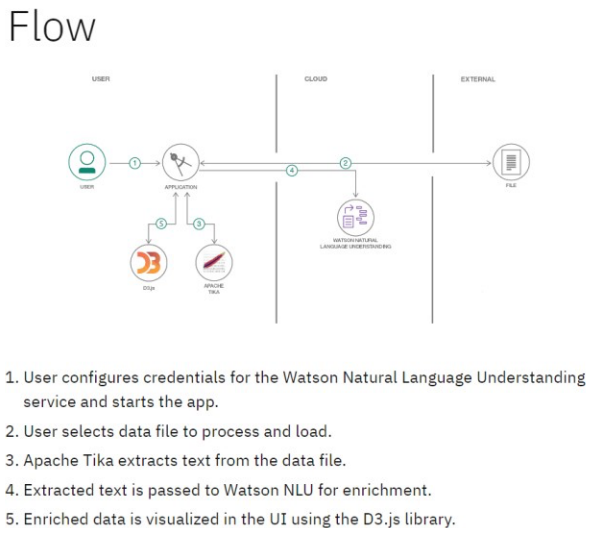
Project Design Phase-II
Data Flow Diagram & User Stories

Date	27 October 2023
Team ID	PNT2022TMIDxxxxxx
Project Name	AI-Based Threat Intelligence Platform
Maximum Marks	4 Marks

Data Flow Diagrams:

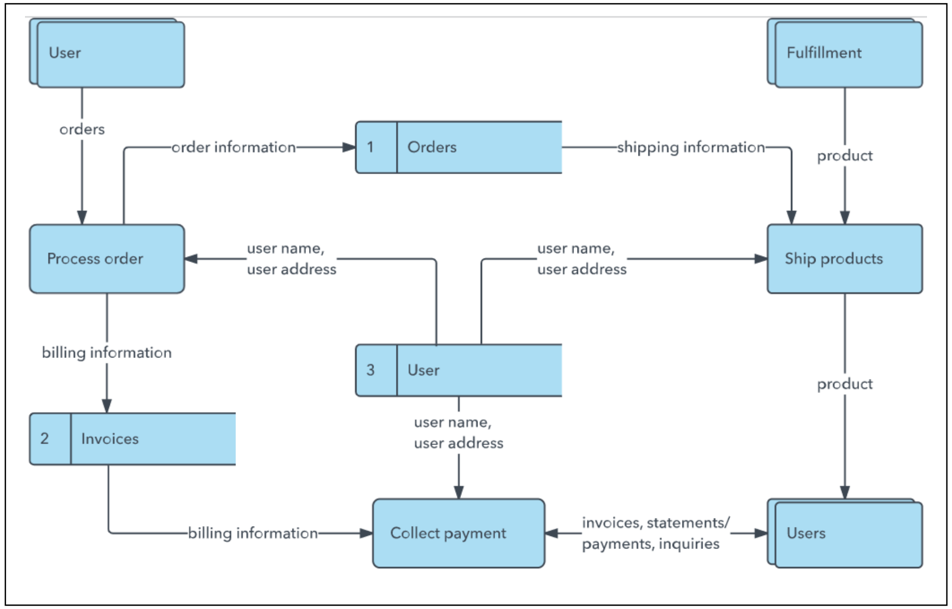
A Data Flow Diagram (DFD) is a traditional visual representation of the information flows within a system. A neat and clear DFD can depict the right amount of the system requirement graphically. It shows how data enters and leaves the system, what changes the information, and where data is stored.

Example:


Flow

1. User configures credentials for the Watson Natural Language Understanding service and starts the app.
2. User selects data file to process and load.
3. Apache Tika extracts text from the data file.
4. Extracted text is passed to Watson NLU for enrichment.
5. Enriched data is visualized in the UI using the D3.js library.

