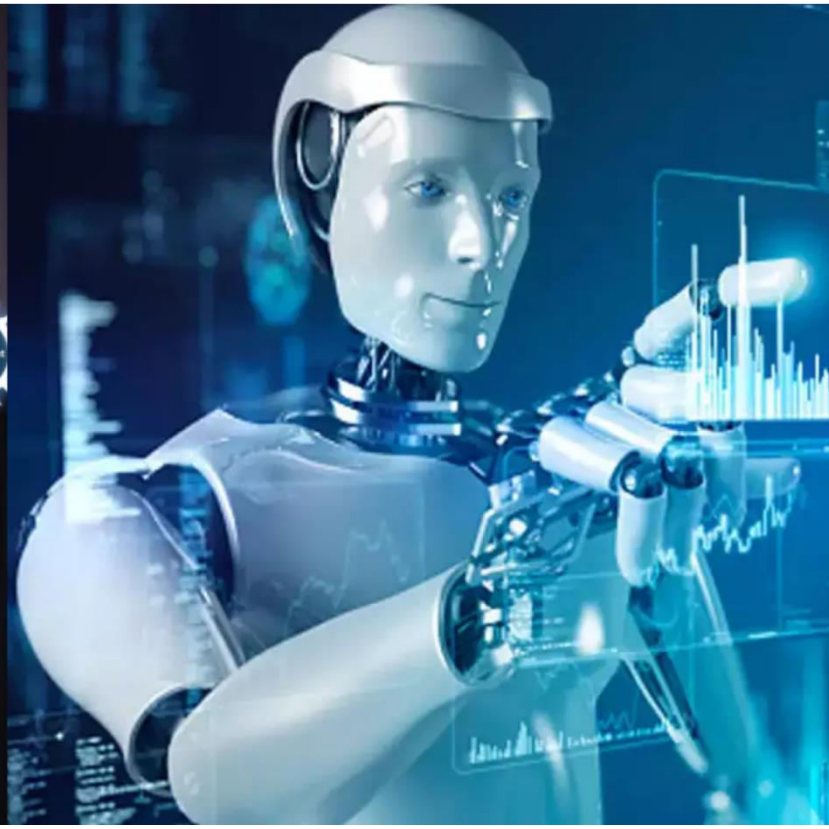
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

# International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

*(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)*

**Impact Factor: 8.699**

**Volume 14, Issue 11, November 2025**

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 11, November 2025

|DOI: 10.15680/IJIRSET.2025.1411135|

# CAM Defender: Android Intrusion Shield for Enhanced Camera Privacy Protection

**Karthik B Chavhan, Noor Fathima Mulla, Rehmate Afsha, Simran, Bhavana S. Patil**

Department of Computer Science and Engineering, STJ Institute of Technology, Ranebennur, Karnataka, India

***ABSTRACT:*** Smartphone cameras are powerful sensors that, when exploited by malicious applications, can severely violate user privacy. This paper presents CAM Defender, an Androidbased intrusion detection and prevention system focused on protecting camera resources. CAM Defender performs permission analysis, runtime monitoring of camera access, real-time user alerting, and selective blocking where platform APIs permit. The system is implemented as a lightweight foreground-compatible service to minimize termination by the OS. Experimental evaluation on multiple Android devices demonstrates that CAM Defender detects unauthorized camera usage with high accuracy while incurring low performance and energy overhead.

***KEYWORDS****:* Android security, camera intrusion, privacy protection, intrusion detection, mobile security.

## I. INTRODUCTION

Mobile devices contain a range of sensors that, in malicious hands, become tools for privacy invasion. The camera is especially sensitive because it can record visual information without a user's awareness. While Android's permission model and marketplace scanning (e.g., Google Play Protect) mitigate some risks, they do not provide runtime awareness or direct protection when a malicious app activates the camera stealthily. CAM Defender addresses this gap by continuously monitoring camera access, alerting users at the time of use, and taking configurable mitigation actions. This work's contributions are:

- Design and implementation of a deployable, user-space Android service that monitors camera usage in real time.
- A lightweight detection algorithm that balances responsiveness with energy efficiency.
- An evaluation across devices and app scenarios demonstrating high detection accuracy and low overhead.

## II. RELATED WORK

Research on mobile privacy covers permission systems, static and dynamic malware analysis, and sensor-specific defenses. Permission managers provide control at install time but offer limited runtime awareness. Kernel-level or system-hook approaches enable deeper monitoring but typically require elevated privileges or custom ROMs, reducing deployability. CAM Defender focuses on a practical, non-root solution using publicly available Android APIs and careful service design to remain active and effective.

