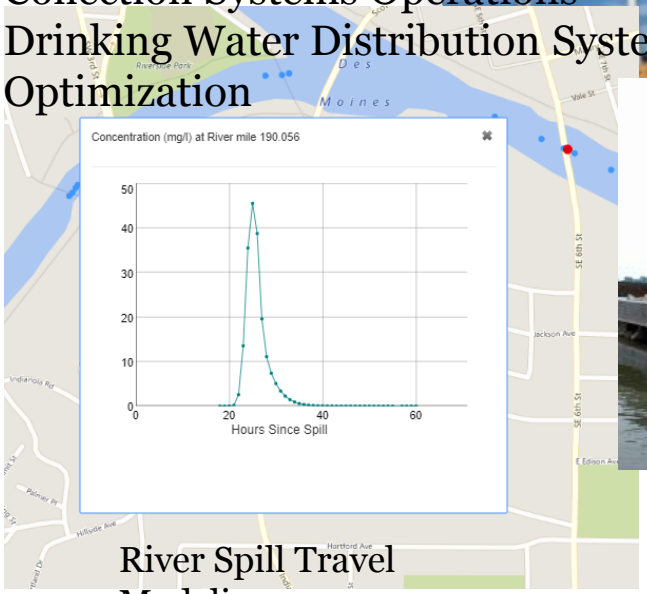
Smart Replicable Solutions to Water-Energy Nexus Challenges

gqc HydroTrek

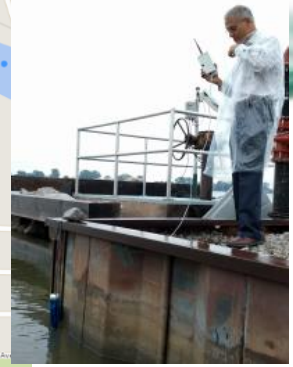
cleveland water alliance

Groundwater Monitoring

Internet of Things (IoT) Sensor Networks
Artificial Intelligence for Water Quality Predictions
Pumping Energy Optimization with Smart Modeling
Smart Leak Detection
Big Data and Cloud-based Analytics
Collection Systems Operations
Drinking Water Distribution Systems Optimization



River Spill Travel Modeling



Harmful Algal Bloom Monitoring

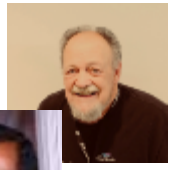
A secure solution for monitoring harmful algal blooms

Sudhir Kshirsagar, Jacob Specht, Vijay Raman, Murali Singamsetty, Steve Mylroie

June 20, 2018

Our Roles

- **Dr. Sudhir Kshirsagar (Architect), Global Quality Corp.**
- **Jacob Specht (Developer), Global Quality Corp.**
- **Dr. Steve Mylroie, (Embedded Systems) Roietronics**
- **Murali Singamsetty (SDN Architect) Sayantek.com**
- **Vijay Raman (SDN Strategy) Sayantek.com**

Connection – Distributed Monitoring Vision

- Monitoring stations
- Telemetry data local to each region
- Analytics at each monitoring station
- Aggregation of events at a central place (Cloud)
- Monitoring of inputs to the Lake

Detection, Connection, Analysis, Interoperability and Scalability

- Developed an affordable battery-powered IoT Nitrate sensor node with low power (LP) long range (LORA) wide area network (WAN) low-cost telemetry functionality
- Implemented Resilient Fog computing -Software Defined Networking (SDN) and Software Defined Applications (SDA) and event detection (EDX)- on Edge gateways (gateways that capture messages from the IoT nodes) with eRED/Node-RED
- Transmitted IoT Sensor messages to a scalable resilient Cloud-based IoT Hub using MQTT and AMQP
- Implemented Software Defined (SD) Cloud-based Orchestration and Management of the WAN with eRED/Node-RED
- Created Cloud-based REST web services to capture real-time JSON data from our IoT Hub and from existing monitoring networks (GLOS and USGS) in Node-RED
- Implemented Cloud-based storage and visualization of Lake Erie monitoring data
- Implemented Lake Erie specific Cloud-based analytics and runoff modeling

Technologies Used

- Vernier Nitrate ISE
- MultiTech LoRaWAN modules and gateway
- mbed RTOS and C++
- Multi Tech Condut LoRaWAN gateway
- Sayantek eRED (Node-RED based)
- Node.js
- Amazon AWS
- Azure IoT Hub and Azure
- HydroTrek EDX (Event Detection)
- Misc. (PVC plumbing, cable glands, IP-67 enclosures, water bottles….)

