## Data Flow and Processing

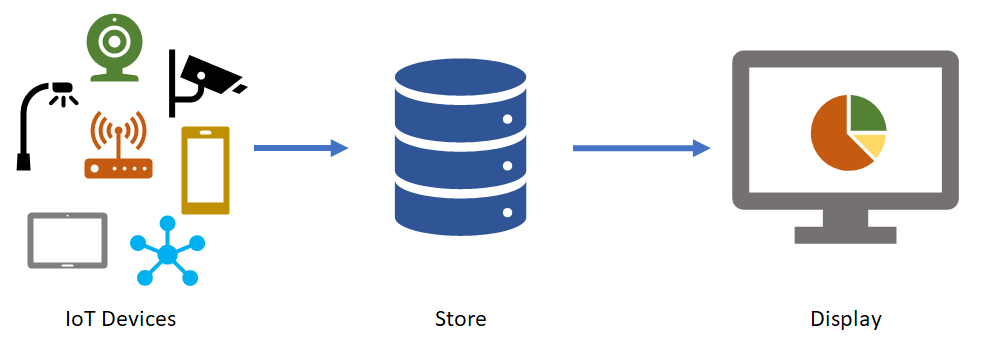
As data is delivered to the IoT backend, it is important to understand how the flow of data processing may vary. Depending on scenarios and applications, data records can flow through different stages, combined in different order, and often processed by concurrent, parallel tasks.

These stages can be classified in four categories - storage, routing, analysis and action/display:

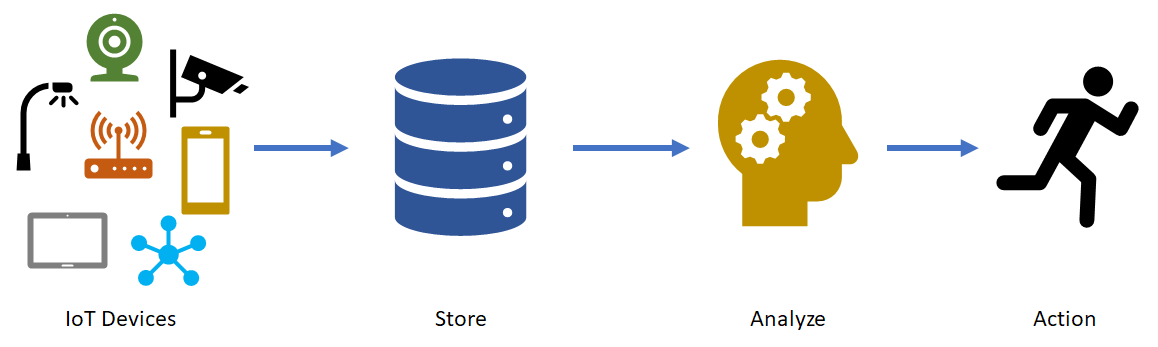
* Storage includes [in-memory caches](https://en.wikipedia.org/wiki/CPU_cache), temporary queues and permanent archives (e.g. a database).
* Routing allows sending data records to one or more storage endpoints, analysis processes, and actions. Routing makes decisions on what data should go which target and when.
* Analysis is used to run data records through a set of conditions and can produce different output data records. For instance, input telemetry data encoded in one format may return output telemetry [encoded](https://en.wikipedia.org/wiki/Code) in another format.
* Original input data records and analysis output records are typically stored and available to display, and may trigger actions such as emails, instant messages, incident tickets, CRM tasks, device commands, etc.

These processes can be combined in simple graphs, for instance to display raw telemetry received in real time, or more complex graphs executing multiple and advanced tasks, for example updating dashboards, triggering alarms, and starting business integration processes, etc.

For example, the following graph represents a simple scenario in which devices send telemetry records which are stored, and then are immediately displayed on graph on screen for visualization:



The following graph represents another common scenario, in which devices send telemetry, the data is stored and, shortly after analyzing the data to detect anomalies, then trigger actions such as an email, SMS text, instant message, etc.:



IoT architectures can also support multiple systems that can accept and do something with data. For instance, some telemetry storage and/or analysis may occur on premise, within devices and field/edge gateways. In other scenarios, [protocol translations](https://en.wikipedia.org/wiki/Protocol_converter) may be required to connect constrained devices to the cloud. While the resulting graph is more complex, the logical building blocks are the same:

