IoT Marketplace: A data and API market for IoT devices

Bhaskar Krishnamachari, Jerry Power, Cyrus Shahabi, Seon Ho Kim
University of Southern California

January 15, 2017

1. Description of USC IoT Marketplace

IoT Marketplace is a new platform to integrate IoT applications with financial transactions and brokerage concepts for IoT data and services (including marketing and pricing) so that IoT sensor data, access to actuators, and relevant data processing/analytics functions (through APIs) can be efficiently listed, searched, and traded among users (i.e., sellers, buyers, and brokers).

IoT Marketplace envisions a world where application developers can gain access to the myriad of sensors and/or actuators that others have deployed and connected to the network, and sensor owners can take the initiative and deploy intelligent sensors in anticipation of an emerging and independent application market that will utilize their data for the benefit of its users.

With the IoT Marketplace platform, IOT device owners will be allowed to access/trade their different kinds of sensor data and actuator access with many different vendors to create a supporting environment so advanced data analytics programs can be efficiently developed and supported in a multivendor-multi-owner device environment. The IoT Marketplace provides methods to make it much easier to develop and deploy IOT applications and devices by maximizing the level of data reuse and interoperation among different applications

2. Background

Connectivity in the world around us is being extended through the Internet of Things (IoT). With smart wearables, smart homes, smart factories, smart cities, and other applications, we are seeing a surge in the number of connected IoT devices. Thus, many targeted IoT cloud and application platforms have been developed and currently in service, such as Amazon AWS IoT, MS Azure IoT, etc. The purpose of any IoT device is to connect with other IoT devices and applications (cloud-based mostly) through the Internet. These connections can be complicated for a cloud or application to manage without the use of intermediary IoT Platforms (also referred to as IoT middleware platforms). The intermediary IoT Platform seeks to fill the gap between the device sensor/actuators and the central cloud based systems in order to make it easier to develop applications that are dependent on data generated by different devices with many different owners. Such a platform connects the data network to the sensor/actuator arrangement on one side and connects to the application network on the other. As a composite system, this makes it easier for application developers

to 1) provide complex insights using backend applications to make sense of plethora of data generated by lots of sensors, and 2) take complex action though the use of many connected actuators. To date, most existing IOT platforms assume the sensors are either owned by the application owner or that the sensor owners will graciously provide application access to their sensor data in exchange for access to the application.

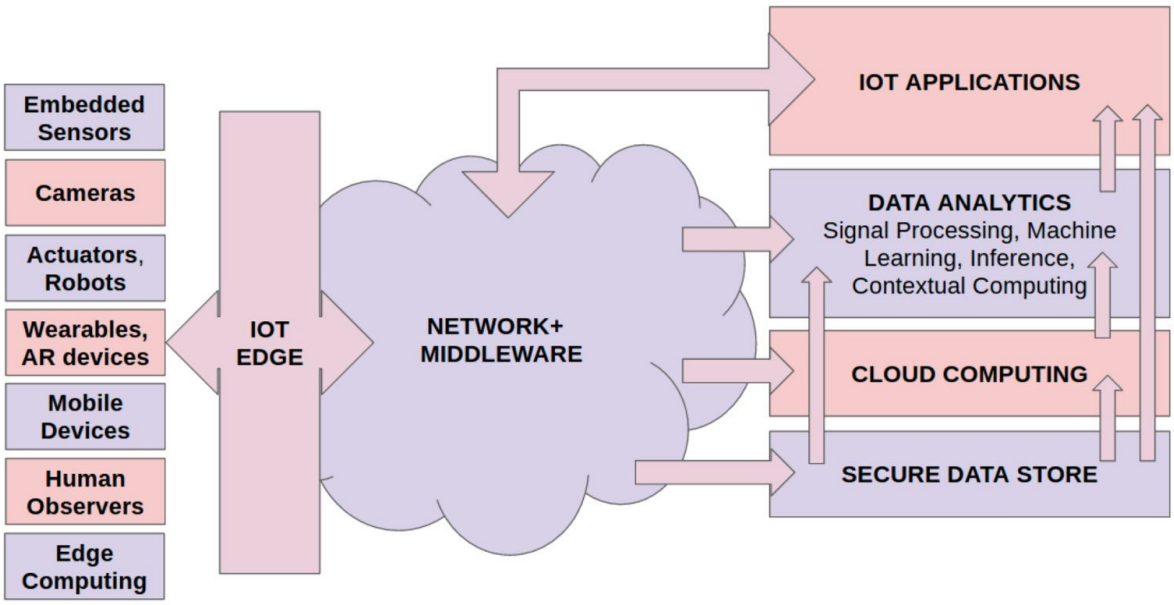

Figure 1. Typical IoT System Architecture

The existing cloud based IoT platform technologies and solutions have been mainly focused on the realization of IOT application functionality (i.e., design and implementation of fundamental infrastructure to collect, transfer, store, interact with targeted sensor data needed to fulfill the mission of a specific application). They are rather limited in scope, with vertical integration of all aspects of a constrained IoT system (see the architecture shown in Figure 1) owned and coordinated by a single organization: the same entity must necessarily develop and deploy sensors and other IoT edge devices as well as the cloud-based storage, computing and analytics engines needed to support end user applications.

As IoT technologies continue to mature and become more diverse, new challenges are emerging because of the increasing complexity of the real world. These challenges include security, privacy, legal, interoperability, etc. These challenges become especially complicated in a fragmented and proprietary IoT environment as the ecosystem continues to grow. The technical implementations of these systems will inhibit value for users and industry. While full interoperability across products and services is not always feasible or necessary, potential IoT

users will be hesitant to buy IoT products and services if there is integration inflexibility, high ownership complexity, concern over vendor lock-in, and the user does not have control of the data their devices generate. The use of generic, open, and widely available standards as technical building blocks for IoT devices and services will support greater user benefits, innovation, and economic opportunity but proposed solutions are not capable of supporting the diversity of IoT devices ultimately envisioned. Future implementations must go further to involve sensor owners are partners in the value creation process. This state of the art approach is limiting and results in an economically significant gap — IoT applications have no value till they have data, yet device owners are nervous about disclosing personal data to third parties. Meanwhile, application developers do not always have the wherewithal to deploy their own devices but are forced to do so. Until this chicken-and-egg problem is solved, application developers will struggle to break free and unlock the potential that IoT represents.

Another major trend is the increased emphasis of IoT data usability and analytics. According to the CEO of Infobright –In the new brave world of IoT analytics companies will struggle to handle the unpredictable data reality. The problem these companies will be facing is not only storing and handling vast volume of data but also converting it into actionable information. Thus, one of the critical new challenges in IoT is to make the IoT data more usable.

The proposed IoT Marketplace aims to satisfy the challenge of IoT data usability and sensor/actuator owner participation by providing a marketplace for IoT applications. It accomplishes this through the concept of brokerage where data producers, consumers, and brokers are able to search, buy, and sell IoT data in a democratic way. Further, as device owners begin to monetize the IoT data their sensors generate as well as access to their actuators, brokers will emerge to provide value-added processing and analytics as well as control services to further enhance the IoT data and manage actuation'

3. Overview of the Proposed System

This system is based on the hypothesis that properly motivated, individuals will contribute sensed data to a managed IoT marketplace that will make data from different owners available to different application developers to create value for end users. If developers were to compensate device owners for the use of their data, we could create an ecosystem where data owners compete to increase the value of their data in order to attract more applications. We are therefore designing a marketplace where device owners, application developers and data brokers can come together to form an ecosystem that goes significantly beyond today's homogeneous vertical deployments.

We refer to our marketplace platform for IoT as I3 (which stands for Intelligent IoT Integrator). The following figure shows the basic architecture of this service system.