Security and Resilience

- The network resilience is achieved through the management of the gateways through the eRED client on the gateways that is securely managed by per-tenant Cloud-based orchestrators
- Cybersecurity is achieved through a combination of the proprietary LoRaWAN protocol combined with Secure Sockets Layer (SSL)
- The firmware implemented on the microcontroller chip is proprietary and cybersecure
- Vandalism related threats can be addressed through addition of geo-tracking to the modular architecture
- The single sensor failure scenarios can be countered by deploying multiple sensors of the same type because the total cost of ownership (TCO) is very low
- The gateway failure scenarios can be similarly addressed through the provisioning of standby units

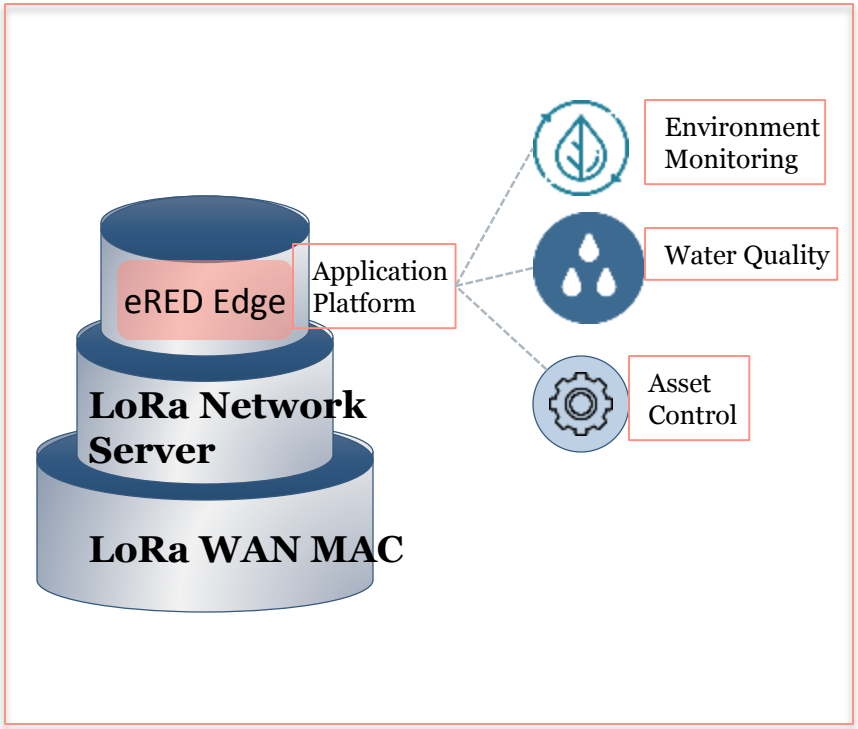
- **Scalablility**
  - Achieved through the management of the gateways through the eRED client on the gateways that is securely managed by per-tenant Cloud-based orchestrators
  - Deployment of thousands of nodes that require a handful of gateways
  - Cloud-based storage and analytics
  - Cloud-based run-off modeling

Sensor Node & Node to Gateway Security

1. Sensor Node
    1. Primary Physical
    2. Software embed un-modifirable firmware
    3. Limited Access from Cloud
2. Node to Gateway Transfer
    1. LoraWan Security Designed into Standard
        1. Packet Encryption
        2. Device Authentication
        3. Small Packets
        4. Spread Spectrum
        5. Multiple Channels
    2. Future Secure Support for Secure OTA software updates
    3. Public vs Private Network
    4. FCC Certification of Firmware stacks

