**Cyber-Chemical Sensor Cloud Information System: A unique proposal to manage IoT risks based on NISTIR 7951**

**#1 Problem Statement/Use Case:**

*Chemical Sectors* have plants that produce various types of substances. Obviously critical to modern infrastructure but can be harmful to humans and the environment. These are required in real-time by other sectors too, as they are intertwined with healthcare, manufacturing & agriculture sectors, etc.

Despite being a Critical sector, accidents are not uncommon and human interventions are required for managing inventories, supply chains and monitoring of the plant equipment. Chemicals such as "vinyl chloride, hydrogen iodide and methyl acetate" are harmful and can cause burns and toxicity. Hazardous consequences on organs, directly or indirectly by polluting the environment, water or air and cause degradation of soil quality.

**a. Proposed solution:** For our use case of Chemical manufacturing plants. In the last couple of years quite a few accidents have been in the news. Due to human errors or due to lack of inter device communications. Which inspired us to give an IoT overhaul to the chemical sector and reduce the risk of such accidents by making the Chemical Sector a robust IoT environment (powered by cloud computing, automation & artificial intelligence).

**Executive Summary:** We are upgrading these plants to Cyber-Chemical Sensor Cloud Information Systems (CCSCIS), to be an IoT environment. This makes the Plants robust, cost efficient, and operationally efficient. IoT Transducers provide scalability to monitor quality (e.g. prevent hazardous mix-up of Chemicals) and label reading using Computer Vision and combine it with pH, temperature sensing to prevent fire accidents. The environment is integrated to have multiple IoT Fogs with distributed processing, it prevents accidents by alerting if a worker enters a restricted/quarantined area. Or if a worker is operating an unauthorized machinery or without training. This is done using RFID & Geolocation tags in real-time by combining sensory data from pressure plates, cameras, etc. Defects are detected using ultrasonic sensors (to detect volume-levels for auto-cutoff to prevent spillover), optical monitoring of vats & pipes to detect cracks and provide real-time solution such as Laser welding the chinks.

The cloud component comes into picture for advanced data analysis, log storage, simulation, and AI-based prediction to thwart incidents. Automated inventory and supply chain management (in real time) - by keeping locations tracked of samples/beakers/boxes, etc. with help of QR codes, barcodes, and AR (augmented reality) labels. Coupled with communication on-site to cloud from when in transit (maps data, geolocation, etc.).

