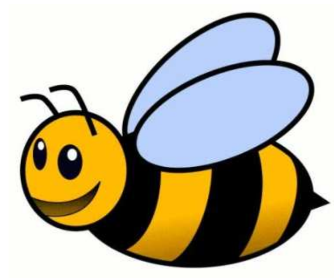
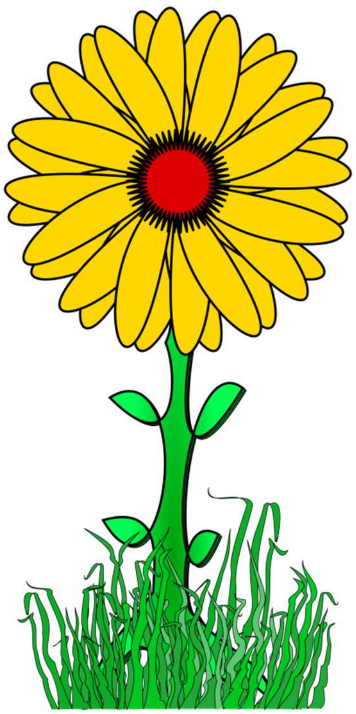




I^3

Intelligent IOT Integrator (I^3)
University of Southern California
A joint project: Marshall and Viterbi

Scenario Driven Requirements

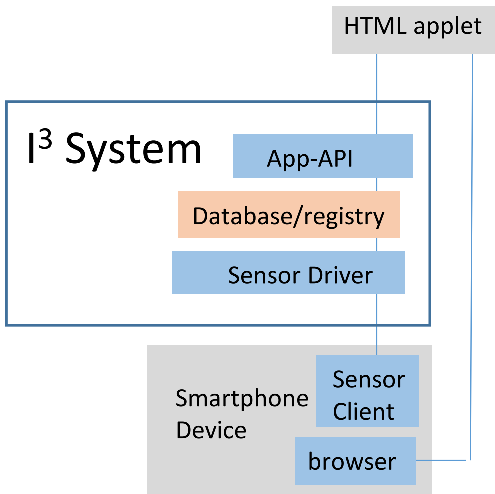
Jan 14 2017

Bhaskar Krishnamachari (bkrishna@usc.edu)
Cyrus Shahabi (shahabi@usc.edu)
Jerry Power (jerry.power@marshall.usc.edu)
Seon Ho Kim (seonkim@usc.edu)

1. **I^3 Usage Scenarios**

1.1 Scenario: Smartphone

Smartphones are interesting devices in that they can serve two purposes in an I^3 system. Because a user can access the internet from the smartphone, the smartphone can be used to provide access to an I^3 application which provides intelligent access to the I^3 database/registry. The smartphone can also act as an independent sensor in the I^3 environment and support a sensor client that reports status information to the database/registry. For example, a smartphone could report the user's location on a periodic basis (e.g. every 15 minutes) or when polled from the I^3 smartphone sensor driver.



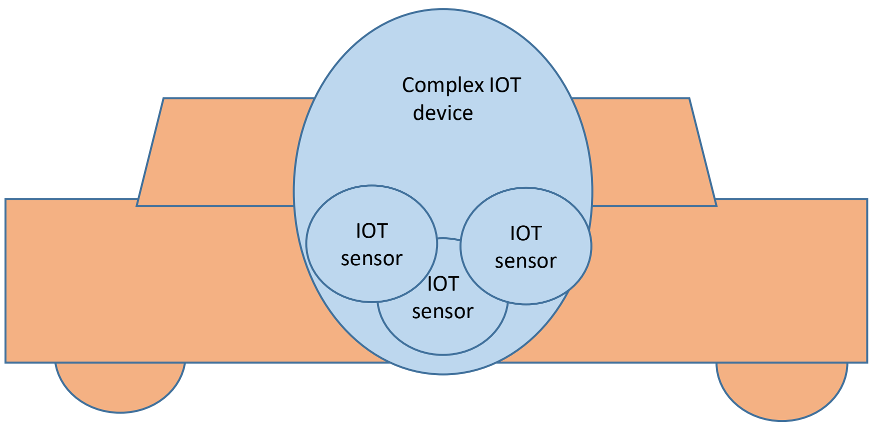
When a user joins the I^3 community, they will download a single I^3 software application. This application will report all smartphone sensor data to the I^3 registry/database. The smartphone application will report to the I^3 software driver based on a configurable schedule or whenever the driver module asks for an update. [Sidebar: The smartphone application for the iPhone and for the android systems will be different].

