Safeguarding User Footprints in Shared Spaces: App-Based Privacy Controls for IoT

Ireish Purohit
Arizona State University

Atul Prakash
Arizona State University

Anand Gupta
Arizona State University

Anoop Reddy Repaka
Arizona State University

Preetham Akunuri
Arizona State University

ABSTRACT

As the proliferation of IoT devices continues to enhance daily living, concerns about privacy and data security become increasingly critical. Despite a general concern for privacy, individuals often remain unaware of and powerless against the invasive data collection practices of these devices or sensors. This paper introduces an IoT privacy infrastructure, designed to address these concerns by educating users about the privacy implications of IoT devices. The infrastructure empowers assistants applications to identify IoT sensors within the proximity of their users. The assistant mobile application detects IoT devices via BLE (Bluetooth Low Energy) beacons and provides users with detailed information regarding the data collection practices of each detected device.

1 INTRODUCTION

In an era increasingly dominated by the Internet of Things (IoT), the protection of individual privacy has become paramount. As IoT devices—equipped with cameras, microphones, and sensors—become ubiquitous in both public and private spaces, they silently harvest vast amounts of data about everyday activities. This data collection, while often benign and intended to enhance user convenience and security, can inadvertently lead to significant privacy invasions if not managed properly. For example, guests in environments with pervasive IoT infrastructure might not be aware that their actions are being monitored or recorded, potentially leading to discomfort or misuse of the collected data. This situation underscores the pressing need for solutions that empower users, enabling them to understand and control the privacy implications of IoT devices around them.

This report discusses the development of equivalent functionalities for the IoT and specifically emphasizes the essential privacy infrastructure necessary to facilitate privacy assistant applications tailored for the IoT ecosystem. Our research draws insights from studies indicating that individuals often harbor concerns regarding the data collection and utilization practices inherent to IoT technologies. The project contributes to this field by not only proposing a refined IoT infrastructure embedded with enhanced privacy controls but also demonstrating its efficacy through a mobile application and server infrastructure.

2 RELATED WORK

In the early 2000s, Marc Langheinrich [3] introduced a concept for privacy assistants in computing environments, emphasizing the use of beacons alongside service discovery protocols to communicate the privacy policies of data collection services. This framework aimed to establish a strict regulation of personal information flows through privacy proxies and a centralized privacy-focused database. In 2016, Edwards [2] also advocated for the development of intelligent systems capable of assisting users in making semi-automatic privacy decisions in IoT contexts.

Recent research highlights the increasing complexities and privacy challenges associated with the deployment of IoT devices. In their work, Das and Sadeh [1] emphasize the development of privacy assistants aimed at enhancing user control over personal data in IoT environments. Their proposed infrastructure supports the discovery of IoT resources and their data practices, enhancing user awareness.

Marky and Gerber [4] address privacy concerns from the perspective of guests in IoT-equipped households. Their research involved both qualitative and quantitative methods to understand the expectations and needs of both hosts and guests regarding privacy. We learned that privacy protection should facilitate cooperation without severely impacting the guest experience, proposing the use of automated personal privacy assistants to manage privacy without extensive guest interaction.

Prior research underscores the need for transparent and customizable privacy controls in IoT devices. Studies emphasize the importance of user visibility and the ability to adjust settings, such as guest modes, to protect data during visits, along with the financial implications of designing such systems. Additionally, innovative IoT privacy infrastructures have been developed to aid Personal Privacy Assistants (PPAs) in informing users about IoT resources and their data practices, showing promise in enhancing notice and choice mechanisms in these settings.

Challenges persist in implementing privacy choices, especially for smaller stakeholders with limited resources to comply with regulations like GDPR. Innovative methodologies involving user-centered and design space analysis have been proposed to improve user interactions with privacy settings in IoT systems.

