2025 International Conference on Advancements in Smart, Secure and Intelligent Computing (ASSIC) | 979-8-3315-2302-2/25/$31.00 ©2025 IEEE | DOI: 10.1109/ASSIC64892.2025.11158601

CenterYou++: Lightweight Privacy Enforcement for Android Using Hybrid AI and Cloud Decision Support

Seyedmostafa Safavi
School of Technology
APU Malaysia
Kuala Lumpur, Malaysia
safavi@takhosting.info

Zarina Shukur
Faculty of Information Science & Technology
Universiti Kebangsaan Malaysia
Selangor, Malaysia
zs@ftsm.ukm.my

Muhammad Ehsan Rana
School of Computing
APU Malaysia
Kuala Lumpur, Malaysia
muhd_ehsanrana@apu.edu.my

***Abstract*—While the Android operating system provides a vast application ecosystem offering extensive functionalities, it concurrently introduces substantial challenges to preserving user privacy. Mobile applications frequently engage in widespread collection of personal data, and users often encounter difficulties in managing application permissions effectively, creating exposure to potential privacy infringements. Existing techniques for privacy enforcement frequently encounter difficulties in achieving an optimal balance among scalability, user-centric design principles, and the critical need for timely responsiveness. To overcome these limitations, this work introduces CenterYou++, a novel privacy enforcement framework engineered specifically for Android environments. This framework employs a hybrid architecture, distinctively merging the capabilities of lightweight, on-device artificial intelligence (AI) agents with the resources of cloud-based decision support. The on-device AI facilitates low-latency, localized privacy enforcement actions grounded in learned behavioral patterns and predefined rules. Concurrently, the cloud component furnishes access to current privacy policies and global threat intelligence, while also underpinning the system's scalability. This synergistic design yields considerable advantages, encompassing real-time privacy enforcement capabilities, a more intuitive user experience achieved through automation and transparency, and strengthened policy enforcement mechanisms. The overarching objective is to establish an equilibrium between robust privacy protection and a fluid, unobtrusive user experience.**

***Index Terms*—Android Privacy, Lightweight AI, Hybrid Architecture, Real-Time Privacy Enforcement, Cloud Computing, Edge AI, Mobile Security, Permission Management, Federated Learning.**

I. Introduction

The inherent openness and receptiveness of the Android platform, when considered alongside the extensive and diverse assortment of applications that are readily available for users, creates a significant array of privacy-related challenges and threats that are faced by individuals utilizing this technology. Applications that function within this particular ecosystem frequently make requests for access to a broad spectrum of sensitive personal data belonging to users, which may include, but are not limited to, information such as geographical location tracking, access to contact lists, and the utilization of camera functionalities. It is not uncommon for these requests for permissions to extend well beyond the limits or parameters that are strictly necessary for the basic operational requirements of the application in question [1].

This particular issue is further exacerbated by the fact that users typically confront substantial challenges when it comes to fully comprehending the ramifications or implications associated with granting such permissions, a misunderstanding that can unintentionally lead to severe data breaches or unauthorized access to sensitive information. Moreover, security vulnerabilities that may arise either within the Android operating system itself or within the applications that have been installed can be manipulated by malicious actors, thereby compromising user privacy without the explicit awareness or consent of the users involved. This intricate and multifaceted landscape highlights a fundamental conflict that exists within the Android ecosystem: a persistent and ongoing dichotomy between the wide-ranging functionality and capabilities that applications provide and the critical need to protect user data from potential exploitation and misuse [2].

In light of the recognized deficiencies and inadequacies present in contemporary privacy protection solutions, there exists a distinct and pressing need for innovative frameworks that not only offer effective safeguards for the privacy of user data but are also sufficiently lightweight in nature to operate efficiently on mobile devices that are typically characterized by limited processing and resource capabilities. In addition to this, it is imperative that such frameworks possess the necessary scalability to effectively accommodate the vast and diverse demographic of Android users across the globe. A multitude of existing privacy frameworks, however, fall short of achieving this precarious balance. Some frameworks may prove to be excessively demanding in terms of system resource consumption, while others may introduce undue complexity that poses challenges for the average user, and still others may lack the requisite real-time responsiveness needed to effectively counter immediate and emerging privacy threats [3].