Example: DFD Level 0 (Industry Standard)



For web

```
graph LR
  A[User] --> B[Web Interface]
  B --> C[Threat Intelligence API]
  C --> D[Data Sources]
  D --> E[Data Collection]
  E --> F[Data Analysis]
  F --> G[Data Dissemination]
  G --> B
  subgraph Data Sources
    D1[OSINT] --> E
    D2[Commercial Feeds] --> E
    D3[Government Reports] --> E
  end
  subgraph Data Analysis
    F1[NLP] --> F2[ML]
    F2 --> F3[Sentiment Analysis]
    F3 --> F4[Threat Scoring]
    F4 --> F5[Threat Classification]
    F5 --> F6[Threat Correlation]
    F6 --> F
  End
```

This is a data flow diagram that shows how a user interacts with a web interface and a threat intelligence API to access data from various sources. The diagram has the following components:

- User: The person who uses the web interface and the API to view and download threat intelligence data.
- Web Interface: The graphical user interface that provides the user with a dashboard, reports, alerts, and settings for the threat intelligence platform.
- Threat Intelligence API: The application programming interface that allows the user to query, filter, and download the threat intelligence data in different formats (such as JSON, XML, CSV, etc.).
- Data Sources: The external sources of threat intelligence data, such as open-source intelligence (OSINT), commercial feeds, government reports, etc.
- Data Collection: The process of gathering and aggregating the data from different sources using various methods (such as web scraping, crawling, parsing, etc.).
- Data Analysis: The process of applying artificial intelligence (AI) techniques to analyze and enrich the data, such as natural language processing (NLP), machine learning (ML), sentiment analysis, etc.
- Data Dissemination: The process of distributing and delivering the data to the user through the web interface and the API.

For app

```
graph LR
  A[User] --> B[Mobile App]
  B --> C[Cloud Service]
  C --> D[AI Model]
  D --> E[Credential Leakage Database]
  E --> F[Credential Leakage Detection]
  F --> G[Credential Leakage Notification]
  G --> B
  subgraph Cloud Service
    C1[Authentication] --> C2[Authorization]
    C2 --> C3[Synchronization]
    C3 --> C4[Configuration]
    C4 --> C
  end
  subgraph AI Model
    D1[Crawler] --> D2[Parser]
    D2 --> D3[Indexer]
    D3 --> D4[Matcher]
    D4 --> D5[Filterer]
    D5 --> D6[Risk Assessor]
    D6 --> D
  End
```

- As a user, I want to install the mobile app of the threat intelligence platform, so that I can monitor my online accounts and credentials.
- As a user, I want to connect the app to the cloud service of the platform, so that I can sync my data and settings across devices.
- As a user, I want to use the AI model of the platform to scan the web for potential credential leakage incidents, so that I can identify and mitigate the risks.
- As a user, I want to receive notifications from the app when a credential leakage is detected, so that I can change my passwords and secure my accounts.

- The cloud service includes authentication,

User Stories

Use the below template to list all the user stories for the product.

User Type	Functional Requirement (Epic)	User Story Number	User Story / Task	Acceptance criteria	Priority	Release
Customer (Mobile user)	Registration	USN-1	As a user, I can register for the application by entering my email, password, and confirming my password.	I can access my account / dashboard	High	Sprint-1
		USN-2	As a user, I will receive confirmation email once I have registered for the application	I can receive confirmation email & click confirm	High	Sprint-1
		USN-3	As a user, I can register for the application through Facebook	I can register & access the dashboard with Facebook Login	Low	Sprint-2
		USN-4	As a user, I can register for the application through Gmail		Medium	Sprint-1
	Login	USN-5	As a user, I can log into the application by entering email & password		High	Sprint-1
	Dashboard					
Customer (Web user)	Sign-up	USR-1	The graphical user interface that provides the user with a dashboard, reports, alerts, and settings for the threat intelligence platform.		High	Sprint-1
		USR-2	As a user, After signup it can use the credentials To sign-in			Sprint-1
		USR-3	As a user, I can register for the application through Facebook		Low	Sprint-2
		USN-4	As a user, I can register for the application through Gmail		Medium	Sprint-1
	Sign-in	USN-5	As a user, I can log into the application by entering email & password		High	Sprint-1
Administrator			Manage the configuration and settings of the threat intelligence platform, such as defining the intelligence sources, requirements, preferences, and goals.		High	Sprint-1
			Authenticate and authorize the users and stakeholders who access the threat intelligence		High	Sprint-1

			platform, such as analysts, managers, and executives.			
			Synchronize the data and settings across different devices and platforms, such as web interface, mobile app, and cloud service.		High	Sprint-1
			Coordinate and collaborate with other teams and roles involved in the project, such as developers, testers, analysts, and vendors.		Low	Sprint-2