**System Requirements:**

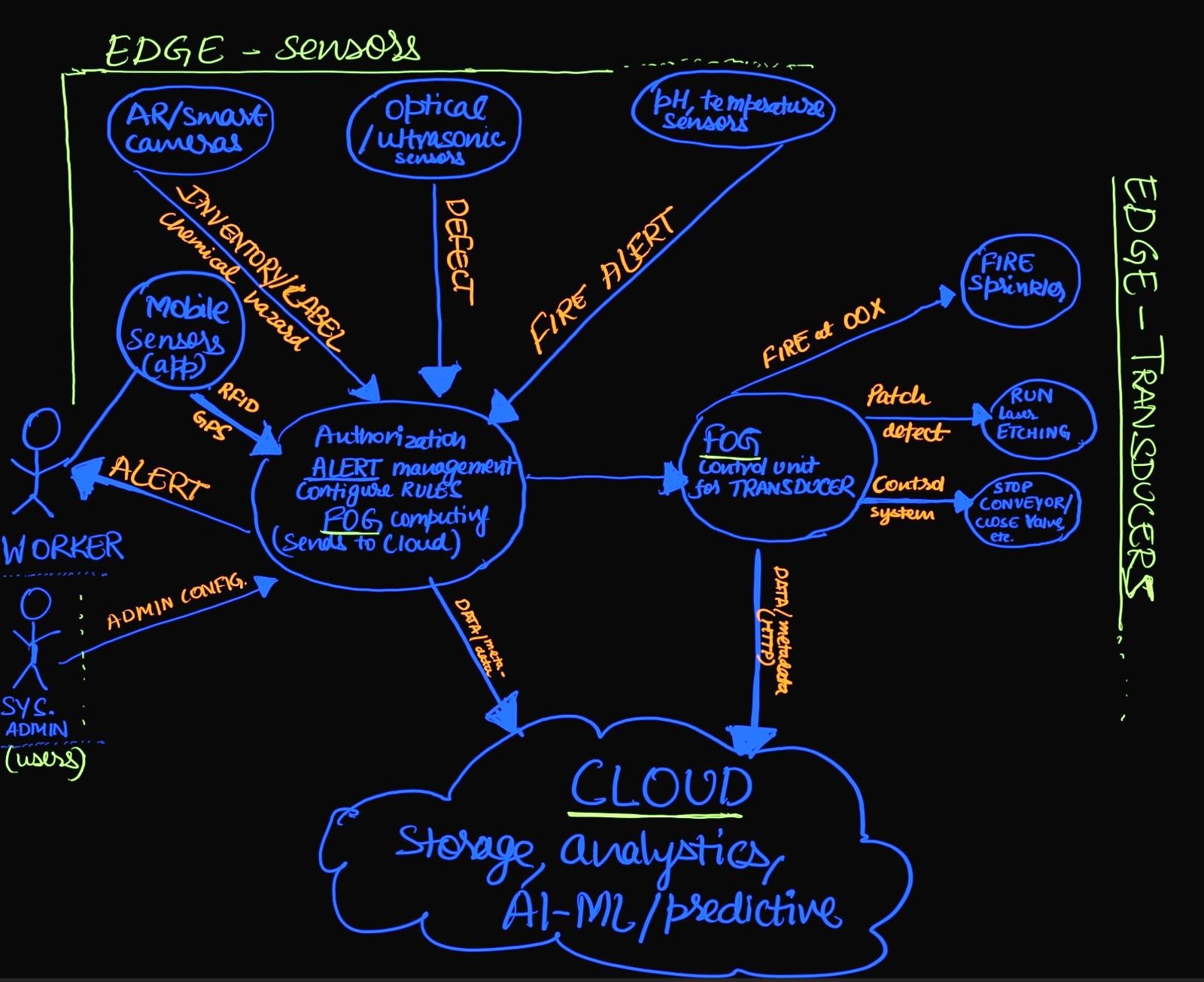
1. **Advanced Sensors Network and Industrial Control Systems:** Comprehensive sensors, including infrared thermometers, pH level sensors, and pressure sensors, optical sensors, ultrasonic sensors; for volume control and laser/infrared monitoring systems for detecting defects (e.g. cracks in pipes). RFID and GPS sensors for location tracking and securing authorization level that supports real time operation.
2. **Augmented Reality (AR) and Smart Camera Integration:** Deploy AR-equipped cameras for label reading and hazardous mix-up detection. These cameras should be capable of text extraction from various labels, etc.
3. **Network Firewalls and Security Measures:** Network firewalls, with access points, are required to protect the IoT environment from unauthorized access by external entities. Standardized physical security measures.
4. **Comprehensive Communication Protocols:** For covering various IoT systems within the IoT environment.

We need 4G/5G network, Ipv6, high-speed WiFi, wireless internet with CoAP, HTTP, MQTT, Ethernet/IP protocol.

1. **Cloud based data analysis:** A truly next-gen feature which will store and process images, inventory metadata

(e.g. Compound NaOH+HCl = Dangerous/explosive) and provide Intelligent AI-based analysis for predicting incidents. This can be achieved after collecting data and itemizing the entire process.

**#2 Use-Case Diagram & Description:** Figure 1 - Cyber-Chemical Sensor Cloud Information System



**Description:** Several components of this IoT environment function to prevent incidents, recover from chemical hazards, ensure safety of humans and the entire Chemical Plant. Key Components include:-