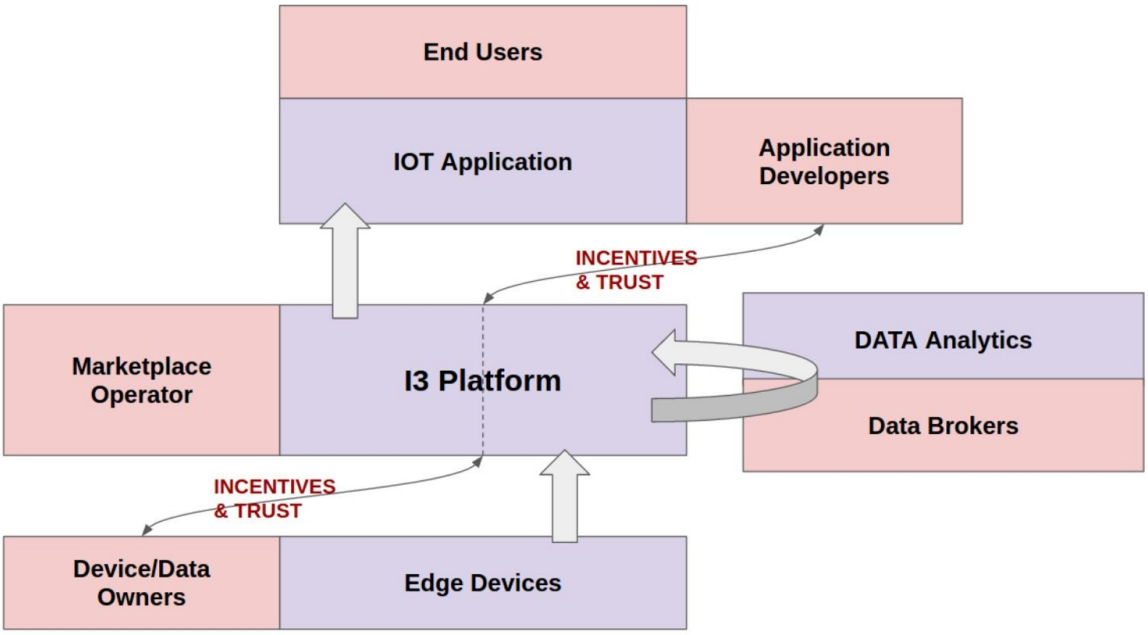

Figure 2. Players of IoT Marketplace Platform

At the core of the I3 platform is a *publish-subscribe middleware* that allows publishers of data to efficiently send real-time data to multiple subscribers anywhere via an intermediate broker. The platform will allow sensor device owners to advertise the kinds of data streams published by their devices and indicate both a) how they wish to value (price) that data, and b) conditions under which they would allow the data to be used. Similarly the platform will allow actuator device owners to advertise the kinds of actions their devices can take and indicate both a) how they wish to price access to the actuators, and b) conditions for access. The platform will also allow for application developers to browse or be recommended relevant published data streams to which they could subscribe or actuators that they could access by agreeing to the terms and conditions of use of the data and device access (such as limitations on usage, resale, further release, or in some cases, on commercial use) and by agreeing to the payment or other incentive terms.

The platform will also provide mechanisms for buyers to offer their own incentives for device owners to participate in providing them with relevant data and access. Once the agreements for use of data and payment for it are in place, subscribe requests by the buyer are authenticated by the I3 platform and result in real-time data transfer to the subscriber upon publishing (there may be just one or multiple real-time data transfers to multiple subscriber devices, whatever is allowed per the agreement). Similarly once agreements for access to one or more actuator devices are in place, the buyer is authenticated by the platform to be able to send control signals to the device(s) in real time (for instance through suitably formatted publish messages that are subscribed to by the device(s)). The I3 platform provides for monitoring and metering of data (how much data did the subscriber get and when) and actuator access (how often the actuator was activated, when, and in what way) and applies the

payment rules to bill the IoT sensor data or actuator access buyer accordingly. Note that sensor data and actuator access may be handled separately or bundled together as suitable.