As a result of these identified challenges, the primary

*Corresponding author: safavi@takhosting.info motivation and driving force behind the development of CenterYou++ is the formulation of a privacy solution that is not only robust in its protective capabilities but also pragmatic and feasible for widespread application across various user demographics. This endeavor necessitates the engineering of a sophisticated system that is capable of delivering substantial assurances regarding privacy without adversely affecting the usability or overall performance of the devices on which it operates. CenterYou++ seeks to introduce an innovative approach by integrating on-device artificial intelligence with cloud-based policy support in order to achieve this ambitious objective. This hybrid methodology effectively leverages the rapid processing capabilities inherent to on-device artificial intelligence to facilitate immediate and proactive privacy enforcement directly at the device level. Simultaneously, the cloud-based component provides users with access to a comprehensive and dynamically updated repository of privacy policies and threat intelligence, while also ensuring that the system is equipped with the capacity to scale effectively as user demands evolve and grow [1], [4].

The synergy that is achieved through the combination of device-level computation and cloud resources culminates in the establishment of a privacy management system that is both adaptive and holistic in nature, effectively addressing the inherent limitations that are often associated with solutions that rely solely on local processing or exclusively on cloud infrastructure. The principal contributions of this research endeavor are meticulously delineated as follows:

1) **A hybrid AI model for privacy enforcement:** CenterYou++ utilizes lightweight AI models, potentially including rule-based classifiers or embedded machine learning algorithms, operating directly on the Android device [5]. These models are optimized for efficiency and are designed to identify potentially hazardous permission requests and anomalous application behavior in real-time. Although specific training methodologies warrant further exploration, the current design anticipates initial model training using aggregated, anonymized datasets. There is potential for future integration of federated learning techniques to enhance privacy during subsequent model updates. The core focus lies in developing AI models capable of efficiently predicting potential privacy risks based on observed application activities and requested permissions, thereby enabling proactive user protection.
2) **A lightweight architecture for Android:** The architectural framework of CenterYou++ emphasizes minimal resource utilization on the host Android apparatus. Fundamental elements comprise an on-device artificial intelligence agent designated for local enforcement, a cloud-based decision-making engine accountable for policy administration and intricate analysis, a secure communication interface guaranteeing safeguarded data transmission, and a user interface facilitating engagement with privacy configurations. The operational procedure fundamentally involves a systematic approach whereby solicitation requests for application permissions are intercepted and subsequently processed through an advanced on-device artificial intelligence system, which is adept at handling such requests efficiently. Moreover, when the situation necessitates a more nuanced decision-making process or when policy modifications are required, this on-device intelligence then consults the cloud infrastructure to ensure that the most current and relevant guidelines are applied. This deliberate and calculated division of responsibilities is designed to ensure that operations requiring significant computational resources are effectively relegated to the cloud, while simultaneously allowing the on-device agent to provide immediate, low-latency protective measures that safeguard user privacy in real time.
3) **Comparative analysis with prior systems like CenterYou:** In a significant advancement over its predecessor, CenterYou++, represents a notable evolution that is fundamentally built upon the core principles that were originally established by the earlier CenterYou framework, as documented in previous scholarly works [1], [2]. Unlike the initial iteration of the CenterYou system, which was heavily reliant on a purely cloud-based decision-making framework and employed pseudo-data methodologies to regulate privacy settings on Android devices, CenterYou++ significantly enhances this existing model by seamlessly integrating on-device artificial intelligence functionalities. This innovative hybrid architecture directly confronts and addresses the limitations that are inherent to a system that depends solely on cloud computing, such as the potential issues related to communication latency and the dependence on uninterrupted network connectivity for effective operation. By incorporating edge intelligence into its design, CenterYou++ aims to deliver a privacy enforcement mechanism that is not only more immediate and contextually aware but also significantly more robust in its capabilities compared to its predecessor, thereby providing users with enhanced control over their privacy [1], [6]. This iterative enhancement not only rectifies the vulnerabilities that were acknowledged in the previous generation but also highlights a deliberate and purposeful progression toward the development of more effective mobile privacy solutions that are better suited to meet the evolving needs of users in an increasingly digital and interconnected world.