3 APPROACH

Our research began with a comprehensive review of existing literature, which highlighted the increasing concern surrounding the privacy management of IoT devices in various environments. Most of the existing solutions to improve privacy in shared spaces rely on formal conversational chains with the device and data owner. However, our goal is to bring this closer to individuals and enable them to adjust the data collection settings if they're the ones being recorded. This review directed our focus towards a user-centric solution that empowers individuals to control the data collection behavior of IoT devices within their proximity

To address this, we conceptualized and developed an infrastructure that integrates IoT device management with user privacy preferences in professional settings such as offices or conference venues, where the presence of guests and visitors is frequent. The core of our proposed infrastructure is a mobile application, designed to discover nearby beacons. These beacons are placed strategically by the infrastructure admin to mark areas around which data is being recorded. These could be meeting rooms, labs, or even publicly accessible areas inside a building. These beacons are essential for identifying the specific locations of users and corresponding IoT devices that are active in those locations

The architecture of our system includes a central database maintained by an administrator. This database is crucial for mapping each area within the venue to its respective IoT devices, which are capable of recording various forms of data considered private to the user present in that area. As a user enters a specific room, the mobile app detects the nearby beacon. This detection enables the app to display the type of data being collected in that vicinity, along with several essential attributes such as the retention period and the device owner. We've empowered users with three significant privacy control options within the app:

- **Direct Mitigation:** For devices where users have direct control, they can choose to turn off specific devices directly through the app, ceasing all data collection immediately.
- **Indirect Mitigation:** Users can request the system administrator to delete/mask their data, providing a reactive control mechanism.
- **Alternate Location Search:** For users uncomfortable with any data collection, the app can guide them to alternative areas where no recording devices are active.

To simulate a real-world application of this infrastructure, we developed a prototype comprising the described components: beacons, a mobile application, and database hosted on a cloud service provider. This setup not only demonstrates the feasibility of our approach but also provides a scalable model that can be adapted to different professional settings, ensuring that privacy concerns are addressed dynamically and efficiently.

4 DESIGN & IMPLEMENTATION

In the landscape of smartphone usage, users exercise control over the apps they install and benefit from unified permission management tools, enabling them to review and regulate app permissions. However, the IoT realm presents a contrasting scenario. Here, users engage with technologies they often didn't deploy and may not even be aware of. This lack of awareness, coupled with a scarcity of user-accessible settings for managing IoT resources, poses a considerable challenge in informing users about data collection practices.

In the IoT sphere, users typically lack knowledge regarding the devices in their vicinity, the data these devices gather, and the subsequent utilization of that data. Addressing this challenge requires an infrastructure capable of facilitating the discovery of nearby IoT resources and elucidating their data practices. Alongside resource discovery, this infrastructure must facilitate the disclosure of information regarding the collected data and its utilization. Equally crucial is the provision of mitigation strategies to empower users to opt out of data collection.

To tackle these issues, we propose an architecture comprising three essential components: *Beacons and IoT sensors setup, a mobile application for sensor discovery*, and *Server to manage IoT infrastructure*.

4.1 Beacons and IoT sensors setup

Devices equipped with beacon technology can operate efficiently using various power sources. They can run for over a month on coin cell batteries, or for months with larger batteries, or even be powered externally for extended duration. Through Bluetooth Low Energy, beacon advertisements convey crucial information such as the UUID (16 bytes), major (2 bytes), and minor (2 bytes). Typically, this information follows a hierarchical structure, with the major and minor fields allowing for the subdivision of the identity established by the UUID. These values are configured by the deploying entity, offering flexibility in beacon deployment. Beacons serve to enhance context-awareness by determining whether an entity is within range. The granularity of location data required may vary across different scenarios. Hence, the combination of UUID, major, and minor fields can be utilized hierarchically in diverse manners to categorize and accommodate varying location granularity needs.