In addition to application developers, other users of the I3 platform may be data brokers that buy raw data streams and ”sell” refined versions of those stream (e.g., applying data cleaning, de-noising, classification, pattern recognition or other forms of data analytics and machine learning). Yet other users of the I3 platform may be brokers that provide a new way or algorithms to visualize, aggregate, and control actuators. Both kinds of brokers would provide added value in the form of improved quality, features, performance, and convenience to application developers over and above raw sensor data and actuator access.

The smartness of the I3 platform consists in the ease with which it can allow buyers, sellers, and brokers to interact with each other — the recommendation engine enables intelligent automated matching of buyers and sellers, including the ability to easily offer and accept prices/incentives from both sides. Authentication mechanisms ensure the right subscriber gets the right data and trust mechanisms such as those based on ratings and reputation serve to encourage constructive creation of value for both parties.

When moving past individual edge IoT networks to connecting very different types of sensors and actuators to the cloud platforms and application developers, there is a need to identify a suitable middleware. Here there has been some prior work, particularly in the context of middleware for event-based systems. Most such prior works focused on publish-subscribe middleware for real time communications across thousands of devices across the Internet. A popular open-source middleware system is *MQTT*, which provides for publishers and subscribers to connect to specified named topics on a centralized broker (with additional authentication plugins allowing for secure and confidential access). There are also commercial Platform as a Service (PaaS) providers such as PubNub, which provide publish-subscribe API’s for customers to develop their own real-time applications, and take care of hosting an authentication-based middleware broker on their own cloud. PubNub also provides for additional functionality by allowing publishers to place pre-specified computations on their cloud. The PubNub project offers an open-source implementation of publish-subscribe middleware. These prior solutions assume that the devices and application are owned by the same entity.

4. Description of IoT Marketplace

The main idea of a market for IoT is to allow owners of sensors and actuators to charge IoT application developers for use of sensor-generated data and for access of actuator capabilities. This type of marketplace goes beyond support of immediate device owners and application developers to allow a new class of data-centric value added service providers to emerge where data processing/analysis can be provided to sellers and buyers of IoT data by brokers.

To be functional as an effective marketplace, I3 incorporates and provides the following mechanisms:

- the sellers to post their available sensor streaming data and actuator access products along with some indication of their value and conditions of use
- application developer and data/actuator access broker buyers to browse or be recommended relevant sensor data streams/device owners as well as data brokers to connect with. This can be in the form of a directory and/or a recommendation engine (see below).
- incentive mechanisms for sellers to provide useful data and actuators, such as monetization per unit quantity of data or actuator access
- routing of real-time data from sensor data sources to all consumers that are authorized based on the agreements entered into (including payments, usage policies)
- routing of real time actuation and control signals from authorized users (buyers) to actuators
- trust and reputation measuring mechanisms for users to rate each other
- metering and billing mechanisms to enforce market agreements
- data naming and structuring functions, as well as privacy mechanisms to filter data being routed through the marketplace
- API's and SDK's for programmatic access to various functionalities of the platform

Thus the IoT Marketplace provides 1) efficient sharing/trading of data, 2) convenient negotiation and transactions of data and access price and usage policy models, and 3) data
flow control to implement the brokerage concept.

