Secure Data-Intensive Services with IoT, Fog Computing and LASAGNE

Blake Fetherstonhaugh, Mitchell McCue, Peter Stockwell (blake.fetherstonhaugh, mitchell.mccue, peter.stockwell)@student.adelaide.edu.au
Supervised by Prof. M. Ali Babar, Christos Sioutis, Matthew Thyer, (ali.babar)@adelaide.edu.au, (christos.sioutis, matthew.thyer)@dsto.defence.gov.au
School of Computer Science

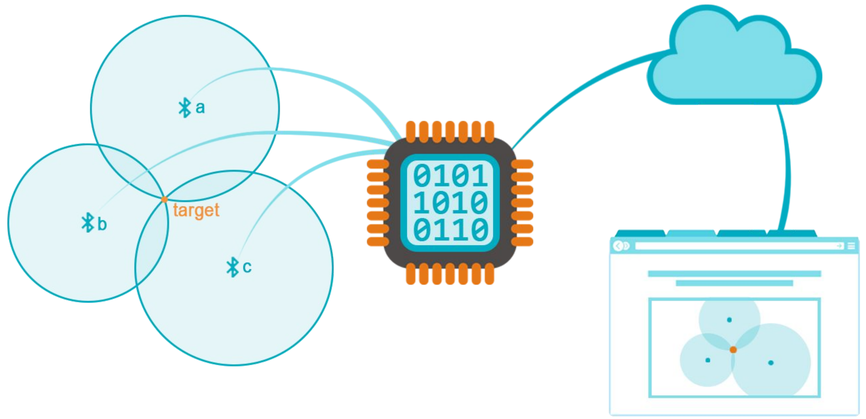
Introduction

- The Internet of Things (IoT) is an assortment of networked devices that contain sensors and actuators to facilitate the collection and exchange of data.
- Vast amount of data generated by IoT devices is time sensitive and requires significant network bandwidth to transport to the Cloud.
- Fog Computing seeks to alleviate this reliance on the network, where data is processed on the edge of a local network with low latency, with computations published to the Cloud [1].
- Layered Approach to Service Architectures for a Generic Networked Environment (LASAGNE) facilitates easy deployment of service components [3][4]. By employing a secure, data-centric publish-subscribe communication approach, the main goal of this project is to experiment using services implemented in LASAGNE to determine how employing a Fog Computing approach can improve performance of networked applications.

Objectives

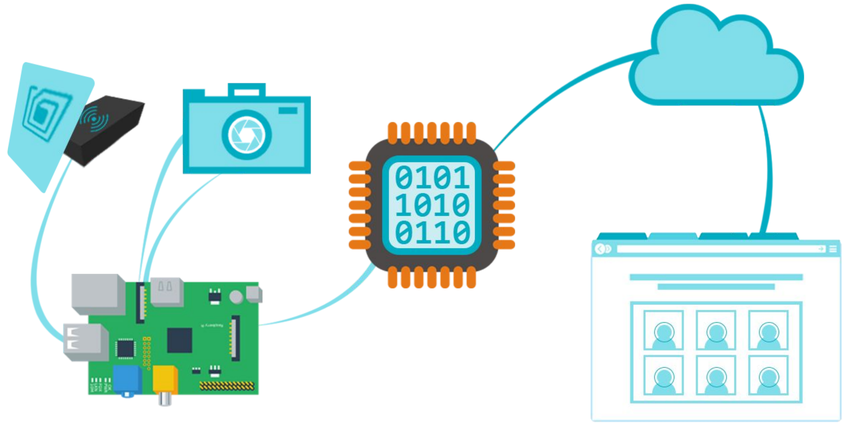
- Based on examples discussed in the Amazon Web Services (AWS) Innovate conference [2], design and develop two usage scenarios using LASAGNE services: a Bluetooth device trilateration application and an RFID-triggered face detecting camera application, which use multiple Raspberry Pi's as the IoT sensors.
- Design the usage scenarios with an emphasis on the security of the transmitted data, providing message confidentiality, authentication, integrity and protection against replay attacks.
- Leverage LASAGNE's simple redeployment facilities by changing the location of service component deployment to perform experiments.
- Experiment with the usage scenarios contrasting a Fog vs. Cloud computing approach, to determine if and how each application may benefit from using a Fog approach when internet bandwidth is reduced and latency is increased.

Experimental Studies



Study 1: Beaconisis

- Multiple sensors (or beacons) each detect a target device via Bluetooth signal strength readings and deliver these to a server for filtering of noise and conversion to distances, for accurately computing the target device's location.
- Using trilateration, the processing service uses the locations of each sensor and its distance reading from the target, in order to compute the relative position of the target.
- Performed in real-time, the computations are delivered to a web server for visualising where each sensor and the target device are located.
- Deploying the service which computes the trilateration result on the Fog relieves the Cloud of computation, reducing bandwidth consumption outside of the network.



Study 2: Face Detection with RFID

- An RFID reader attached to a Raspberry Pi triggers the Pi's camera to take a photo when an RFID tag is in range.
- The Raspberry Pi securely publishes the picture to a subscribing Processing Service. The Processing Service uses the OpenCV library to detect faces and draws a circle around them.
- The Processing Service securely publishes the result to a subscribing Cloud Service, which can then displays the resulting image in a web application.
- Deploying the Processing Service which detects the faces within an image on the Fog reduces the load on the Cloud and the outer network.

What is LASAGNE?

- The LASAGNE framework is a "Layered Approach to Service Architectures for a Generic Networked Environment" and has been developed by the Defence, Science and Technology (DST) group. The framework is suited for efficient, scalable, Internet of Things (IoT) style applications written in C++ as reusable services.
- Features platform, operating system and vendor middleware independence (leveraging the ability to create portable applications), modularity, point-to-point and data-centric publish-subscribe communication models, and high performance intra/inter-process communication.
- Built on the open-source ACE framework which provides a large set of classes implemented according to the Pattern Oriented Software Architecture (POSA) approach. Point-to-point and object centric communication (including a discovery service) is provided by The ACE Object Request Broker (TAO).
- Supports four Data Distribution Service (DDS) implementations with middleware independent access through a meta-programming layer.

Security

- OpenDDS does not currently support security, as such we have implemented our own secure communication. Our implementation of security has focused on securing the application layer 'payload' itself.
- The payload is encrypted with AES-128 encryption using CBC block cipher mode, provided by the Crypto++ library, to ensure data is kept confidential.
- Hash-based Message Authentication Code (HMAC) is performed on the payload using SHA-256 to ensure the message has originated from an authenticated source and its integrity is maintained.
- A unique identifier in each topic is checked to protect against replay attacks.

Acknowledgements

We would like to thank Christos Sioutis from Defence Science Technology (DST) Group for his assistance with the LASAGNE framework, and to Matthew Thyer from DST Group for being a tremendous source of knowledge and guidance throughout the entire project. We also appreciate the feedback given by Dr. Christoph Treude.

References

[1] https://www.cisco.com/c/dam/en_us/solutions/trends/iot/docs/computing-overview.pdf
[2] https://aws.amazon.com/events/aws-innovate/
[3] LASAGNE Architecture Overview v1.1.2gh, Defence Science Technology (DST) Group
[4] LASAGNE Cookbook v1.1.2gh, Defence Science Technology (DST) Group