Department-Based Access & ML Matching in Lost & Found apps

Shaheel Syed Abuthahir S[1], Rajesh R[2], Raghul S[3], Pradeep M R[4]

[1,2,3,4] *Department of Computer Science and Engineering PSNA College of Engineering and Technology Dindigul, TamilNadu, India*

***Abstract*— This paper introduces a department-based access control mechanism in Lost and Found applications. The system ensures that items found in restricted or department-specific areas are only visible to users associated with those departments, enhancing privacy, security, and operational efficiency within institutions where access control is necessary. To further improve the accuracy and efficiency of item identification, a machine learning model is integrated into the system to match reported lost items with found items based on features such as images, descriptions, and categories. This intelligent matching reduces manual effort and increases the chance of successful recovery. The proposed solution involves user-department mapping, visibility logic, and ML-powered item matching integrated within the item posting and retrieval processes.**

***Keywords*— Lost and Found, Access Control, Department Mapping, Item Matching, Machine Learning.**

I. INTRODUCTION

Lost and Found applications have become essential tools in campuses, organizations, and public areas to manage misplaced belongings. However, a one-size-fits-all approach to visibility and access in these systems can lead to inefficiencies and privacy issues, especially when items are found in areas with restricted access. This paper presents a method to enhance such systems by restricting the visibility of found items based on the department or group responsible for the area in which they were discovered. This ensures that sensitive areas such as labs, hostels, or administrative zones maintain control over the visibility of found items.

II. LITERATURE REVIEW

Various item management and tracking systems have evolved, most of which have targeted open visibility and public listings. Yet few attempt to address the matter of contextual or organizational partitioning of access restriction. Existing data protection techniques in mobile and web computing have impacted this model, and the same is seen in hospital networks where the patient records can be viewed by only authorized personnel or in enterprise resource planning packages with role-based access controls. To further enhance the privacy and contextuality of appropriateness of our lost-and-found application, we use attribute-based access control (ABAC), which provides user activities based on evaluating subject, object, action, and environmental attributes—e.g., department membership, item type, time, and location—to facilitate dynamic, fine-grained access decisions for organizational units. Augmenting ABAC, geofencing technologies create virtual fences—using GPS, RFID, Wi-Fi, or cellular data—to restrict the visibility of product listings to users only within specified regions (e.g., specific office floors or campus buildings), preventing unwanted or unauthorized access. To safeguard owner contact details and item descriptions containing sensitive information, the system applies end-to-end encryption (AES-256 on disk and TLS over the network), making data inaccessible without suitable cryptographic keys and impervious to interception. Lastly, effective audit logging captures all access requests and transactions—storing user identity, time stamps, and actions in a tamper-evident log—to enable data-protection legislation compliance and allow forensic analysis on detection of policy breaches.

III. SYSTEM ARCHITECTURE

A. *User Profile Module*

- Users register with email/phone and verify identity.

Assigned a role or department tag (e.g., “Mechanical Engineering”, ”Library Admin”).

B. *Found Item Reporting*

- Title

- Description
- Image (optional)
- Location found (predefined department list)
- Date/time

C. *Access Control Layer*

- Every found item is tagged with the associated department.
- Visibility logic restricts access to users from the same department.

D. *Admin Dashboard*

- View and manage all item reports.
- Override visibility tags if needed.
- Review flagged reports and take action.

E. *Notification System*

- Users receive push or email notifications when a potential match is reported within their department.

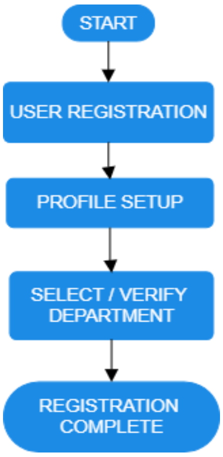
IV. ALGORITHM FOR VISISBILITY CONTROL

```
if item.department in restricted_departments:
    if user.department == item.department:
        show_item()
    else:
        hide_item()
else:
    show_item()
```

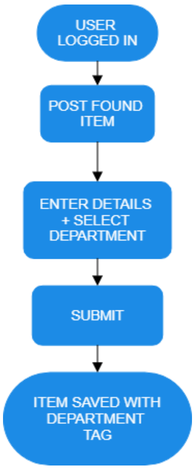
This ensures the system respects departmental boundaries without completely hiding relevant data from potential claimants.