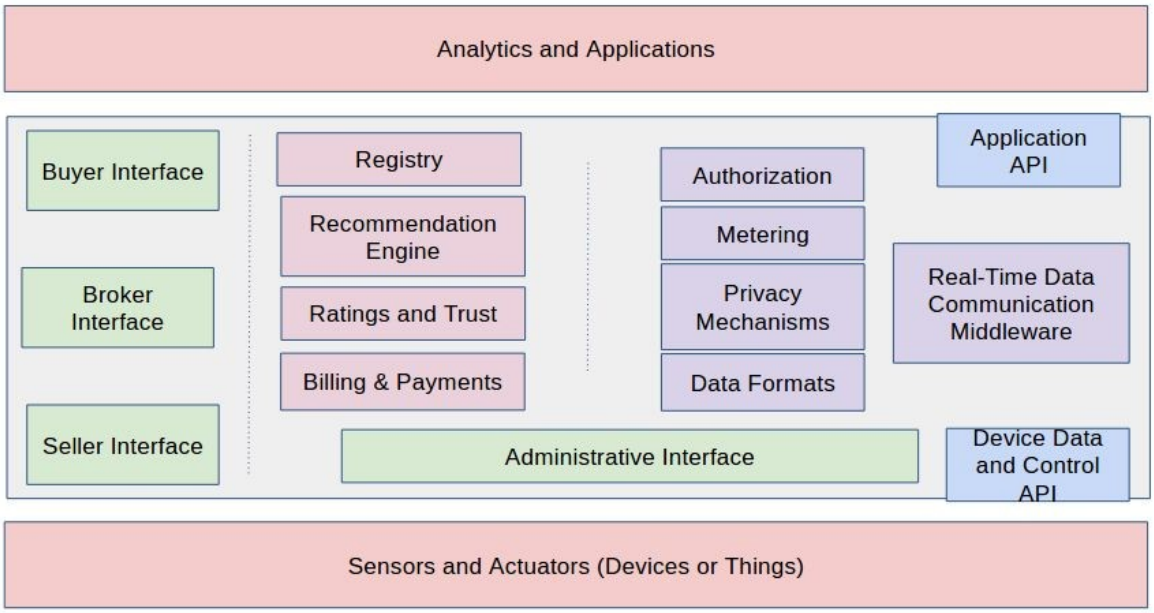

Figure 3. Components of IoT Marketplace Architecture

In the following sections we detail the various key components of the IoT Marketplace.

4.1 User Interfaces

There are three main groups of users of the IoT Marketplace:

- Seller: the owner of IoT sensors, actuators: these are the producers of data or controllers of access to connected actuated devices.
- Buyer: the developer of IoT applications that wish to gain access to IoT sensor data (raw or processed) or actuators in order to derive insight or take action on a derived insight.
- Broker: anyone who provides value added technical services (such as data processing and actuator control mechanisms) and business (mediation) services to buyers and/or sellers in IoT Store

In addition, there is an administrator of the IoT domain that acts as the operator of the marketplace. The administrator may / may not be a device owner / application developer as well, but has the ability to set up, configure, and maintain the marketplace.

Seller Interface: In I3, Sellers (owners) describe and post their data and capability (of sensors/actuators) in the form of metadata including information about the types of sensors, locations, etc., and sample data if necessary. They may add additional data or metadata to increase the value of the sensor stream, or provide value-added actuation control capabilities beyond the raw capabilities of actuators. They can also browse/find postings by developers and brokers in order to search for potential Buyers. Sellers set prices of data for different licensing / sale models such as possess, reuse, use for limited time, resell, process/re-package, etc. To support dynamic nature of IoT applications, I3 may provide dynamic pricing options with which Sellers can change prices, renegotiate prices between Sellers and Buyers, limit access and approve the use of their data to particular applications, classes of applications, e.g., non-profit or research purposes. Furthermore, Sellers may be allowed to charge differential prices to different users, and rate buyers, whom they have interacted with, to evaluate their reputation. Sellers may also set conditions for use that buyers must agree to abide by and possibly even provide relevant documentation for, before being provided access to the relevant data. In some cases, sellers may allow access to data / actuators by certain users without charging any price for it, so long as the users satisfy certain conditions specified by the seller. E.g., access to traffic sensors owned by a department of transportation in a city may be provided free of cost to an application owned by a department monitoring environmental quality in the same city.