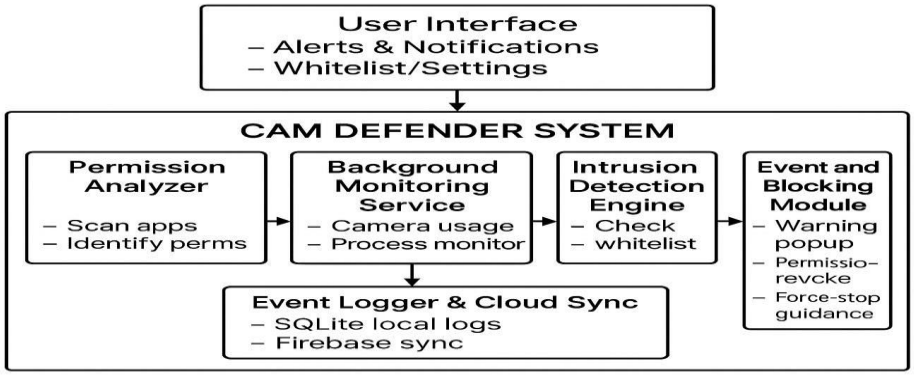



Fig. 1: CAM Defender high-level architecture (placeholder image).

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 11, November 2025

|DOI: 10.15680/IJIRSET.2025.1411135|

## III. SYSTEM ARCHITECTURE

Figure 1 shows CAM Defender's high-level architecture. The core modules are:
1) Permission Analyzer: Scans installed applications for camera-related permissions and builds an initial risk profile.
2) Background Monitor Service: Observes camera usage events and running processes in real time.
3) User Alert System: Notifies the user with a highpriority dialog and logging details when suspicious access is detected.
4) Blocking Mechanism: Attempts to restrict or pause the offending app using available APIs (e.g., revoking permissions where supported, bringing the app to the foreground to interrupt covert capture, or prompting the user to force-stop).
5) Activity Logger: Records events (timestamp, package, action) locally and optionally syncs anonymized logs to Firebase for further analysis.

## IV. DETECTION ALGORITHM

The detection algorithm focuses on identifying camera access events and deciding whether they are authorized. Pseudocode is shown in Algorithm 1.
Algorithm 1 Camera Access Monitoring
1: Initialize monitoring service and whitelist of trusted packages
2: while service active do
3: Read camera usage events from CameraManager or system logs
4: for all event in events do
5: pkg ← event.packageName 6: if pkg not in whitelist then
7: Raise user alert with package details
8: Log event with timestamp and context
9: If possible, attempt mitigation (revoke, pause, prompt)
10: end if
11: end for
12: Sleep for configurable interval (e.g., 500 ms)
13: end while

## V. IMPLEMENTATION DETAILS

CAM Defender was implemented in Android Studio (Java) and tested on devices running Android 10 to Android 13. Key implementation notes:

- The system uses Android's CameraManager and the Camera API where available to check camera device state.
- A foreground service with a persistent notification is used to reduce the chance of OS termination.
- Local logging uses SQLite; optional upload to Firebase requires user opt-in.
- The UI provides whitelist management, event history, and controls for mitigation preferences.

## VI. EXPERIMENTAL EVALUATION

We evaluated CAM Defender under mixed workloads: benign camera apps, background camera usage, and custom test apps simulating covert capture.

*A. Setup*

Devices: three Android smartphones (brands and models anonymized) running Android 10, 11, and 13 respectively. Test apps included common camera apps and a set of custom apps that attempted to access the camera without showing UI.

*B. Metrics*

We measured detection accuracy (true positives / total positives), false positives, response time (time between camera activation and user alert), and energy overhead (battery percentage per hour during monitoring).

*C. Results*

Table I summarizes the evaluation.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 11, November 2025

|DOI: 10.15680/IJIRSET.2025.1411135|

TABLE I: Experimental Results

| Metric | Value | Notes |
|---|---|---|
| Detection Accuracy | 96% | True positive rate over test set |
| False Positive Rate | 3% | Benign apps incorrectly alerted |
| Response Time | <1 s | Median time from activation to alert |
| Energy Overhead | 2.1%/hr | Measured during continuous monitoring |
| User Satisfaction | 9/10 | Small user study (N=15) |

## VII. DISCUSSION

The user-space approach is attractive for deployability but has limitations: Android's security model prevents fully forcing another app to stop without user consent or elevated privileges. Therefore, CAM Defender emphasizes user-notification and guided mitigation rather than silent termination. Future work will explore tighter integrations with OEMs or an enterprise MDM approach to enforce stricter controls.

## VIII. FUTURE WORK

Planned improvements include expanding monitoring to microphone and other sensors, integrating lightweight behavioral models to reduce false positives, and providing optional enterprise features for centralized policy management.

## IX. CONCLUSION

CAM Defender provides a practical, low-overhead system to protect Android users from unauthorized camera access. By combining permission analysis, runtime monitoring, and clear user interaction, CAM Defender increases visibility and control over camera usage.

## X. ACKNOWLEDGMENT

The authors thank the STJ Institute of Technology faculty and the student testers for their support.

## REFERENCES

[1] Google Android Developers, "Camera API Documentation," 2024.
[2] L. Chen et al., "Privacy Protection in Android Devices," *IEEE Access*, 2023.
[3] R. Singh, "Real-Time Intrusion Detection Systems on Mobile Devices," *Springer Security Journal*, 2022.
[4] H. Wang, "Analysis of Mobile Privacy Threats and Defenses," *Computers & Security*, 2021.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

## IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details