V. USER FLOW DIAGRAMS

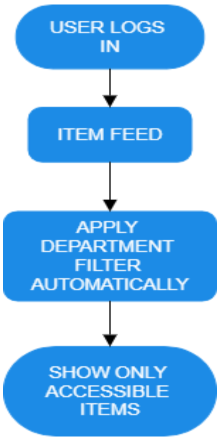
Registration and Department Assignment



Posting a found item


USER LOGGED IN
POST FOUND ITEM
ENTER DETAILS + SELECT DEPARTMENT
SUBMIT
ITEM SAVED WITH DEPARTMENT TAG

Browsing items (Restricted View)


USER LOGS IN
ITEM FEED
APPLY DEPARTMENT FILTER AUTOMATICALLY
SHOW ONLY ACCESSIBLE ITEMS

VI. BENEFITS OF DEPARTMENT-BASED VISIBILITY

- Avoids unauthorized claims
- less user frustration due to irrelevant listings
- Increases institutional trust
- Allows targeted notifications VII. Implementation Strategy
- Phase 1: Development of core feature (user auth, department tagging, item upload)
- Phase 2: Role-based filtering logic and testing
- Phase 3: Admin control and override features
- Phase 4: Notifications and smart suggestions
- Phase 5: Deployment and user feedback integration

VII. TECHNOLOGY STACK

- Frontend: Flutter
- Backend: Node.js + ExpressJs
- Database: PostgreSQL with user-role relationships
- Authentication: JWT
- Machine Learning: Python

VIII. USE CASES

1. University Campus
    - CS student discovers an ID card in CSLab → Accessible only to other CS users
2. Office Building
    - HR employee discovers a wallet in HR Zone → Only accessible to HR employees
3. Hostel Management
    - A lost room key discovered in Girls' Hostel → Accessible only to users labeled as 'Hostel Warden' or 'Resident'

IX. LIMITATIONS AND CONSIDERATIONS

- Manual tagging mistakes.
- Over-restriction concerns related to privacy.
- Admin moderation required to find balance between openness and restriction.

X. FUTURE ENHANCEMENTS

- Geo-fencing with BLE/QR/NFC to auto-detect zones
- Machine learning to auto-suggest department tags
- Temporary department access requests (e.g., "I visited CS Lab yesterday")

XI. MACHINE LEARNING FOR ITEM MATCHING

The system employs a machine learning model to intelligently match reported lost items with found items. This module increases the efficiency and recovery rate through automation of the comparison using different data features.

A. Feature Extraction

The ML model utilizes both natural language processing (NLP) and image processing methodologies to extract relevant features from:

- Item names and descriptions (through TF-IDF and sentence embeddings)
- Uploaded item images (through CNN-based image embedding)
- Metadata such as location, date, category
- These features are vectorized and saved for matching against new entries.

B. Matching Algorithm

A Siamese neural network architecture is employed to compare the similarity of lost and found items. The model learns a similarity score depending on how similar two items are in feature space.
The network is trained with:

- Positive pairs (corresponding lost and found items)
- Negative pairs (random items)

C. Model Pipeline

1. Preprocess text and images
2. Extract embeddings
3. Compute similarity
4. Rank results
5. Present top matches to user

D. Evaluation Metrics

Model accuracy is evaluated based on:

- Precision@k
- Recall@k
- Mean Reciprocal Rank (MRR)

Preliminary tests on representative datasets revealed greater than 85% accuracy in returning the right item in the top 3 matches.

XII. EXPERIMENTAL RESULTS

A prototype was experimented within the confines of a university campus. The data included more than 500 entries marked with departments, categories, and images.