In our infrastructure, a single UUID identifier is utilized to recognize any region associated with it. Each distinct region is then assigned a unique major value, facilitating device identification of specific buildings. Additionally, within individual buildings, floors are distinguished by separate minor values, although these remain consistent across buildings to simplify floor identification for device applications. We have established a mapping between the IoT sensors located in the vicinity and the beacons installed in the corresponding areas. This mapping ensures a many-to-one relationship between IoT sensors and beacons. Consequently, we can determine all the sensors nearby a person by identifying which beacon's advertisement is being broadcasted. This approach enables efficient sensor discovery based on the proximity of the individual to specific beacon signals.

4.2 Mobile application for sensor discovery

Usually mobile applications employ two key methods, monitoring and ranging, to discover beacons.

Monitoring involves the application periodically scanning for beacon signals using the beacon UUID. When a beacon is detected, the application triggers a notification. This method is used by the application for detecting when a person enters or exits a specific area associated with a beacon.

Ranging, on the other hand, involves estimating the distance to each beacon based on signal strength after it has been discovered. This method provides more precise location information, allowing our application to determine the proximity of the user to each beacon.

In our mobile application, we've opted to utilize only the monitoring method to discover nearby beacons and subsequently locate nearby IoT sensors. Ranging, while a common approach in many applications, isn't applicable to our specific use case. This decision

stems from the fact that ranging primarily provides proximity information to beacons themselves rather than to the IoT devices mapped against those beacon identifiers.

4.3 Server to manage IoT infrastructure

All configuration data related to our IoT infrastructure is stored within a database. The schema consists of three main tables: Beacons, IoTDevices, and MitigationStrategies. The Beacons table includes fields for UUID, major, minor, and the associated IoTDeviceId. The IoTDevices table stores information about each IoT device, including its unique identifier, associated beacon ID, device type, name, location, owner, contact details, data collection requirements, data usage, retention period, data sharing information, compliance details, and last update timestamp. Additionally, the MitigationStrategies table contains fields for the IoTDeviceId and various mitigation options, such as direct, indirect, and alternate mitigation options, along with counts for each option selected by users.

Table 1: Data Model

Table Name	Fields
Beacons	uuid, major, minor, IoTDeviceId
IoTDevice	id, beaconid, deviceType, name, location, owner, contact, isDataCollectionRequired, dataCollectionType, dataUsage, dataRetentionPeriod, dataSharingInfo, dataComplianceInfo, lastUpdatedAt
MitigationStrategy	IoTDeviceId, directMitigationOption, indirectMitigationOption, alternateMitigationOption, directMitigationOptionSelectedCount, indirectMitigationOptionSelectedCount, alternateMitigationOptionSelectedCount

We provide access to this data through RESTful APIs exposed by our server, allowing the mobile application to fetch information about IoT devices associated with a specific beacon identifier, retrieve details about a particular IoT device, access mitigation options associated with an IoT device, and store the selected mitigation option chosen by the user. This architecture enables seamless communication between the mobile application and the server, facilitating efficient retrieval and management of IoT infrastructure information and mitigation strategies.

4.4 Interaction between components

4.4.1 IoT Device Discovery. The sequence diagram 1 illustrates the communication flow between self-broadcasting beacons, an iOS mobile application, and the server.

The process begins with the iOS mobile application initiating beacon scanning by invoking the startScanning(Beacon_UUID) function, specifying the UUID of the beacon to be scanned for. As long as beacon scanning is not stopped (stopScanning(Beacon_UUID)), the LocationManager within the iOS app continues monitoring and ranging for nearby beacons.