While it is possible for the user to load a user-centric application on their smartphone that directly interacts with that smartphone's sensor data, this practice should be discouraged for applications that are within the I^3 sphere of influence as it sidesteps the I^3 security and usage monitoring features. As an example, assume a person has a number of wearable IOT devices that use the person's smartphone as a Bluetooth hub. If the smartphone hubbing software forwards the sensor data to the I^3 database/registry, the application is a participating member in the I^3 system and the user would interact with their local sensors via the I^3 database/registry. If the smartphone software directly interacts with the sensors, not going through the I^3 database/registry, the application is operating outside the I^3 system.

Smartphones can also be loaded with software that uses the smartphone as a sensor hub. For example, smartphone smartphone software might poll the user's car via Bluetooth when the smartphone is in the vicinity of the car and report the car's sensor data to the I^3 a driver module on behalf of the car. This scenario might be extremely useful for cars that do not support an autonomous connection to the internet. In this situation, the I^3 registry/database would maintain a log and status flag indicating if the car is or is not visible to the I^3 system (connectivity being dependent on whether the owner is in the Bluetooth vicinity of the car).

As an example, consider that there are applications that make it easier for smartphones to post UGV (User generated Video) to facebook and YouTube. This software could be modified so that when media is uploaded from the smartphone to the cloud based application, the same software can be used to geotag the software and at the same time it can report sensor status information to the I^3 system). The status report that goes from the smatrphone to the I^3 system can include location status information along with a URL reference pointing the uploaded cloud application. An application accessing the I^3 system would then be alerted to know new UGV was uploaded along with the time/date of the video creation.

Complex IOT systems, such as cars have IOT controllers in the car that manage and make use of a network of IOT sensors within the car. The point of egress for data to and from the car is the IOT controller. For the purposes of the I^3 system, the IOT controller is considered the IOT device and the individual sensors within the car are consider a part of the controller but not directly visible to The I^3 system.



1.2 Scenario: Commercial Centers

The I^3 system might be deployed and operated by a retail mall, shopping center, or a mixed use building in order to make the space more attractive to tenants. Tenants would benefit from the I^3 system through increased security and improved tracking of customers/tenants. Malls and shopping centers can be considered cooperative ventures among multiple merchants in that groups of stores work together to share store operating costs. This same concept of sharing of costs can be extended to the IOT space where a mall might track shopper presence in the mall and, through the use of IOT, alert customers of specials in nearby stores or alert stores of the presence of a highlighted shopper in their vicinity.

Stores have two primary use of IOT. One is to improve the store operation internal to the store and the other is to increase customer awareness about the store's offerings. Much of targeted customer purchasing is moving on line however the physical store still has advantages for browsing based purchasing and these establishments need to embrace this altered mission of their customers. Successful companies know that product placement is one of the keys to optimizing sales. Therefore it is important to know where, in a particular store, different customers spend their time. Sales are increased if the merchant can increase the convenience for the customer by placing desirable products in easy reach. If the store is optimized for the customer internally, the next challenge for the merchant it is to make sure the customers visit the store as frequently as practical. This means understanding when customers are in the vicinity who may have interest in a product or special that is available at the store.

Beacons might be deployed in such circumstances. Beacons are non-networked devices that serve to wake up an application residing on a cellphone when they are close to the beacon. The application has the intelligence that it can be programmed to transmit location and other detected sensor data (such as the identification of the beacon that triggered the activation) to the I^3 registry/database.

When there is no I^3 system the smartphone must be loaded with beacon detectors and registry reporting software for each application the smartphone owner wishes to use. Where there is an I^3 system, a single alerting system notifies the registry/database and the I^3 system manages notification messages to the application of interest. Since each application may expect special messages, it should be possible for the I^3 system to support application specific driver modules that can create and respond to application specific alerts. By moving application multiplex point to the I^3 registry/database and away from the smartphone, the message load on the communication network is reduced thereby improving LAN performance and possibly saving the smartphone owner usage fees.