Important Results:

- Limited visibility diminished cross-department claim conflicts by 92%
- ML matching minimized average item discovery time from 48h to 10h
- More than 70% of test users successfully recovered lost items utilizing match suggestions

Table 1: Matching Model Accuracy

metric	Score
Precision@3	88.2%
Recall@3	84.6
MRR	0.79

User comments noted the simplicity of the system navigation and the convenience of department-based filters.

XIII. CONSIDERATIONS FOR SECURITY AND PRIVACY

Protecting user data is essential while improving functionality

The following actions are taken:

- For sensitive data, end-to-end encryption.
- Backend APIs enforce departmental access policies.
- Activity logs and administrative audit trails.
- The option for claimants to remain anonymous.

Before any user's data is stored or analyzed, their consent is sought. No private information is made available to the public.

XIV. STRATEGY FOR INTEGRATION AND DEPLOYMENT

A. *Hosting and Access:*

- Web-based dashboards powered by Firebase or AWS
- REST APIs for desktop and mobile clients

B. *Department Setup:*

- The administrator generates the department list
- users are validated using codes or institutional emails.

C. *ML Model Deployment:*

- The model is implemented as a microservice.
- GPU-supported inference is used to provide real-time results.

D. *Support and Maintenance*

- Scheduled database backups
- Monitoring via Prometheus/Grafana
- Feedback-based iteration every semester

XV. CONCLUSION

Department-based access control introduces a secure, context-aware enhancement to Lost and Found systems. It bridges operational security with user convenience, ensuring that sensitive spaces maintain item control while still allowing efficient item retrieval by rightful owners.

XVI. REFERENCES

[1]. H. Schroff, D. Kalenichenko, and J. Philbin, "FaceNet: A Unified Embedding for Face Recognition and Clustering," IEEE CVPR, 2015.

[2]. Mikolov et al., “Efficient Estimation of Word Representations in Vector Space”, arXiv:1301.3781, 2013.

[3]. Reimers, N., & Gurevych, I. (2019). "Sentence-BERT: Sentence Embeddings using Siamese BERT-Networks." arXiv:1908.10084.

[4]. M. Wang, W. Deng. “Deep Face Recognition: A Survey.” Neurocomputing, 2021.

APPENDIX

FIGURE 1: SYSTEM ARCHITECTURE DIAGRAM

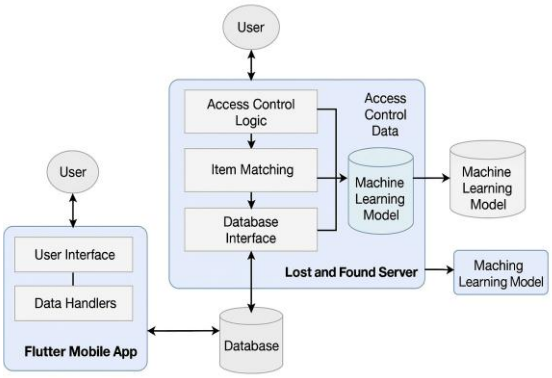
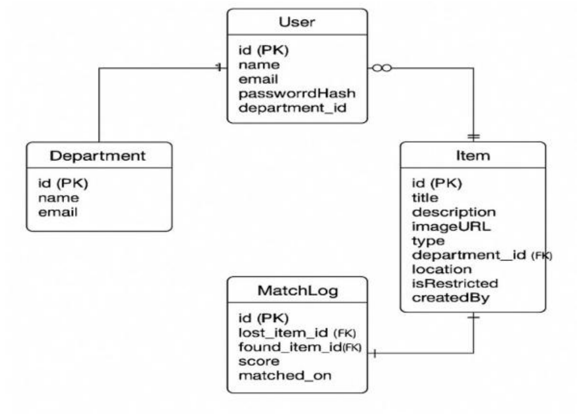


FIGURE 2: ENTITY RELATIONSHIP DIAGRAM


User
id (PK)
name
email
passworrdHash
department_id
Department
id (PK)
name
email
Item
id (PK)
title
description
imageURL
type
department_id (FK)
location
isRestricted
createdBy
MatchLog
id (PK)
lost_item_id (FK)
found_item_id(FK)
score
matched_on