II. Related Work

In their 2020 publication, ”Android Privacy Made Easier the Cloud Way,” Safavi and Shukur introduced the CenterYou framework, conceptualized as a cloud-based system aimed at simplifying Android privacy management for end-users [1]. The primary objective of CenterYou was to shield users from permissions requested unnecessarily by installed applications, achieved through reliance on a cloud-hosted decision-making system coupled with a pseudo-data technique. However, any approach predicated solely on cloud infrastructure inherently confronts operational constraints. Such systems necessitate uninterrupted network connectivity to maintain full functionality. Moreover, the latency introduced by transmitting all application behavior data to the cloud for analysis and subsequently receiving directives can obstruct effective real-time privacy enforcement [7]. An additional concern involves the privacy implications of transmitting potentially sensitive application behavior metrics to a centralized server. The hybrid design of CenterYou++ directly mitigates these specific drawbacks. By performing initial privacy assessments and enforcement actions locally on the device using lightweight AI, it diminishes the reliance on continuous cloud communication and significantly improves system responsiveness, addressing the core limitations identified in the cloud-only predecessor.

A subsequent paper by Safavi, Safavi, and Shukur in 2023, titled ”Investigating the Role of Blockchain in Enhancing Home Security,” delves into the application of decentralized security principles, specifically leveraging blockchain technology, to bolster security and privacy within distributed systems, examined through the lens of home security scenarios [8]. The principles of decentralization, data immutability, and operational transparency afforded by blockchain technology hold considerable relevance for mobile privacy challenges, particularly concerning the management of privacy policies and user consent mechanisms. Although the currently proposed architecture for CenterYou++ does not incorporate blockchain elements directly, the concepts articulated in this related work establish a valuable foundation for investigating future enhancements. Specifically, blockchain presents a potential mechanism for managing and disseminating privacy policy updates across the CenterYou++ ecosystem in a secure, transparent, and tamper-evident manner, thereby potentially increasing the integrity and trustworthiness of the policies enforced by the system. This demonstrates an awareness of adjacent technologies that could further strengthen the framework's security posture in future iterations.

The preceding 2020 scholarly endeavor by Safavi and Shukur, ”CenterYou: A cloud-based Approach to Simplify Android Privacy Management,” furnishes a more meticulous elucidation of the architecture and functionalities intrinsic to the original CenterYou framework [2]. This research accentuates CenterYou's reliance on a cloud-based decision engine for orchestrating application permission governance and emphasizes its employment of pseudo-data methodologies designed to safeguard sensitive user information. CenterYou++ signifies a notable advancement from this foundational model. It amplifies the cloud-exclusive architecture into a hybrid lightweight framework through the essential incorporation of on-device artificial intelligence. This architectural augmentation enables more prompt and context-sensitive privacy enforcement directly on the user's device, effectively surmounting the inherent latency and offline operational constraints characteristic of the original cloud-centric design. The transition towards a hybrid model signifies a clear advancement towards developing a more proactive and dynamically responsive privacy management system for Android users. The explicit comparison and contrast with the previous generation system clearly articulates the evolutionary step taken and the rationale underpinning the novel hybrid approach.