As an example of this scenario, consider the case of the retail Lemonade restaurant. Lemonade could deploy people counters at the door to its restaurant which allow them to monitor customer flow and could also give customers advance warning when lines become long. Under the I^3 system, they would have the choice to keep the counters private (proprietary) or they can sell the data from these sensors to offset sensor deployment costs. Other stores in the vicinity may be interested in purchasing the data so they can determine if their area is experiencing a local customer slump or surge. These same counters could be linked to the mall environmental systems so temperatures can be kept comfortable and to mall security.

Commercial centers might include hotels. As guests arrive at a hotel for a pending conference, sensors detect their presence in the lobby and report it to the I^3 system. An application associates the guests arrival with a pending reservation, alerts housekeeping, and sends the guest a code to unlock an available room. An updated conference schedule is delivered to the guest with welcome refreshment by an autonomous-automated porter that offers to make dinner reservations at a number of local restaurants.

Commercial centers are most commonly thought of as a collection of independent stores. Consumers move through stores, select the merchandise they want, and check out when they leave each store. Under the I^3 system it would be possible to tag merchandise with a price and merchant ID so a single store can support multiple merchants with a seamless customer experience. At checkout, the purchased product data would be matched to the proper merchant and their account would be properly credited. A merchant would no longer have to rent a specific store, they could rent (or bid on) shelf inventory which allows them the flexibility to dynamically adjust their presence based on available inventory.

1.3 Scenario: Smart factory

In today's world, many factory operations are already automated. These factory systems (SCATA) should be integrated into the I^3 system. The I^3 system takes the level of automation in today's factories to another level by 1) integration supply-chain management concepts into the automated factory, 2) integration of service departments (and their test systems, vehicles, carts, etc) into the system, 3) integration of factory alarm and environment systems, and 4) integration of office worker support systems into one complete factory support system.

Different manufacturing facilities are connected together through multiple supply chain networks (trains, trucks, ships, planes) allowing value to be added to raw materials as the product moves through the supply/delivery network. Connecting these systems together with the automated factory through the I^3 system forms a more complete production system that allows all phases of the production process to be tightly integrated. This I^3 enabled vision allows a real –time view of flow through the entire production process. When this same network is connected to market side demand indicators, it becomes possible to create a just-in-time (JIT) manufacturing process that flows from raw material to customer.

The I^3 peering system allows an even larger scale view of IOT driven manufacturing processes when I^3 systems are connected across corporate boundaries to include suppliers and partners. This further enhanced perspective allows a company to create a production process that is responds to conditions outside the perimeter of its own dedicated IT infrastructure by including ecosystem situational awareness. Ultimately the I^3 system will enable better management of the work-in-progress, improves capital utilization, customer responsiveness, and corporate profitability.

1.4 Scenario: Smart City

Smart Cities are special IOT environments that can benefit significantly from I^3 system concepts. What makes Smart Cities challenging for automation is that the resources needed to support the operational needs of the city and the citizens are spread over a wide area, budgetary constraints are high, and device/application options vary widely city-by-city and even within a single city.

Smart Cities may include any or all of the following types of installations:

- Airports (big data applications)
- Utility companies (water, power, gas, electric [including enterprise and residential solar panels]). This also includes smart metering which allows billing for services based on time of day and service cut-offs that may be needed during times of rationing. (
- Jails (detecting/monitoring prisoners, opening/closing doors, alarm systems ,et
- Emergency response (data, voice, video) from police, fire, ambulance
- Smart buildings (locks, lights, heat, AC, Co2, alarm systems, video monitoring, personnel tracking, visitor tracking, prisoner tracking)
- Road/traffic monitoring (traffic volume, average speed, etc)
- Traffic light management and detection/recoding of traffic light violations
- Voting and citizen input (using magic band or other sensors as a means of citizen verification)
- Metro, Staff car, trucks, buses, trains, and boats are all tracked by location and vehicle status. Vehicle alarms are also supported as well as conditional data that support logistics management (including route scheduling and management; this includes counting people on buses/trains, bus and train diagnostic, on/off schedule,
- Parking (meters, traffic lots monitoring, parking space management)
- Crowd management (parades, county fairs, street festivals, etc)
- Event venues (convention centers) concessions, tickets, security

- Tax collection, ticket collection, restraining orders,
- Court management (remote arraignment, scheduling, document delivery)
- Irrigation/water management (detecting leaks, on/off valve switches, flow measures, activation of flood control measures, managing grey water, rain water capture effectiveness, etc)
- Waste management including disposal trucks, processing facilities, and drainage plumbing. A city might even put sensors on each garbage can.

