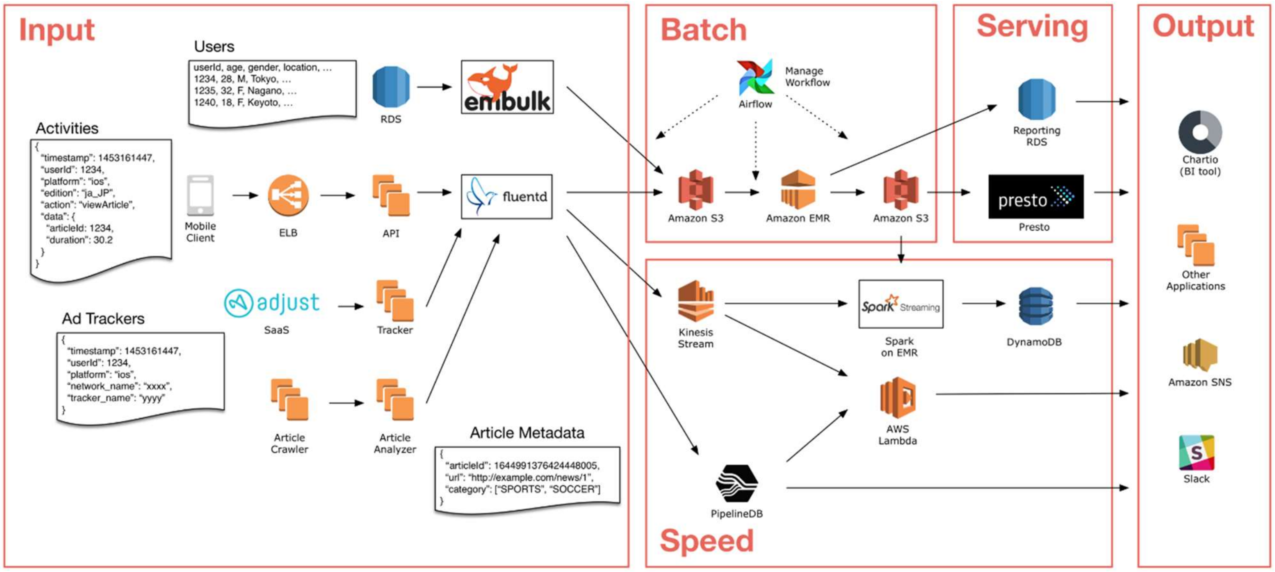
Alex Smetana

CIS360 – Lab02

03/10/2023



INPUT

Security Patterns: SP-024: IPhone Pattern

ACTOR: **Mobile Client** - User inputs data and inputs information to database storage. Uses Embulk and Fluetd to collect data inputed by a user and sends it to storage.

Embulk - a bulk data loader. It helps transfer between types of databases or storage.

Fluentd – Open-source data collector

Controls:

- AC-07 – Unsuccessful Login Attempts – Enforces a limit of consecutive invalid access attempts by a user.
- AT-02 Security Awareness – Provides basic security training to all users.
- IA-03-Device Identification and Authentication- System identifies and authenticates specific devices before a connection occurs.
- PS-06 – Access Agreements – Completes signed access agreements before authorization.
- PL-04 – Rules of Behavior – Agreement to the individual acknowledging that they agree to the behavior.

- SA-07 - User Installed Software - Users can install software if it is permitted by the organization.
- SC-18 – Mobile Code – Authorizes/monitors the use of mobile code in a system. Restricts mobile code based on potential to cause damage to a system.

BATCH/ SERVING

Security Pattern: SP-008 Public Web Server Pattern

ACTOR: **AWS Storage** - Data is sent to Amazon S3 and Amazon EMR using AWS. Managed by Apache Airflow.

Amazon S3 – Simple Storage Service, used for storage using AWS.

Amazon EMR – Simplifies running big data frameworks using AWS

Presto – Database Query Engine. Allows for SQL.

Apache Airflow – Open-source workflow management platform for data engineering pipelines

Controls:

- CP-06 Alternate Storage Site – Organization identifies alternative site for backup.
- CP07- Alternate Processing Site- Organization identifies alternative processing site for critical business functions.
- CP-09 Information System Backup – Organization conducts backups of both user-level and system level information. Protects backup storage physically.
- MP-04 Media Storage – Organization physically controls and stores information within stored areas.
- MP-06 Media Sanitization – Organization sanitizing both physical and nonphysical media.

SPEED

Security Pattern: SP-0111 Cloud Computing Pattern

ACTOR – Database Server - Data is sent to Database storage and servers. Data is output for a user to view.

Spark on EMR - Distributed processing system commonly used for big data workloads.

Controls:

- IA-02 – User Identification and Authentication - Information system protects the confidentiality of transmitted information
- SC-05 Denial of Service Protection – Information system protection from DOS attacks
- SC-08 – Transmission Integrity - Information system protection of integrity of the information.
- SC-09 – Transmission Confidentiality – Information system protects the confidentiality of transmitted information.
- SC-13 – Use Of Cryptography – Uses cryptography during the transfer of data.

General Security

Security Pattern: SP-016

ACTOR: **Security Operations** – General rules that will apply across all systems.

General Controls:

- AU-07 – Audit Reduction and Report Generation – The information system provides an audit reduction and report generation capability.
- CA-03 – Information System Connections – Organization authorizes all connections using system connection agreements and monitors the system.
- CA-04 – Security Certification – Assesses security controls to determine if the controls are working correctly and producing the desired outcome.
- CA-05 – Plan of Action and Milestones - The organization develops and updates [Assignment: organization-defined frequency], a plan of action and milestones for the information system that documents the organization's planned, implemented, and evaluated remedial actions to correct deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system.
- MP-02 Media Access – Restricts access to information system media to authorized individuals.
- RA-05 – Vulnerability Scanning – Organizations scans for vulnerabilities and reports them when found.
- SA-05 Information System Documentation – Organization obtains, protects, and makes available to authorized individuals documents of the system.
- SI-03-Malicious Code Protection – The information system implements malicious code protection.