III. Proposed Methodology (CenterYou++ Framework)

The CenterYou++ framework employs a layered architectural structure to realize its hybrid privacy enforcement capabilities. At the heart of the system resides an on-device lightweight AI agent, designed to operate collaboratively with a cloud-based decision engine. Facilitating the necessary exchange of data and policy information between these two core components is a secure communication interface. Complementing these elements is a user interface that allows end-users to interact with and configure their privacy preferences. Figure 1 provides a conceptual depiction of the layered architecture of the CenterYou++ framework, illustrating the interplay between the on-device AI agent, the cloud-based decision engine, the secure communication pathway, and the user-facing interface. The on-device lightweight artificial intelligence agent assumes the obligation for executing real-time privacy enforcement directly upon the Android apparatus. This agent employs computationally efficient artificial intelligence models, such as rule-based classifiers or embedded machine learning frameworks. The selection criteria for these models prioritize minimal computational overhead and reduced power consumption, rendering them appropriate for resource-constrained mobile environments. Initial training of these models is executed utilizing aggregated and anonymized data sets, enabling them to discern patterns indicative of precarious permission requests or anomalous application activities. Subsequently, these models can be dynamically refreshed with novel privacy regulations and behavioral patterns disseminated from the cloud. The principal functions conferred upon the AI agent encompass: intercepting application permission requests as they transpire, analyzing these requests against assimilated patterns and current privacy policies stored locally, detecting potentially detrimental or excessive permission demands, and providing immediate privacy recommendations or initiating

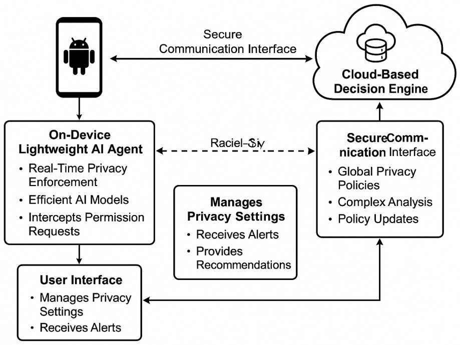

Fig. 1. Conceptual architecture of the CenterYou++ hybrid privacy enforcement framework

enforcement actions, such as denying a permission request or notifying the user. Functioning as the central intelligence repository for the CenterYou++ framework is the cloud-based decision engine. This engine sustains a comprehensive and perpetually updated knowledge base comprising privacy policies, identified application behavior patterns, and global threat intelligence aggregated from diverse sources. Key responsibilities of this engine include synthesizing global privacy policies derived from the analysis of data collected across numerous devices (handled in an anonymized and aggregated fashion) and incorporating information from external security feeds. It is also equipped to manage more complex privacy analyses that necessitate substantial computational power, such as identifying subtle correlations between disparate application behaviors and known privacy vulnerabilities. Crucially, the cloud engine periodically pushes updates, including revised privacy policies and refined AI model parameters, to the on-device AI agents. This mechanism ensures that the local agents possess the most current information required for effective privacy enforcement, highlighting an ongoing, necessary interaction between the cloud and device components for sustained effectiveness.

The allocation of decision-making authority regarding privacy enforcement is dynamically distributed between the on-device AI agent and the cloud-based decision engine, governed by several operational factors. For situations demanding immediate, low-latency responses—for instance, blocking a permission request flagged as high-risk by the on-device AI—the decision is rendered locally. Conversely, more intricate analyses or decisions requiring access to broader contextual information or significant computational resources are offloaded to the cloud infrastructure.

As an example, if the on-device AI encounters application behavior that does not conform to known patterns, it can transmit relevant metadata (anonymized where appropriate) to the cloud for deeper scrutiny and potential policy refinement. Network availability also plays a role in this dynamic distribution. The on-device AI is engineered to provide a foundational level of privacy protection even when the device is offline or experiencing limited network connectivity, relying on its locally cached policies and models. The system architecture inherently prioritizes on-device processing to maximize efficiency and responsiveness, resorting to cloud-based decision support only when essential or when a more thorough, computationally intensive analysis is deemed beneficial. The specifics of this dynamic allocation, such as the precise triggers for cloud consultation, represent an area of implementation detail requiring careful design and tuning. To provide a clear overview of the system's structure, Table I summarizes the key architectural components and their primary functions.