SDA LoRaWAN Gateway

- eRED Edge instance on each LoRa gateway for cloud integration
  - Support for common messaging protocols MQTT, AMQP, more
- Native application platform
- Centralized managing of device provisioning and application configuration
  - Remote debug of headless devices



Stack at LoRa WAN Gateway

Gateway Security (with eRED platform)

Comprehensive framework consisting of:

Editor & Admin API: username/password based, pluggable OAuth/OpenID or custom authentication schemes

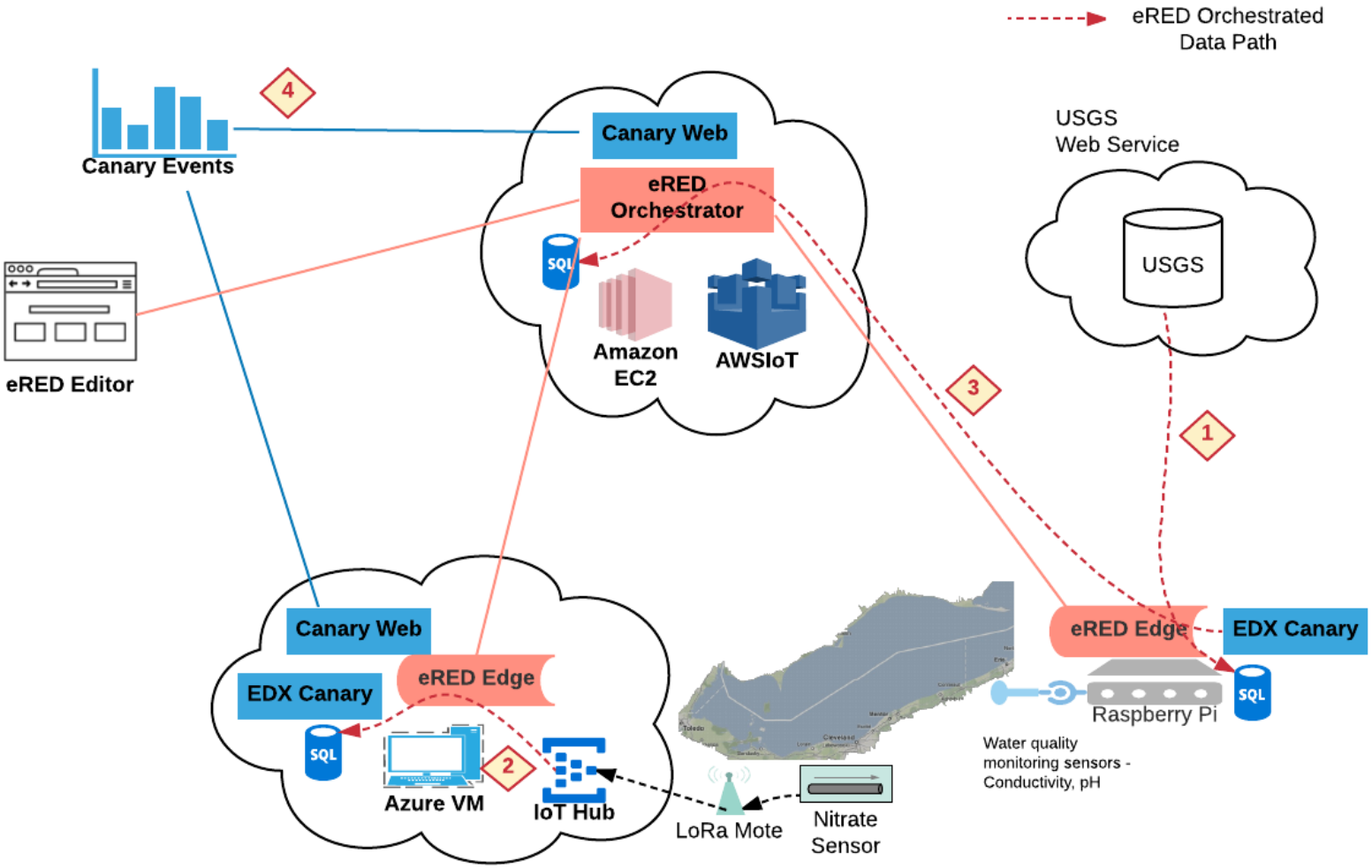
Controller & Gateway communications: HTTPS with TLS. Cert based mutual authentication.