Cities have numerous city buildings that must be managed (city hall, library, schools, fire-stations, police stations, jails, community centers, event venues, airports, train stations, etc). Cities also have large fleets of vehicles that might include cars, buses, trucks, lawn mowers, ambulances, fire engines, and even helicopters. Cities also have a large number of employees (civil servants) and citizen volunteers (e.g. volunteer firemen, neighborhood watch, chamber of commerce, parent-teacher associations, etc). Every building, vehicle, and citizen represents a resource that can benefit from information and can improve city operations through the data they produce.

Weather and emergency system sensors may be deployed throughout the city in order to report rain, humidity, temperature, earthquake, and other situations to the city manager. When street lights are converted to LED (they can be converted to a platform for sensors that include weather, pollution, seismic, traffic, and people sensors); cities may start with stand-alone system sensors, evolve to monitored LEDs that report on/off only, and then evolve further to support these advanced integrated systems. In future, commercial buildings may have sensors that detect earthquakes, temperature, humidity levels that may predict future building code issues.

Administrators who oversee I^3 systems will have the capability to go into the system and set the permissions of the system making sensor visibility limited to a specific department, to a number of departments, to the citizens or to the public at large (citizens and non-citizens). City administrators should have the ability to 'sell' access to their data to non-citizens as a source of government revenue.

Smart cities may include many aspects of smart factories, smart office buildings, etc, however, the scale is different in terms of number of sensors, the geographic distribution, and the potential number of users.

Government facilities will be a natural target for terrorists and criminals. This implies a need for extensive alarm/intrusion detection on all government facilities especially facilities that are operational lights-out facilities (those with no local human presence). The pipes, overhead lines, and other facilities should also be alarmed. Finally extreme measures should be taken to secure the I^3 system from human and virtual attack (this may also drive a need for I^3 system redundancy (where one I^3 system might serve as a backup for another I^3 system housed in a different facility.

Smart cities should not just save costs but should significantly cut taxes for citizens. Cutting taxes means fewer city employees per citizen; rather than eliminating jobs, the goal of the I^3 system should be to allow significant growth of the city without driving a corresponding need for increased civil servants. As an example if security is a major driver for IOT in one city, the I^3 system should be able to support sufficient use of video monitoring to maintain a constant level of security while avoiding the need for a significant increase in police.

The I^3 system should all a private alarm system (e.g. the alarm system on a corporate building) to feed sensor data directly to the police allowing police to monitor building alarm systems (possibly for a fee).

When a security issue is detected, the police should be able to quickly respond by dispatching officers to a potential crime scene and by quickly and efficiently opening the sensor permissions so that information is fed to ambulance, fire, hospital and other emergency response units. Video systems should also be able to be monitored and then quickly opened to other support resources during crisis situations. If future drone based video surveillance and illumination system should feed information back to the I^3 system and the I^3 system should be able to manage the drone activity as well.

Sensors normally associated with police, fire, and ambulance support services can be linked together in order to improve emergency support services. This same information can be linked to nearby municipal authorities such as neighboring cities or unincorporated areas to provide these areas an ability to coordinate emergency response efforts. And, in times of extreme crisis, the system should be quickly reconfigured to provide access to National Guard and other federal agencies.

City vehicles can be equipped with sensors that record video images as the vehicle moves through the city and vehicle impacts that might imply poor road conditions or an accident. These images can be analyzed to identify roads in need of repair, missing signage, graffiti, etc and other conditions that may warrant dispatch of city services.

Cities might ask subcontractors to deploy sensors as a prerequisite to obtaining a city services contract. When the subcontractor deploys the sensor, the subcontractor will be the sensor owner of record. If the city expects to have visibility of these sensors, it may require the subcontractor to give read/write permission to one or more of the city's departments.

The city will likely not have the resources to deploy all possible sensors within the city limits. The incentive mechanisms of the I^3 system are intended to encourage citizen deployment of sensors, sensors that can be integrated into the city's I^3 support system. IF a residence deploys a mini I^3 system to support their residential needs, the city I^3 system can treat the residential system as a peer and keep a reflection of the residential registers (e.g. alarm registers) in the city's persistent database.

