Task 1: Project Size Measurement Using FPA

Project Work

University of Insubria

Authors: Roberto Vicario, Emanuele Andreu

2024/2025

Application Boundary

The application boundary includes **internal data files** and **core functionalities**, which are detailed in the following sections. These elements represent the internal logic, configurations, and data storage that the application directly manages and maintains.

Vice versa, the boundary excludes components that are **data sources** controlled by external systems. By placing these outside the boundary, we clarify that while the application interacts with them, it does not manage or control them.

Logical Data Files

Internal Logical Files (ILF):

- **User Data:** Contains information about authorized users, including names, credentials, and access profiles.
- **Access Log and Notifications:** Stores access events with timestamps and user details, or attempts at unauthorized access.

External Interface Files (EIF):

- **External Cloud Data:** Data stored and managed by external cloud providers, offering storage and backend functionality.
- **IoT Devices:** Interfaces with data from IoT devices, possibly managed by other systems but used for data collection, such as sensors or cameras.

Transactions

External Inputs (EI):

- **Video Input from IoT Cameras:** Incoming video streams feed the facial recognition algorithm to identify individuals.
- **Configuration Input from Administrators:** Allows administrators to set security thresholds, configure authorized users, and manage alert escalations.

External Outputs (EO):

- **Real-Time Security Notifications:** Sends notifications to administrators in case of unauthorized access, including details like time and location.
- **Periodic Access Reports:** Regularly generated reports on access activity, including statistics on authorized and unauthorized access attempts.

Transactions

External Inquiries (EQ):

- **Access History Consultation:** Enables querying the historical log to verify who accessed or attempted to access the system.
- **Security Configuration Inquiry:** Provides configured security information.

Key Components

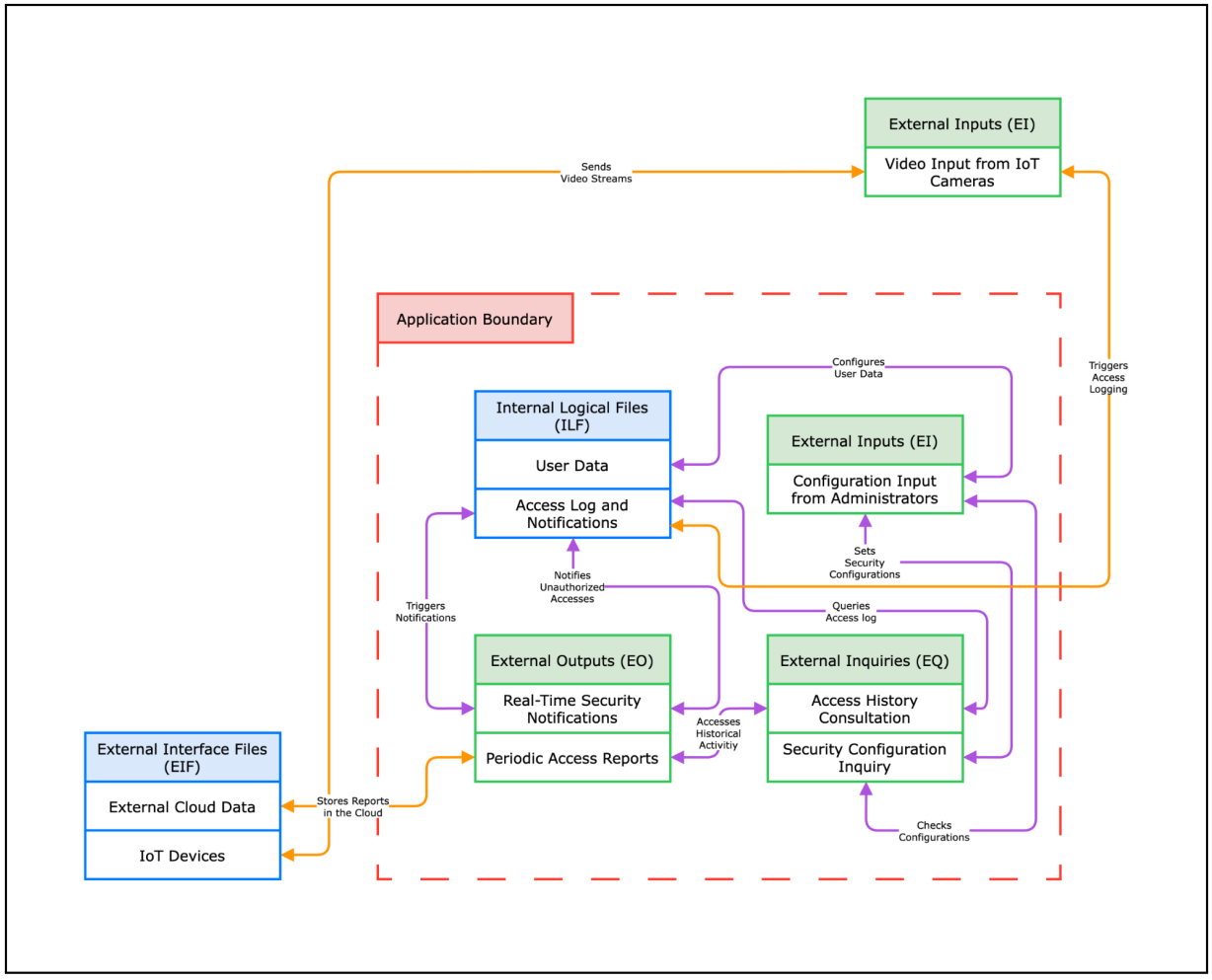

Figure: The diagram shows data flow between the system components.