Distributed flow messaging: ZMTP 3.0 with CurveZMQ forward security and peer authentication. Curve25519 256-bit keys with ~3072-bit RSA strength

Flow credentials storage: Encrypted by BCRYPT algorithm with a key size of 256 bits.

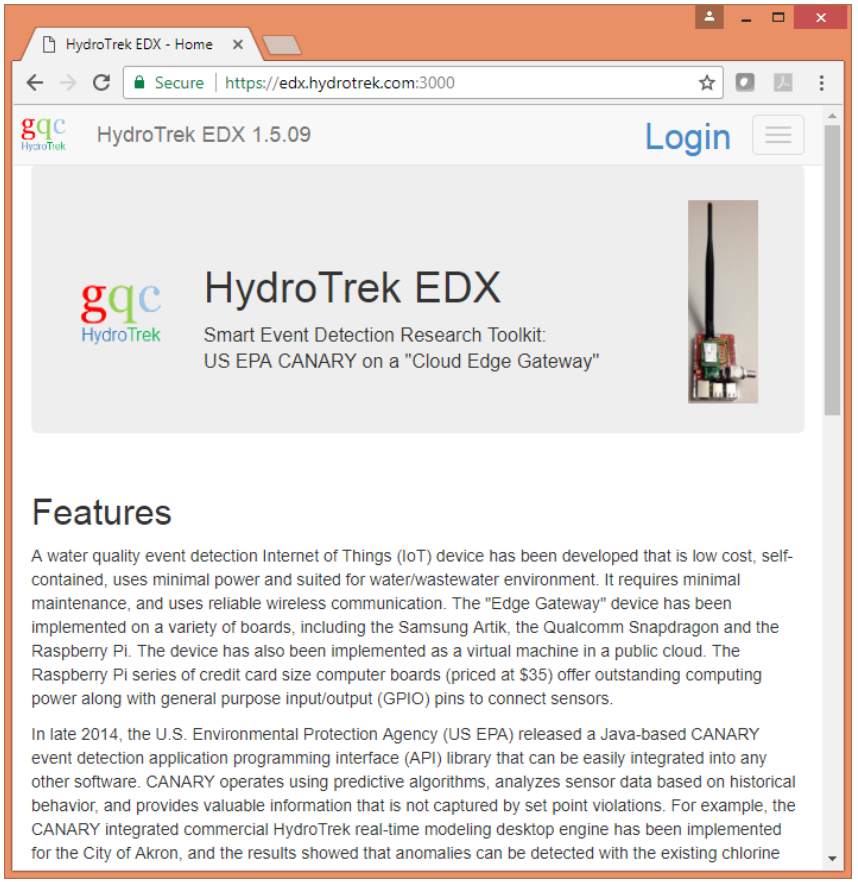
Provisioning & key management: provisioning phase security with factory keys. Registration & periodic check-ins to enforce key rotation & refresh. Instance specific key & certs used to limit exposure. Policy based dynamic key rotation scheme.

Complete Solution Implementation



Analysis: Anomaly Detection with Machine Learning

- US EPA Java Runtime
- HydroTrek Event Detection Extension
- HydroTrek Node.js based secure web server
- Azure Machine Learning for Analytic
- Multiplatform: Runs on Gateways and VM's



Q&A

Useful URLS

Robert Miller WMR Labs Biggest Risk Key compromise
https://labs.mwrinfosecurity.com/assets/BlogFiles/mwri-LoRa-security-guide-1.2-2016-03-22.pdf

http://www.sayantek.com/2018/02/sayantek-wins-best-network-technology-award-at-internet-of-h2o/

https://docs.microsoft.com/en-us/azure/iot-hub/iot-hub-devguide-security

http://www.hydrotreck.com

https://www.multitech.com/brands/multiconnect-mdot