1. **Edge Sensors:** Includes AR based smart cameras, optical/ultrasonic, pH and thermal sensors.The goal is to record information by interacting with the physical world like pipes, vats, etc. for gas leak detection, etc.
2. **Edge Transducers:** Includes fire sprinklers, laser etchers & valves, etc. They interact with the Fog Computing units and perform actions often automatically to patch defects, extinguish fire, prevent incidents.
3. **Workers and System Administrators:** The human component in this design, they sit and interact with the edge and fog using Human computer interfaces and/or sensors. The workers are equipped with RFID, GPS based applications in their smartphones and/or ID cards.
4. **Fog Computing Units:** Critical tohave for low-latency operations on the plant. There is distribution of these units based on their specific purpose (alerting or controlling). For e.g. they process information & send alerts to workers software applications, and control critical industrial systems such as Laser etchers and conveyor belts.
5. **Cloud:** A key component for long-term data storage for analytics and AI-ML predictions. Data needs is sent the over internet. Information from clouds can be sent back to the system admins and fog.

**#3 IoT Technologies (Edge Devices, Comms, Fog, Cloud):**

**a.** **Four Sensors and Actuators interacting with the physical world:**

1. **Sensor – computer vision cameras** *(e.g. Allied Vision’s Alvium 1800 U-120c):* They capture high-resolution images and send it to dedicate Fog Computers for processing, including any locally processed metadata (e.g. Text labels). Using machine vision technologies provides real-time tracking and depth-based detections in 3Dimensional space. **Processing:** MEDIUM, **Storage:** MEDIUM, **Networking:** HIGH, **Energy:** LOW.
2. **Sensor - thermal imaging and temperature** *(e.g.**FLIR A65/A35):* Can capture very small temperature differences (~50 mK difference). Require uploading to Fog computers detect cavities and fractures in pipes of steel, glass, etc. **Processing:** LOW, **Storage:** LOW, **Networking:** HIGH, **Energy:** LOW.
3. **Actuator - Laser powered mold repair machines** *(e.g. by 301/302 by Han’s Lasers):* Modularity is essential to automate patching of small cracks and crevices. Therefore, Fog Processing will be necessary to target, set the laser frequency, etc. **Processing:** MEDIUM, **Storage:** LOW, **Netowrking:** LOW, **Energy:** HIGH.
4. **Actuators – Smart Valves** *(e.g. Microfluidic smart valves by EveFlow):* Scalable and micro-controllable valves. For high-precision and “chemical compatibility”. **Processing:** MED, **Storage:** LOW, **Networking:** LOW, **Energy:** LOW.
5. **Communications:** A Chemical Plant will have floors, basements, andthick walls.People on site require *4G* for higher penetration.Cameras will have *power-over-USB* connectivity to the Fog for high-bandwidth, alternatively they can use Wi-Fi where communication needs to be wireless. *EtherNet/IP* will be used for “Laser Actuators” since it has security built-in, and we need the High-powered Lasers to be secure.

For valves using “Microfluidic” actuators we will use *Zigbee* protocol stack (for edge-to-edge & to fog connection) it is efficient for lower-powered devices (battery operated) and has low-latency for quick actuation of valves. Various other types of sensors (like pressure, pH sensors, etc.) will communicate using *“MQTT”* the broker will be the Mobile-App (of Fog where alerts go through the Fog).

**Network:** Ipv6 is scalable and can be deployed en-masse. Useful where IoT environments have plethora of devices.

**Transport:** TCP (reliable for transmitting data for storage & good for critical communication) and UDP (loweroverhead good for real-time operation of devices susceptible to latency).

**Application:** HTTP (for Fog to Cloud data upload) and Ethernet/IP (e.g. Laser-Devices). MQTT for constrained IoT sensors, devices that do Machine-to-Machine communication. SSH for secure logins to computers by admins.

1. **Fog Computing:** Fog computing is critical to our design choice. Since it minimizes allowing quick actions in situations such as gas leaks, fire, harmful or incorrect chemical mixtures, etc. There are multiple Fog Computing nodes for specific functions such as Alert nodes and Fog Controller nodes.

The system administrators will also interface with the Fog nodes to configure policies for smart devices manually, read monitoring logs, or provide special authorization to a worker.