Data Elements Type (DETs)

Internal Logical Files (ILF):

- **User Data:** Includes ID, name, role, biometric data, access status, etc. (30 DET).
- **Access Log and Notifications:** Access log, timestamp, user ID, action, criticality level, recognition result, notifications, etc. (55 DET).

External Interface Files (EIF):

- **External Cloud Data:** Cloud provider configuration data, ID, timestamp, status, fault tolerance, etc. (15 DET).
- **IoT Devices:** IoT device information, ID, type, status, connection, firmware, etc. (20 DET).

Data Elements Type (DETs)

External Inputs (EI):

- **Video Input from IoT Cameras:** Video feed with metadata: timestamp, camera ID, resolution, etc. (12 DET).
- **Configuration Input from Administrators:** Configuration parameters, ID, security, authorizations, etc. (20 DET).

External Outputs (EO):

- **Real-Time Security Notifications:** Content, timestamp, type, level, recipients, etc. (18 DET).
- **Periodic Access Reports:** Access report, violations, timestamp, aggregated details, etc. (25 DET).

Data Elements Type (DETs)

External Inquiries (EQ):

- **Access History Consultation:** Access history: date, user ID, type, query results, etc. (20 DET).
- **Security Configuration Inquiry:** Displays configuration, ID, security status, access level, etc. (15 DET).

Record Elements Type (RETs)

- **User Data (3 RETs):** User data management includes three distinct categories of data:
  1. Identification data (e.g., user ID, name, role), used for registration and access management.
  2. Biometric data (e.g., facial data), used for facial recognition.
  3. Access and security data, for traceability and control.
- **Access Log and Notifications (4 RETs):** This file includes four distinct types of logs:
  1. Access log (e.g., timestamp, user ID, access type), to record access activities.
  2. Notification log (e.g., criticality level, notification type), for security notifications.

Record Elements Type (RETs)

3. Violation log (e.g., user ID, unauthorized action), that records unauthorized access.
4. Change history, to track all administrative actions.

- **External Cloud Data (2 RETs):** Includes data from various cloud providers to ensure availability and fault tolerance:

1. Provider configurations (e.g., provider ID, connection status).
2. Backup of critical data (e.g., timestamp, backup status) for operational continuity.

Record Elements Type (RETs)

- **IoT Devices (3 RETs):** Gathers information from IoT devices in three distinct categories:
  1. General device data (e.g., ID, type, status).
  2. Firmware update data (e.g., version, update timestamp).
  3. Connection data and current device status.

File Types Referenced (FTRs)

External Inquiries (EQ):

- **Video Input from IoT Cameras (2 FTRs):** References the following files to collect and manage camera metadata and monitor access:
  1. IoT device data to obtain information about recording devices.
  2. Access log and notifications to monitor access and security.
- **Configuration input from administrators (3 FTRs):** Configuration input uses the following files for security configurations:
  1. Authorized user data to specify roles and authorizations.

File Types Referenced (FTRs)

2. Access log and notifications to monitor configuration changes.
3. IoT device data to update device configurations.

External Outputs (EO):

- **Real-Time Security Notifications (2 FTRs):** References the following files to send notifications based on access events and recipients:
  1. Access log and notifications to get details of access events.
  2. Authorized user data to identify notification recipients.
- **Periodic Access Report (3 FTRs):** The periodic report accesses the following files to aggregate and present information:

File Types Referenced (FTRs)

1. Access log and notifications for access details.
2. Authorized user data to link access to users.
3. IoT device data for information on device access.

External Inquiries (EQ):

- **Access History Consultation (3 FTRs):** Consults the following files to display the complete activity history:
  1. Access log and notifications for detailed access logs.
  2. Authorized user data to identify the users involved.
  3. IoT device data for information on devices used in access.

File Types Referenced (FTRs)

- **Security Configuration Inquiry (2 FTRs):** References the following files to display the current security settings:
  1. Security parameter configuration for details on current configurations.
  2. Access log and notifications to verify recent configuration changes.

System Complexity

Component	Type	RETs	DETs	FTRs	Complexity
Authorized User Data	ILF	3	30	-	Average (10)
Access Log and Notifications	ILF	4	55	-	High (15)
Cloud Provider Configurations	EIF	2	15	-	Low (5)
IoT Device Data	EIF	3	20	-	Average (7)
Video Feed for Facial Recognition	EI	-	12	2	Average (4)
Security Parameter Configuration	EI	-	20	3	High (6)
Real-Time Alarm Notifications	EO	-	18	2	Average (5)
Access and Security Report	EO	-	25	3	High (7)
Access History Consultation	EQ	-	20	3	High (6)
Current Security Configurations View	EQ	-	15	2	Average (4)

Table: System complexity calculation.

Function Points (FPs)

Component	Low	Average	High	Total
Input	0 x 3	1 x 4	1 x 6	10
Output	0 x 4	1 x 5	1 x 7	12
Inquiry	0 x 3	1 x 4	1 x 6	10
ILF	0 x 7	1 x 10	1 x 15	25
EIF	1 x 5	1 x 7	0 x 10	12
FP				**69**

Table: Function Points (FP) calculation.

Conclusion

The analysis has provided an overview of the application's structure, focusing on its internal data files, core functionalities, and interactions with external systems.

The system's complexity has been evaluated using function points, revealing a moderate overall complexity score of 69.

Bibliography

The analysis was carried out with guidance from the materials of the course [1].

Luigi Lavazza.
Functional size measurement. software project management, 2024.