Services are managed to the sub-residence (multiple families in a single home) with smart meters that allow a single service management device to support many service-oriented sensors. This fine grain management allows services to such as water consumption and water rationing rules to be applied to individual houses.

Sensors can be applied to individual parking spaces to locate free parking spaces for citizen benefit (and to increase parking meter revenues while reducing traffic congestion), sensors can be applied to car and bike share vehicles so such shared resources are not tied to a specific application further improving citizen convenience, turning location into a revenue source for the drivers and an incremental tax source for the city.

With I^3 a systems in-place, sensors that are embedded into the streets to detect traffic volume can be logically linked to applications that control street lights to alter traffic flow in congested areas to alleviate congestion. Fees on toll roads can be dynamically adjusted to reflect traffic conditions. Weather sensor data can be incorporated into traffic management algorithms. In general, roadways become smart-roads that reflect the status of the city.

911 service centers have represented a significant step forward in terms of public safety, and the near ubiquitous availability of mobile phones represents another step forward in this space which has been

citizen funded. The augmentation of video and sensor data to emergency call reports has the potential to be equally as significant. While the city may fund sensor deployment in public areas, it is important that citizen funded sensors in private areas can be equally integrated into the network of sensors.

Emergency Services have historically allocated different radio spectrum to different emergency services and the lack of commonality and interoperability has created communications difficulties during times of emergency. The FirstNet initiative represents a solution to the communications issue and the I^3 system represents the next logical step which allows emergency services departments to share sensor data between private and public entities.

A city developed application could temporarily shut off water from users who have exceeded their quota. Analytics running within a city application might detect when a water heater has broken and water is running free; the city application could shut water at that specific house until the situation can be investigated.

Citizens are the option to offer their sensor data to a government I^3 system. If they do this the government may offer them a discount on their utility or tax bills with the understanding that the government entity will sell access to their data to commercial interests. Thus the data from its citizens becomes a potentially lucrative source of non-tax income for the cities.

1.5 Scenario: Smart Campus

A smart campus includes many aspects of a smart city and adds to that mix the need to support faculty research and student learning. The concept of a private, public or community smart-campus is often applied to high education but the requirements can be applied albeit at a smaller scale to high schools, elementary schools, and even at a lower level to preschools.

A smart campus has to support student (and faculty) day-to-day retail activities. For example, students should be able to use magic band devices to pay for goods and services.

A smart-campus is a semi-autonomous environment where security requirements are higher than they might be in a non-campus environment. Ideally, security should be able to find a specific student at a moment's notice through the use of IOT. Magic bands should work with or without cellphones; if a cellphone is near the magic band might act as a beacon and cause the smartphone to report the student's location and when the cellphone is not near (or powered off) it might act as a beacon triggering receptors at strategic locations throughout the campus.

Buildings should be monitored to count the number of students in any specific building. When the number of students exceeds a given threshold, interior environmental conditions (heating, air conditioning) may need to be adjusted and additional security may even be dispatched to manager larger crowds. When it is time to close a building, the building should be scanned to ensure that no students (or faculty) are still in the building.

In a catastrophic situation, for instance should an active shooter be discovered on campus, security should be able to should be able to make a best effort to isolate the shooter. They should be able to track movements inside and outside the building even if the shooter is not carrying a beacon or cellphone. This likely involves use of video to identify criminal description and then tracking the criminal while they remain on campus. The system should be able to send out a mass notice to students, faculty, and staff via smartphone, public viewable message scrolls, and other alerting system. Security should also be able to put the university into an automatic lock down mode.

Video cameras at parking structures and gates should be able to record cars/trucks that enter campus. University vehicles (trucks, cars, gold carts, etc) should be tracked based on location and it should be possible to find any university vehicle no matter whether they are active or not. Maintenance and performance data should be collected and reported to the I^3 system so vehicles in need of maintenance can be scheduled with the services hub. Vehicles that have gone missing over a short period of time should result in their own alert.

Many physical packages move through the campus environment. While some packages will have IOT sensors attached to them and some packages will have beacons, not all packages will be properly tagged in the IOT system. The I^3 system should be able to detect the appearance of a new package (or any other entity) under its span of control. These previously unidentified sensors should trigger an investigation. Further, some packages will not contain any IOT sensors. Vision systems should be able to identify the package based on bar codes, facial recognition, or another intelligent identification process.