TABLE I
KEY COMPONENTS AND FUNCTIONS OF CENTERYOU++ ARCHITECTURE

Component	**Primary Functions**
On-Device Lightweight AI Agent	Intercepts permission requests; Performs real-time analysis using local models/policies; Detects risky/anomalous behavior; Executes immediate enforcement actions (block/notify); Operates with low latency and minimal resources; Provides baseline offline protection.
Cloud-Based Decision Engine	Maintains central repository of updated policies, threat intelligence, and behavior patterns; Performs complex, resource-intensive analyses; Synthesizes global policies from aggregated data; Pushes policy/model updates to devices.
Secure Communication Interface	Facilitates protected data exchange (metadata, policy updates, decisions) between the on-device agent and the cloud engine.
User Interface	Allows users to view privacy status; Configure privacy settings and preferences; Receive notifications and recommendations.

IV. DISCUSSION

CenterYou++ emerges as a substantial refinement compared to the original CenterYou framework and other privacy solutions constructed purely on cloud infrastructure. While cloud-centric paradigms present certain advantages, notably centralized policy administration and inherent scalability, they are concurrently constrained by intrinsic limitations. The fundamental reliance on network connectivity introduces communication latency, a factor that can significantly impede the efficacy of real-time privacy enforcement actions.

Moreover, the obligation to convey potentially sensitive application behavior data to a centralized cloud server invariably engenders privacy concerns. CenterYou++ adeptly mitigates these particular deficiencies through the strategic incorporation of lightweight artificial intelligence capabilities directly onto the device. This hybrid approach facilitates instantaneous processing and enforcement of privacy policies at the local level, thereby reducing the necessity for continual cloud interaction and significantly enhancing the system's overall reactivity. By prudently amalgamating the unique advantages afforded by both device-level processing and cloud computing resources, CenterYou++ aspires to provide a privacy solution that is demonstrably more resilient and user-oriented.

The benefits conferred by the hybrid architecture of CenterYou++ are multifarious. The existence of the on-device AI facilitates authentic real-time privacy enforcement, permitting immediate responses to potential privacy threats without the inherent latencies associated with cloud round-trips. By processing a considerable volume of data locally, the framework naturally results in diminished bandwidth consumption; minimizing the quantity of information transmitted to and from the cloud can also yield advantages in terms of conserving device battery longevity. The on-device component inherently provides resilience, ensuring that a baseline level of privacy protection is maintained even during periods of network unavailability or intermittent connectivity. Moreover, by performing analyses of sensitive data locally whenever feasible, CenterYou++ enhances user privacy by reducing the volume of personal information that must be externalized to the cloud. Lastly, the distribution of the processing workload across numerous devices and the central cloud infrastructure contributes positively to the overall scalability of the framework. These benefits directly address the identified weaknesses of latency, connectivity dependence, and data transmission concerns associated with earlier cloud-only models.

Notwithstanding these advantages, CenterYou++ is also characterized by certain limitations that warrant acknowledgment. The initial deployment of the framework may necessitate a network connection to download the foundational privacy policies and potentially the on-device AI models themselves. Although devised for lightweight functioning, the on-device artificial intelligence processing will inevitably exert certain energy requirements, which could potentially be more pronounced on antiquated or less potent hardware. The accuracy and overall performance of the on-device artificial intelligence systems are fundamentally reliant upon the quality and representativeness of the datasets utilized during their training processes; this reality inherently introduces the possibility of biases becoming embedded within the model if the training datasets are not meticulously selected, curated, and managed with the utmost care and diligence. Additionally, the multifaceted challenges of supervising a hybrid setup, which demands the provision of smooth and secure exchanges between the on-device parts and their cloud counterparts, contributes further complexity to the overall architecture, deployment, and sustainability of the system being discussed. Such a candid evaluation of these inherent limitations ultimately offers a nuanced perspective on the capabilities of the framework while simultaneously illuminating the challenges that it faces.

