White paper
Conducting intelligence analysis at the edge.

It is vital that intelligence assessments are provided in a timely fashion. With the exponential increase in data that is becoming available the traditional technical approaches are struggling to keep up. This paper will discuss conducting analysis at the edge of the network as an approach to handle this increase in data and start achieving real time intelligence analysis.

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.

Data to Decision

The problems faced by modern intelligence analysts, security specialists and investigators include extreme time pressures to respond quickly to a wide range of threats in cyber-crime, terrorism, insider threat and unethical or immoral activities. The ability to respond to these activities quickly, often in real time, can be the difference between achieving the organisational goals or not. Additionally, the ability to conduct analysis in real time will open further workflows that were not possible before.

As we move towards 2020 and current intelligence systems attempt to collect and process up to 50 times the data, the data to decision delay will increase due to a number of issues:

- More data to collect, means longer delays transferring from collection systems into the analytical system.
- Additional data means longer delays in processing the information into the intelligence system, such as index building.
- The increasing variance of data adds to the complexity of the information. This complexity means finding the 'needle in the haystack' is more difficult and places additional workload on the analysts.

Intelligence-led agencies must be able to access and use this information before it becomes stale. Unfortunately, for these agencies, an increasingly complex and slowing system is the only option possible when using the current intelligence system paradigm. Even with significant investment in hardware, the best result possible is to slow the decline.

Edge based analysis

Edge based computing states that any computation should be completed at the edge of the network in order to account for the large amounts of data that is becoming available. Edge based analysis is conducting analysis as close to the edge of the network as possible, or as close to the sensors or generation of the data as possible.

By conducting the analysis at the edge of the network, you can often negate the requirement of copying the data into the analytical tool. The sensors no longer provide raw information for analysis, but conduct the analysis themselves and return the results of the analysis into the analytical tool.

While some analytical workflows require information from more than one source, it is still possible to reduce the time to decision by conducting the analysis as close as possible. Additionally, the analytical tool will be able to conduct 'analysis of analysis', which will provide its own insight into the information.

There are a number of major benefits to edge based analysis including:

- The ability to move from collection to analysis in near real time. The reduction in transfer and processing time can often be significant.

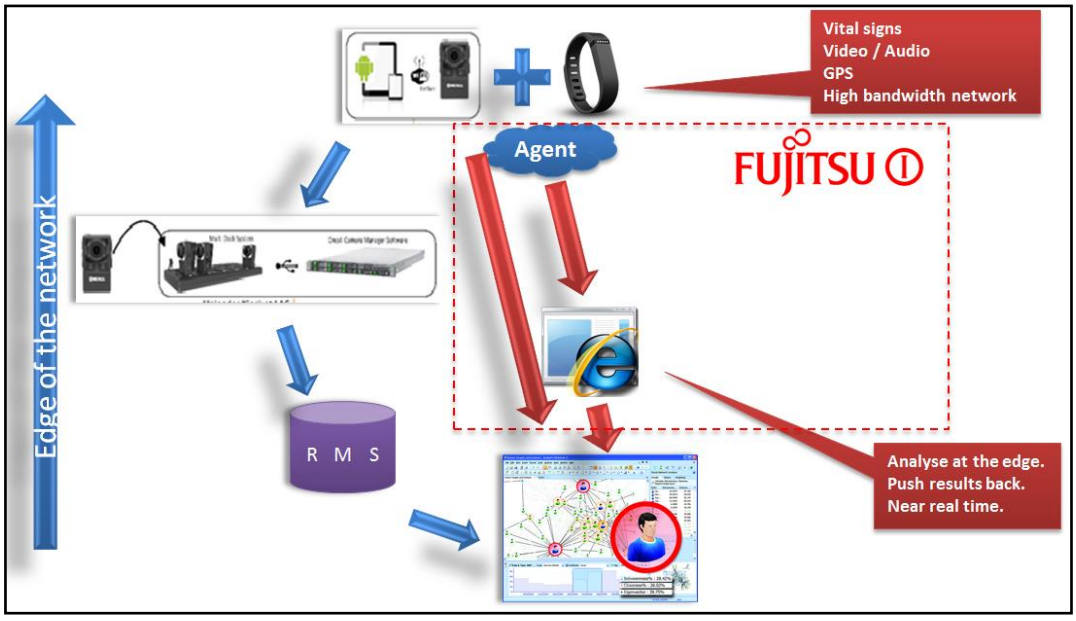

Figure 1 - Body Worn Video example

- Reduced data duplication by only accessing and duplicating information that is required by the organisation's workflow.
- Reduced cost due to reduced data. The reduced cost can be in the form of hardware and licencing costs.

Example – Enhancing Body Worn Video

Figure 1 shows an example of Fujitsu's Body Worn Video (BWV) that is sold into law enforcement agencies. It is capable of providing video capture, live streaming and metadata tagging among many other capabilities. Using a simple workflow, we'll investigate using BWV to automatically check for vehicles of interest as part of an analyst based watch list. In this workflow, the standard intelligence model would be:

- Video is captured in the field.
- Video is uploaded on return to the station (assuming it is capable of recording full time).
- Video is analysed, and licence plate recognition (LPR) is conducted. The results will be synced into the intelligence tool at some later point and compared against the watch list.
- The results of the watch list will trigger an alert to the analyst.

The result of the above workflow is not suitable since if a vehicle is found on the watch list it will likely to be too late to achieve any benefit.

In the edge based analysis paradigm and using Fujitsu's prototype Fujitsu OI (Operational Intelligence) system, the process would be:

- Video is caputured in the field.
- Video is analysed using existing technology available on the officer, such as modern smartphones. It will conduct the LPR on the fly (mobile based LPR) and compare the results to the watchlist (via an API).
- The Fujitsu OI agent on the mobile device will detect any positive results and return this information to the agent server.
- The agent server passes the information to any analyst who is registered to receive updates to the watchlist.

In this example, it is possible that the analyst is alerted to the LPR result within a few seconds and is able to make a timely decision about future actions.

In addition to this information, the BWV and device are capable of collating information available such as GPS location, audio, video, images and from other body worn sensors, such as a fitbits, and return this information to the analyst.

This example could also include facial recognition or any other workflow that uses the BWV device to conduct analysis and send the result back to the intelligence tool.

Fujitsu OI

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

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