An automobile dealer/manufacturer might sell a fleet of vehicles to the university. The university which owns the cars can use the data from the vehicle sensors to manage their fleet. They can open access to these sensors to the manufacturer in exchange for an extended warranty or for a fleet discount. If the car is under lease, the leasing company may demand access to the sensor data in addition to the university's fleet management system. Insurance companies might also offer discounts for access to the data or might pay for access to the data in order to allow them to do proprietary vehicle traffic studies. Data ownership questions become critical in the IOT space and remain largely undefined territory. Our assumption is that at some point the FTC will require manufacturers to open the data streams from their IOT products. Companies that wish to maintain absolute control over their data streams from their products will thereby be forced to move to a leased/rented business model so they maintain ownership of the product. The alternative would be that the companies make warranty services contingent upon continued access to the data stream. Another alternative might be to provide compelling value added services contingent upon access to the data stream. Ultimately, the expectation should be that some percentage of the market will divert the data stream from the manufacturer to an independent data processing service which competes with the manufacturer much like independent auto repair shops compete with dealer service centers. We expect the emergence of I^3 systems will help bring this issue into focus; when users have to explicitly permit application to their data and are enabled to be compensated for release of their data, it become clear that a transaction has occurred. (In Europe, where ownership is considered a basic right which cannot be sold, the clarity of the issue will remain murky as long as European law continues to force its citizens to be data-agoraphobics).

License plates of unknown vehicles should be read and dangerous or unknown plates should create an alert of different severity. The system should be able to report which vehicles are in which lot in case security is looking for a car.

In future, autonomous vehicles that include self-driving cars, delivery trucks, autonomous carts, and drones will be used to manage university operations on campus. These vehicles will be able to report their operational status, condition/type of payload, and location to the I^3 system. Applications with access to this sensor data will be able to coordinate movement of materials through the campus environment.   Robotic loading stations will be able to offload packages from one convenience vehicle and load it to another as packages are sorted for delivery to their intended destination.

Universities also have research and educational needs for IOT. University researchers should be able to quickly build applications that allow researchers to test user responses to different privacy studies, innovative business models, etc. Researchers should be able to detect and report environmental conditions so they can report the weather and other conditions that may impact research conditions. Research projects are not expected to have a long operational lifespan.

Faculty should be able to assign students to projects that require development of IOT applications. Students should be able to create applications to demonstrate subject matter expertise without compromising the operational nature of the I^3 system. Student projects are not expected to have a long operational lifespan.

Over time, cities are expected to evolve and deploy new technologies that are not currently practical in the field. For example, in the future, cities may deploy storage batteries that store solar or wind power in the day and provide a backup source of power at night. Cities might deploy 3D printer kiosks that allow citizens to 'print' emergency keys as a service for its citizens.

1.6 Scenario: Smart Hospital

Hospitals are high technology setting where technology is used to increase patient care, improve efficiency, improve business practices, and drive medical diagnostics to a new level. IOT technology has the potential to drive dramatic improvements on all these fronts and those gains will be maximized if there is a break from looking at IOT as a series of applications and instead begin looking at it as an advanced healthcare platform.

In a hospital/medical center, IOT technology will change the way we collect medical data from machines (diagnostic, monitoring, etc), it will allow us to track doctors, nurses, and staff can be located and quickly respond to emergency situations.

The I^3 system can also be used to track the location of portable diagnostic equipment and can capture diagnostic results as sensor data. Medical applications can use the data in the I^3 system to consider results from multiple diagnostic systems, apply heuristics, and suggest possible diagnosis and even suggest possible treatment options to the attending staff while they are enroot to the patient.

IOT applications can autonomously report patient alarms when data is out of expected bounds. They can schedule reports and deliver them to health care professionals in advance of patient visits and support on-demand report requests for individual patients, for all patients on a floors, for all patients of a specific doctor, and more.   Reports can also be automatically triggered based on location (so a refreshed report is created whenever a doctor is near patient). Patients should also be able to request reports describing their sensor detected activity while they were in the hospital.

When a patient checks out of a hospital room, the sensors monitoring the patient should be remotely (or locally) reset so that a new patient in the same room does not have visibility to any residual data.

Because predictive analytic software would have detail visibility to all patient sensors via the I^3system and that information can be linked to historic patient records, patient diagnostics would be improved and when statistics are run across larger populations, community trends would be quickly identified.