Upon detection of a nearby beacon, the LocationManager triggers the onBeaconDetected(beacons) event, providing details about

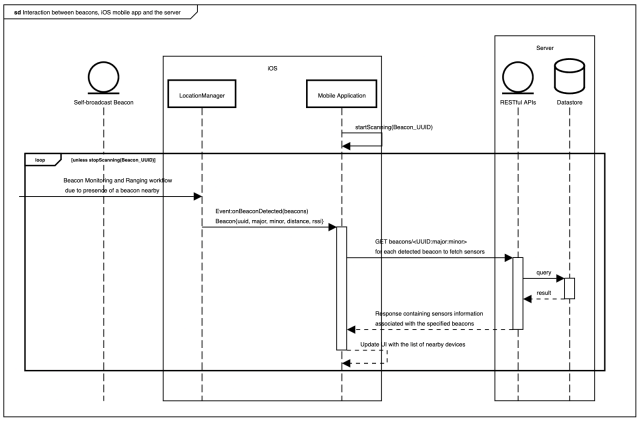

Figure 1: Interaction between components

the detected beacons, including their UUID, major, minor, distance, and received signal strength indicator (RSSI), to the mobile application.

The mobile application then utilizes the received beacon information to make API requests to the server. For each detected beacon, the application sends a GET request to the server's RESTful APIs (GET beacons/<UUID:major:minor>) to fetch information about sensors associated with the specified beacon. The server receives the API request and queries the datastore to retrieve information about sensors associated with the specified beacon. After processing the query, the server responds to the mobile application with the result containing information about the sensors associated with the specified beacon.

Finally, the mobile application updates its user interface (UI) with the list of nearby devices, presenting the information retrieved from the server to the user.

4.4.2 Presenting Mitigation Strategies. When a user accesses information about a specific IoT device through the application, they are presented with comprehensive details about the device itself as well as its associated data collection practices. Alongside this information, users are provided with various mitigation options aimed at preventing or minimizing data collection if they wish to do so. In cases where data collection is mandatory, the application suggests alternative locations to the user where data collection is not required. Conversely, if data collection is optional, the app offers both direct and indirect mitigation options for users to choose from. The user's selected mitigation option is stored in the MitigationStrategy database, allowing infrastructure administrators to leverage this data for making informed decisions regarding the organization of IoT devices and their respective data collection practices.

4.4.3 Prototype workflow. In our implemented prototype for the proposed infrastructure, a workflow will involve screens as in - Figure 2 displaying a list of devices discovered in the vicinity, Figure 3 where users are presented with three available options to mitigate data collection, Figure 4 where mitigation options are tailored specifically for scenarios where data collection is mandatory.

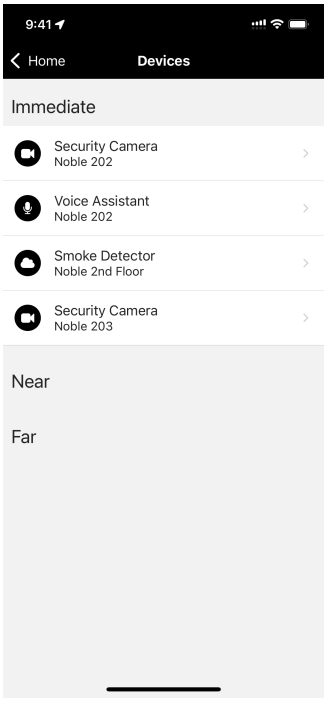

Figure 2: Active devices discovered in the mobile app

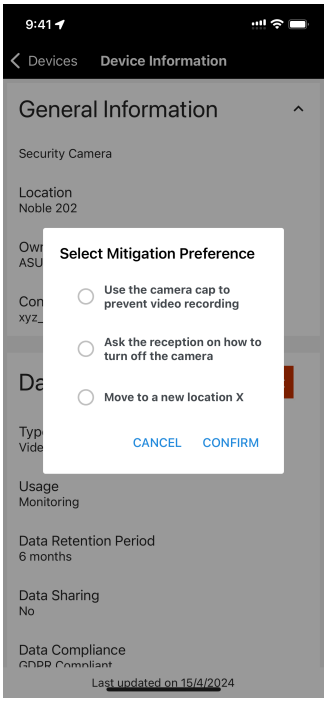

Figure 3: Three mitigation strategies available for the users

5 CONCLUSION & FUTURE WORK

Our project has laid the groundwork for a robust privacy management tool designed for IoT environments, addressing the critical need for user control over personal data. The development of a IoT privacy infrastructure underscores a significant advancement