V. Conclusion and Future Work

In summary, this academic paper has introduced CenterYou++, a framework that can be defined as an innovative and highly sophisticated hybrid system specifically engineered to enforce stringent privacy protections tailored for the Android operating system, thereby addressing an increasingly urgent concern in the domain of digital privacy that affects users globally. Through the intelligent integration of lightweight artificial intelligence that functions directly on the device in conjunction with robust decision-making support systems located in the cloud, CenterYou++ aims to effectively mitigate the various limitations that are frequently encountered in existing privacy solutions available on the market today. This framework not only delivers a broad array of significant advantages, which encompass the capability for low-latency privacy enforcement that significantly enhances the overall user experience, but also features a user-centric design that prioritizes user convenience, augmented functionalities aimed at the rigorous enforcement of privacy policies, diminished bandwidth requirements that facilitate greater accessibility for a diverse range of users, and a pronounced enhancement in operational resilience that is particularly advantageous in situations where offline functionality is of paramount importance. This framework signifies a distinct evolution from the original CenterYou concept, primarily through the incorporation of edge intelligence, which facilitates more immediate and contextually informed privacy protection directly on the user's device.

The avenues for future research and development related to CenterYou++ are both numerous and promising. One significant potential direction involves the integration of federated learning techniques. Employing federated learning could enable the training and refinement of the on-device AI models in a manner that inherently preserves privacy, allowing the system to learn from real-world usage patterns distributed across many devices without necessitating the centralization of sensitive user data.

This approach would further bolster the privacy assurances provided by the framework. Another compelling area for exploration is the potential application of blockchain technology, particularly for managing dynamic policy updates. Blockchain could offer a decentralized, transparent, and tamper-resistant mechanism for distributing and verifying privacy policy updates to all devices operating within the CenterYou++ ecosystem, enhancing trust and security. Further research could also focus on the development of more sophisticated, yet still computationally efficient, AI techniques suitable for on-device privacy analysis. Enhancing the user interface to deliver more intuitive visualizations and controls related to privacy decisions represents another valuable direction.

Finally, conducting comprehensive evaluations of the framework's performance metrics, security posture, and user acceptance within realistic, real-world deployment scenarios is essential for validating its practical efficacy and identifying areas for further refinement. These future workstreams provide a clear roadmap for continued advancement of the CenterYou++ concept.

References

[1] S. Safavi and Z. Shukur, "Android privacy made easier the cloud way," 09 2020. [Online]. Available: https://doi.org/10.20944/preprints202009.0161.v1

[2] ——, "Centeryou: A cloud-based approach to simplify android privacy management," *Cornell University*, 01 2020. [Online]. Available: https://arxiv.org/abs/2008.13405

[3] M. Chamikara, P. Bertök, D. Liu, S. Camtepe, and I. Khalil, "Efficient data perturbation for privacy preserving and accurate data stream mining," *Elsevier BV*, vol. 48, pp. 1–19, 05 2018. [Online]. Available: https://doi.org/10.1016/j.pmcj.2018.05.003

[4] A. Mabina and A. Mbotho, "A hybrid framework for securing 5g-enabled healthcare systems," vol. 2, p. 15, 01 2025. [Online]. Available: https://doi.org/10.48185/smhs.v2i1.1447

[5] S. Y. Liew, V. A. Hameed, M. E. Rana, and S. Safavi, "Navigating the retail 4.0 landscape: The transformative impact of cloud computing," 12 2023.

[6] K. Kubiak, G. Dec, and D. Stadnicka, "Possible applications of edge computing in the manufacturing industry—systematic literature review," pp. 2445–2445, 03 2022. [Online]. Available: https://doi.org/10.3390/s22072445

[7] L. Zeng, X. Chen, Z. Zhou, L. Yang, and J. Zhang, "Coedge: Cooperative dnn inference with adaptive workload partitioning over heterogeneous edge devices," *Institute of Electrical and Electronics Engineers*, vol. 29, no. 2, pp. 595–608, 12 2020. [Online]. Available: https://doi.org/10.1109/tnet.2020.3042320

[8] S. Safavi, S. Safavi, and Z. Shukur, "Investigating the role of blockchain in enhancing home security: A comprehensive study," p. 1, 12 2023. [Online]. Available: https://doi.org/10.1109/scored60679.2023.10563220