Healthcare systems need to meet HIPPA requirements and the I^3system must be able to comply with these requirements. One of the goals of the I^3 system is that the sensor owners should have complete control of their data privacy. In a hospital setting, the hospital owns the sensors that are monitoring the individual patients. Patients or their next of kin would need to provide the authority to allow doctors outside the hospital to see their data. When the patient is incapable of providing electronic authorization, there should be a manual means for the patient to provide verbal/written authorization and a means for the hospital to document that authorization.

Doctor access to sensor data via the I^3.system should be configurable based on shift work so doctors can be prevented from accessing patient data when they are not on duty if that is the administrator's policy. The administrator may alternatively have a policy that only permits doctors access to I^3.data when they are on the hospital grounds.

Doctors often maintain private practices in offices that are distant from the hospital. Doctors should be able to deploy small, remote I^3.systems in their office which can collect local sensor data and share it with a distant hospital. Given that a single doctor may have a relationship with multiple hospitals, these mini I^3.system should be able to link to multiple hospitals using the I^3.peering feature.

Hospitals may also maintain relationships with many local health clinics. These local clinics have the option of deploying their own I^3 system and then linking them together through the peering system or they can have the hospital use its I^3 system to manage the sensors on their premises. When hospitals are a part of a larger health care related system (e.g. World Health Organization), the hospital may use the I^3 system peering facility to link permitted sensor reports to the WHO. It is possible an umbrella organization, like the WHO, would maintain an I^3 system as an umbrella manager where all registers track in the database/registry are mirrored registers that are directly managed by hospitals around the world.

Hospital complexes do experience many operational situations as is faced by a smart city or s smart campus. Hospitals have roads and parking lots that need to be monitored, their security needs (video, alarm systems, etc) are significant, and during a catastrophe they may even need to evacuate patient and staff. Any of the IOT management requirements of these other environments may be present in the hospital setting above and beyond the medical IOT objectives.

Many of these same concepts can be applied to nursing homes, senior activity centers, and retirement living communities. These other entities might deploy their own local I^3 systems to manage their local sensors or they could have the local hospital host the I^3 system in order to provide sensor management for on their behalf. (Possibly in a fee, possibly in exchange for the ability to monetize non-patient data, or possibly as an incentive component of the affiliation agreement).

Hospitals should also have the possibility of using the peer linking facility to have a bidirectional link with the other emergency services departments (fire, police, ambulances, care-flight, etc). If the hospital has increased visibility to an evolving emergency situation, they can be better prepared to respond as needed. And, if the other emergency service centers have visibility to the local hospital conditions, they can steer patients to the hospitals best prepared to deal with situations in real-time.

Patients, at the hospital or at home after hospital discharge can report patient medical data (temperature, respiration, blood pressure, etc) to an I^3 system. Once the data is logged in the I^3 system, it is immediately visible to all doctors and support staff with the proper access credentials.

1.7 Scenario: Research and Student projects

Assume a freshman is planning to attend the university and has given campus security permission to monitor their location. The freshman downloads the appropriate sensor client to their smartphone and the smartphone begins reporting location information to the database/registry on the I^3 system.

A university researcher creates an application that will allow them to study student reaction to various targeted messages. The researcher first sends a request to potential study participants asking for their permission to access their location information as a part of the study. For the participants that agree to participate, the application might send an advertisement to an electronic sign when the participant is nearby. At the end of the day, the researcher follows up with a short survey that tests the participant awareness of the targeted advertisement and the creepiness of the message.

When the research is complete, the researcher deletes the application, releases the application attachment to the register and notifies the participants of the completion of the project.

1.8 Scenario: Transportation

The transportation industry is redefining itself as vehicles of all kinds (cars, trucks, trains, buses, airplanes, boats, and more) become more intelligent, more connected, and ultimately more autonomous. As these vehicles continue to evolve toward a fully autonomous and intelligent vehicle, the wealth of sensor data will continue to expand and an exponential rate. The engine, drive train, fuel systems, braking systems, cooling system, passenger entertainment, climate control system, communications systems can all benefit from the use of complex sensor and controllers. At the owner's request, an intelligent vehicular systems can report complex status information to the manufacturer, insurance company, local or state transportation authority, emergency services, independent service stations, and to home tracking systems. In addition, these forward-looking vehicles can accept inputs from external sensors that allow it to improve its operations; for example the vehicle can adjust its operations based on local road conditions, the traffic situation, and weather. Some sensor operations are expressly designed to improve the operator experience by providing access to video/music entertainment, cellphone communications, and directional guidance services.

