White paper

Edge based agents for intelligence analysis.

It is vital that intelligence assessments are provided in a timely fashion. The status quo of ingesting data into a central hub not only increases data duplication but also delays the decisions of analysis. This paper will outline an architecture that allows analytics to be pushed to the edge of networks allowing true real time analysis of data.

Fujitsu Australia and Operational Intelligence

Fujitsu Australia's operational intelligence team is leading the way in delivering operational intelligence solutions within Federal and State government agencies. Fujitsu has partnered with a number of major vendors in order to delivery customer requirements, including IBM i2 and Palantir Technologies. Whether it is the initial design, implementation, support or user training, Fujitsu is able to provide you a solution.

Introduction

In 2010 the Internet consisted of 10 billion devices, by 2020 that number is expected to grow to over 50 billion devices. These devices will generate up to 50 times the amount of data that is available to agencies to support their intelligence workflows. The current arguments around structured and unstructured data will turn to discussions about audio and video files and how agencies will be able to store and analyse this information.

The reality is that agencies will not be able to access this additional information using the current intelligence system paradigms. The reliance on hub and spoke designs, which replicates data from the edge of the network and stored on large cloud based systems for analysis will grow exponentially and is not financially viable for the majority of customers. Additionally, this increase in information is likely to slow the analyst's ability to make timely decisions as more data is transferred from the edge of the network.

Edge based analysis overview

Edge based analysis states that analytics are to run as close to the generation of the source data as possible – as close to the *edge* as possible. In this instance, it reduces the requirement to duplicate data and the delay imposed by extracting, transforming and loading the information into other data stores. The following scenario outlines the basic concept:

1. A police intelligence analyst is interested in any violent crime that occurs in a certain suburb.
2. An edge based agent runs on the police Computer-aided dispatch (CAD) system. The analyst is able to submit a flag (analytic) to the agent from their desktop without ICT support – look for violent crimes in this suburb.
3. As dispatchers receive emergency calls and enter the information into the CAD system, the agent detects that a flag has been alerted and sends a response to the analyst in real time.
4. The analyst receives the alert and is able to take appropriate action. At this stage they may choose to ingest the CAD event, call the responding officer, or potentially activate the officer's body worn video (BWV) camera to watch the event in real time (see Fujitsu's BWV offering).

Fujitsu OI – Basic components

Edge based analysis is a design architecture similar to cloud computing and other generic concepts. However, Fujitsu are building a prototype to show the potential benefits of the design. Fujitsu are also interested in hearing from customers that are interested in helping shape the prototype and the capability it provides.

The Fujitsu OI demo will work as a standalone product, or be integrated with existing intelligence tools (both COTS and bespoke systems). However, the first prototype of Fujitsu OI will be developed to integrate with IBM i2 EIA and IBM i2 ANB.

The basic components of the design are:

- Client Dashboard. The client dashboard is used to submit and review alerts to available agents that are connected into the Agent Server. The dashboard is a HTML5 based system that connects to the Agent Server using Web sockets ensuring alerts from agents are received immediately.
- Agent Server. The agent server is responsible for brokering alerts and flags between the agents and the users. It is also capable of managing multi-agent alerts, where you can set a flag to occur only when multiple agents have fired.
- Client Agents. Client agents are generic or customised software that can receive configuration (flag) information for predetermined analytics. For each configuration it maintains a state with the Agent Server – it only sends a state change to the server in order to reduce network traffic.

Client Agent Workflow

Each client agent maintains a number of flags, for each flag it maintains a state with the Agent Server. Therefore, if you have an agent searching for a watchlist of people, individual analysts can submit their own watchlists which creates another flag for that agent. For each watchlist a state of 'flagged' or 'not flagged' is managed by the Agent Server and is able to return the current state to the user.

The Agent server is not aware of the specific analytics that is being run, or how it works. It simply knows if the flag has been triggered and the basic metadata that will be passed to any registered users. The ability to keep this generic allows for a wide range of custom agents to be created to suit any workflow or customer.

Multi Agent Flags

Some analytics will require the state of multiple agents. In order to achieve this, the Agent Server is able to maintain its own client agent. This client agent is configured to flag when one or more client agents are in certain states.

Complex agent workflows are also possible, for example, if you are looking for a person swiping into a building while on leave. To achieve this you could have a configuration submitted at the start of each day that takes the staff currently on leave from the HR system and submits it to the pass system agent.

Example Agent – Mobile Agent

The Mobile agent resides on mobile devices and is capable of accessing any of the technology available on modern devices, such as voice, video, GPS and the accelerometer. Additionally, mobile devices are becoming more integrated with a wide range of communication protocols, such as bluetooth and WiFi allowing connections into BWV, and other sensors such as fitbits. As modern devices are becoming more capable, with more CPU and RAM they are also becoming more capable at running analytics directly on the device and provide a very good opportunity to act as a processing hub for *every* person.

Additionally, the improving speed and coverage of mobile internet connections allows for excellent connectivity between analyst / investigator and individual devices. This combines to allow analysts to submit flags directly to individual devices, and receive real time alerts as they occur.

A potential scenario could be to alert when an officer has a spike in heart rate (fitbit-type device) within the past five minutes and their weapon is drawn (RFID tags). At the same time as alerting any users registered to the flag, commence recording of the situation by the attached BWV. At this stage the users who are alerted to this situation will be able to view BWV live via a remote call to assess the situation or immediately send out support to the officers location (which is sent as GPS metadata as part of the initial alert).

A similar scenario would be possible from a military training perspective, where individual health statistics are monitored during field training exercises. By combining fitbit-type technology to monitor heart rate, blood pressure, sleep patterns etc in order to measure a stress level to predict and therefore reduce the likelihood of injury or heat related illness.

Example Agent – SQL Agent

The SQL agent resides on RDBMS systems and looks for certain events in the databases transaction logs, or is fired from a trigger on certain tables. There are a number of options that would be possible in this scenario, including:

- Tripwire - Configuring the agent to look for changes to certain records. Potentially personnel records, or changes to permissions – such as administration access. The analyst / investigator will be able to submit the search criteria to the agent to flag on (such as individual staff, or wildcard entries).
- New data – Configuring the agent to look for new data. For example, new records in a CAD system. The analyst / investigator will be able to submit the search criteria to the agent to falg on (person of interest list, phone numbers, geo-spatial region).

Example Agent – Custom Agent

A custom agent interfaces with the standard Server Agent API in order to receive configuration from users as well as submit flags as they occur. As it relies on standard and common protocols to pass this information the ability to create a custom agent is relatively trivial. The current technology uses a RestAPI, so the options are endless.

Fujitsu OI

The Fujitsu OI product is currently a prototype that is still under development and will be available for demonstration in late 2015.

Additional information about Fujitsu's BWV is available on request.

Operational Intelligence Services

Fujitsu's Operational Intelligence Team is able to support our customers by using our experience in delivering systems Australia wide, and delivering the following services:

Analysis and Design

- Business Analysis
- Solution Architecture
- System Analysis
- Technical design
- Documentation
- Analyst training
- System testing

System Support

- On-going support of the production system.
- Out of hours support.

Development

- Palantir integration and development.
- IBM i2 integration and development.
- Java / J2EE
- Database design and development.
- Hadoop / NoSQL
- Bespoke development.

As well as, software licencing, consulting, programme and project management.

Contact us

For additional information, please contact
Operational.Intelligence@au.fujitsu.com