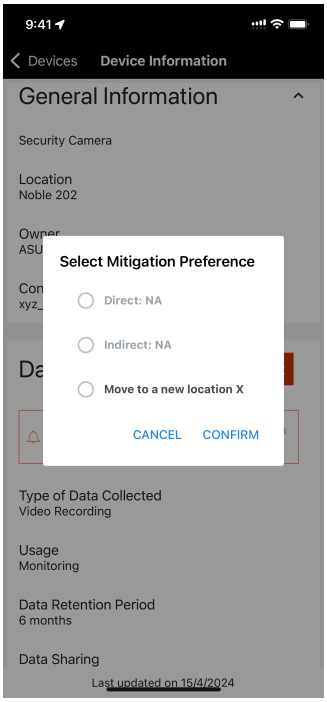

Figure 4: Mitigation strategy available for the user if the data collection is mandatory

in enabling users to manage their privacy through an intuitive application interface. The proposed solution for the mobile application is also significantly less power demanding than running normal location updates constantly in the background. This system uses distance-based measures such as RSSI to theoretically localize beacons, categorizing them as "near" or "far." Although promising, given the challenges related to signal strength and the diverse deployment settings, beacon technology isn't designed for precise location identification purposes. While it aims to offer accuracy at the room level, achieving successful deployment requires careful consideration of various factors. These include the quantity and placement of beacons, anticipated use cases, and numerous other variables essential for ensuring an optimal user experience. An operational challenge within our current system is the manual entry of device data by administrators—a process that could be streamlined significantly through automation. Future iterations of our project could explore automated methods for device recognition, such as employing unique device IDs, Wi-Fi names, or Bluetooth technologies. Automating device data entry would not only increase system efficiency but also enhance user-friendliness by reducing the administrative burden, thereby improving the overall user experience.

Beyond individual privacy management, the practical applications of this technology are vast. In organizational settings such as libraries and offices, our system can be integrated to manage access to meeting or conference rooms, allowing occupants dynamic control over their data and privacy settings. This demonstrates the system's adaptability to various environments where privacy concerns are paramount. To further enhance user control over nearby IoT devices, our project could incorporate machine learning-based prediction models in future developments. These models would

recommend personalized mitigation strategies based on individual preferences and historical interactions with IoT devices, thus refining the app's personalization and effectiveness.

In conclusion, while we have established a solid foundation for managing privacy in IoT environments, there is considerable potential for enhancements and expansions. Future research should focus on deepening automated data integration techniques, broadening the application contexts, and developing more nuanced user control mechanisms

REFERENCES

[1] Anupam Das, Martin Degeling, Daniel Smullen, and Norman Sadeh. 2018. Personalized Privacy Assistants for the Internet of Things: Providing Users with Notice and Choice. *IEEE Pervasive Computing* 17, 3 (2018), 35–46. https://doi.org/10.1109/MPRV.2018.03367733

[2] Lilian Edwards. 2016. Privacy, security and data protection in smart cities: a critical EU law perspective. *European Data Protection Law Review* 2, 1 (15 March 2016), 28–58.

[3] Marc Langheinrich. 2002. A Privacy Awareness System for Ubiquitous Computing Environments. In *UbiComp 2002: Ubiquitous Computing*, Gaetano Borriello and Lars Erik Holmquist (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 237–245.

[4] Karola Marky, Nina Gerber, M Pelzer, and M. Khamis. 2022. "You offer privacy like you offer tea": Investigating Mechanisms for Improving Guest Privacy in IoT-Equipped Households. *Proc. Priv. Enhancing Technol.* 2022 (2022), 400–420. https://api.semanticscholar.org/CorpusID:251384817