In the I^3 system, and intelligent vehicle is treated as a sensor hub. The autonomous vehicle would report a complex set of sensor registers to the I^3 hub as authorized by the vehicle owner.

In some cases the vehicle owner and the operator are the same person, but in other cases these can be different entities. For example, for a fleet of vehicles may be owned by a company and operated by a driver. Within a family, the parents might own the car a child drives. In some cases a lending institution may own the car while a lessee owns and operates the vehicle. It is possible for the primary vehicle owner to give subordinate permissions to alternate administrators of the vehicle. For example, a company that provides its executives with a car may hold the title to the car and may track the car for security purposes; the company may give the employee permission to decide whether or not they share the same location information with their insurance company.

Intelligent vehicles feed location sensor data to the I^3 system allowing applications to track mileage for auto submittal of expense reports, travel time that can be applied to client billings, appointment scheduling, and more.

Some intelligent vehicles, such as trucks, will be able to report the status of the cargo along with the condition of the cargo (for instance, the temperature in a refrigerated truck). Cargo can be tracked as a composite shipment reference, as a series of units (e.g. pallets, or case-lots, or even at the piece-part level. Since cargo specific can vary with each trip, the registers that represent a vehicle's cargo should be able to dynamically expand and contract throughout the life of the smart-vehicle. Further, when cargo is moved from one vehicle to another, it should be possible to move the cargo registers with one vehicle to another vehicle in order to maintain continuity of the tracking system.

Passenger-centric vehicles will track counts of passengers and possibly even use passenger identification intelligences to allow direct billing of passengers for steerage. Passenger vehicles also bring with it the requirements to entertain passengers and may possibly also temporarily incorporate passenger sensor data into the vehicle status registers while the passengers are in-transit.

I^3 systems which provide sensor support of airports, truck terminals, train stations, bus stations, ports, and other smart vehicle hubs will need to track vehicles (and their sensors) while the vehicles are parked at the facility.

When self-driving cars begin broadcasting location/status information to nearby cars, it should be impossible to disable these systems. However, malfunction alerts should be deliverable through the I^3 system.

1.9 Scenario: Residential

Residential I^3 systems, while a smaller scale in terms of the number of supported systems, are every bit as complex as any other I^3 system due to the lack of commonality between residential environments. Alarm systems, heating, air conditioning, kitchens, utility management, resident tracking, and other applications need to be supported. Children, pets, wearable data, and more could be collected by a residential I^3 system and the data would be offered to commercial interests looking to find better ways to satisfy the needs of the consumer.

Low income residential applications may need to be supported with some form of public assistance. In today's world where broadband is considered as baseline communications service, an expectation should be that low income residential units be able to connect basic residential sensors with schools, government services, and emergency services.

Work-at-home sensors should be able tie into a remote I^3 system allowing employers to more effectively manage the employees who are not supported from a local office; these I^3 connections would be funded by the employer and not the residential user.

Multi-unit dwelling environments, such as apartment buildings, will have the need to support multiple tiers of residential services from a single commercial entity. In addition, while each apartment is considered a residence, there may be common areas shared by the residence which need to support IOT applications when residents have left their specific residence but remain on the grounds of the complex. In some cases the complex manager will provide IOT support as part of the complex services which puts them in the position of managing the complex IOT hub. In other cases, each residence will acts as a hub and the manager will only provide services in the common area.

A smart irrigation system could check the soil conditions, weather report, and demand statistics to schedule a future watering schedule.

1.10 Scenario: Data Broker

A data broker is an entity that obtains permission to collect data from a number of IOT devices. The data broker can see the data in the I^3 system database. The broker reads the permitted sensor data and applies some value added algorithmic process to the data to further enhance its value. The enhancement may clean the data (removing faulty data, adding missing data), compress the settings into a summary status report, or it can integrate the I^3 system data with data from a 3rd party.

The results can be issues directly to the data broker's customers or the data broker can write the data back into the I^3 system as a series of pseudo registers. In the latter case, the I^3 system would attempt to resell the data in the I^3 ecosystem.