1. **Cloud Computing and Storage:** We will be using Cloud Computing and storing data for analytics, inventory management, AI, and compliance.More specifically,the system will be integrated with Azure Cloud which itself can be seamlessly integrated with services like “Azure IoT analytics” (e.g. Azure Stream Analytics for real-time data streaming from sensors to cloud)” and “Azure machine learning services” (e.g. predicting failures and chemical incidents by learning from the full-scale IoT environment at every level from Items in inventory, to centrifuges, silos, or in vats being transported).

**#4: Risk, mitigation, and implementation challenges:**

**Risks:** We have identified the following risks when designing a Cyber-Chemical Cloud Sensor Information Systems

1. **At IoT edge:** Devices at edge that are not secured from interference both physically and virtually (using cyberattacks) can fail.In the worst case,there could be compromises of Chemical Plants critical infrastructure leading to operational hazards and environmental incidents. Mitigation can be simply blocking access to critical infrastructure at the Firewall level, allowing only required ports and IPs and restricting every unnecessary port. Alternatively, check & consider proprietary security like “MS defender for IoT” which supports a lot of protocols.
2. **In network communication:** At network level there can be *Co-Channel Interference.* For devices communicating over WiFi there can be frequency-overlap and it can cause co-channel interference. There can be some measures taken to mitigate these, for example the use of 5GHZ frequency band with dynamic channel allocation and filtering. The 2.5GHZ band is more prone to such interferences so it makes sense to reserve it only for devices that intend to use WiFi over longer ranges.
3. **In applications:** Predominantly risk in applications comes from attackers looking to steal information by listening to unsecure ports over the internet. HTTPS (HTTP over TLS1.3) can be used to mitigate this as all the data going to the cloud will be secured using encryption. Furthermore, all applications can have web-based vulnerabilities ports over HTTP/S can be secured using WAF to reduce the risk of top OWASP attacks.

**Implementation Challenges:**

1. **Skilled and Trained Workers:** The cyber-chemical plant requires more skilled than usual workers as there is implementation of interdisciplinary technologies. While automation would reduce the number of incidents, troubleshooting of small systems requires precision and operation of comprehensive hardware on site.
2. **Interdependency to Telecom sector:** It can be difficult finding high-speed WiFi providers or having large 4G,

5G cellular network presence in rural areas. Therefore, it is necessary to consider this as a design challenge whenever implementing this system. Particularly in rural areas.

1. **Extensive Testing and QA/QC:** No implementation can be considered complete without proper testing. Hence, it is important to have a robust Quality assurance and control plan along with regular testing of all physical equipment. Periodic audits, compliance, and adherence to NIST standards for Cyber chemical sector can help.

**References:**

1. **Smart IoT in Chemicals in Industry** [**-** https://www.intuz.com/blog/smart-manufacturing-iot-in-chemical-industry](https://www.intuz.com/blog/smart-manufacturing-iot-in-chemical-industry)
2. **Casualties due to a Chemical leak -**<https://www.washingtonpost.com/nation/2021/07/28/texas-chemical-leak/>
3. **Massive fire at Shepherd chemical plant - A Forklift accident -**

https://www.houstonpublicmedia.org/articles/news/local/2023/11/08/468931/chemical-plant-explosionshepherd-san-jacinto-county/

1. **Setting up a machine vision camera for object detection** [**-** https://medium.com/@smart-designtechology/setting-up-a-machine-vision-camera-for-image-inference-5134bdc30a5b](https://medium.com/@smart-design-techology/setting-up-a-machine-vision-camera-for-image-inference-5134bdc30a5b)
2. **Infrared Thermal Imaging-Based Crack Detection**[**:** https://ieeexplore.ieee.org/document/8928570](https://ieeexplore.ieee.org/document/8928570)
3. **Cavity Detection in Pipes Using Infrared Thermography** [- https://www.mdpi.com/2076-3417/11/9/4051](https://www.mdpi.com/2076-3417/11/9/4051)
4. **Ethernet/IP has authentication, security, scalability over Modbus**https://www.gridconnect.com/blogs/news/modbus-tcp-vs-ethernet-ip-an-engineers-decision-making-guide
5. **Azure IoT analytics and Azure Machine Learning** [- https://azure.microsoft.com/en-us/products/machinelearning](https://azure.microsoft.com/en-us/products/machine-learning)