Thus, through the interface provided by the marketplace, sellers (device/device network owners) can:

- register and login to the marketplace

- describe and post their data and capability (of sensors/actuators) in the form of metadata including information about types of sensors, location, etc., can provide sample data.
- browse/find seller's and brokers' posting
- set prices for data; this may include different licensing / sale models: provide different terms of use, limit time of use, permit resale, allow repackaging
- potentially change prices (or offer dynamic pricing that is automatically adjusted based on relevant factors)
- limit access and approve the use of their data to particular applications, classes of applications, e.g., data sales to non-profits may have different conditions compared to commercial conditions.
- post a form soliciting relevant information about the buyer's background, or an invitation to negotiate the price
- charge differential prices (to different users) , e.g., data sales to non-profits may have different prices compared to commercial prices.
- rate buyers they have interacted with
- append their sensor data with logical data in order to increase the value of the sensor data.

Buyer Interface: On the other hand, Buyers (application developers or analytics-based data brokers) can describe and post their needs for IoT data and networks, can browse/find Seller's and Brokers' posting, can purchase and apply for use when needed. They have the potential to negotiate prices with Sellers, lease/buy data and services, and get access to the sensors and/or actuators as allowed by the application when purchased. To support a large scale application which requires data from various sources, Buyers can combine multiple streams of data into their applications seamlessly through API's/SDK's provided for them to use. Buyers can also rate Sellers they have interacted with in order to highlight sellers with high-quality data or particularly relevant actuators for other Buyers. These ratings would feed into mechanisms for evaluating and building trust.

Thus, through the interface provided by the marketplace, buyers can:

- register and login to the marketplace
- describe and post their needs for IoT data and networks
- browse/find seller's and brokers' posting through directories or a search engine, where the postings describe the sensor/actuators data and metadata, who the relevant owners are, information about pricing, licensing, conditions for use, data and actuation command formats and data/actuator access methods
- be recommended particular types of sensor/actuators to use
- purchase and apply for use as and when needed
- provide payment and billing information
- negotiate, lease, buy data and services
- get access to the sensors, actuators as allowed by the application when purchased
- combine multiple streams of data into their applications seamlessly through API's/SDK's provided for them to use.

- rate sellers they have interacted with
- provide comments and suggestions for improvement of the marketplace

Broker Interface: Brokers can describe and post their capabilities, browse/find Seller's and Buyer's posting, and purchase access to data and actuators. They may negotiate service price, lease/buy data and services, manipulate, and resell the enhanced-value data or enhanced actuator control to other Buyers. Brokers provide value by adding additional technical services and solutions for Buyers and Sellers, e.g., adding IoT data processing or data analytics or actuator aggregation and control mechanisms when Seller cannot provide it and Buyer does not have the capability. In one possible implementation, brokers may simply act as both buyers and sellers.

Thus, through the interface provided by the marketplace, Brokers can :

- register and login to the marketplace
- describe and post their capabilities
- browse/find seller's and brokers' posting
- negotiate, lease, buy data and services, manipulate, and resell
- (if a business broker) find potential buyers and sellers, and offer discounts or other incentives for them to join the market, and be remunerated for their own efforts
- (if a technical broker) add additional technical solutions for buyers and sellers. e.g., add IoT data processing or data analytics which seller cannot provide.
- rate other users

The seller, buyer and broker interfaces will allow for various Pricing Models: to provide different ways to charge for data and actuator access and services, including

- static pricing: fixed
- tiered pricing: fixed but with multiple use categories
- dynamic pricing: changing over time
- negotiated pricing: actively negotiated at the time of sale

Admin Interface: Administrative control over the marketplace may be connected to the domain where it is deployed. For instance, an IoT marketplace system that is associated with a campus, an enterprise, a town or city will have the corresponding organization administer it. The IoT marketplace will provide an interface allowing administrators to:

- login to the marketplace after providing the requisite credentials
- set up and configure various interfaces and elements of the marketplace
- Configure, modify various policies, such as for posting data and actuator access, pricing, negotiation, etc.
- select and configure relevant hardware and software for the marketplace (such as computers and routers if any, databases for registry and authorization, middleware

servers for realtime communications, recommendation engine, privacy mechanisms, cloud computing resources, etc.)
- create whitelists or blacklists of users, ban users
- install and configure other firewalls as needed for ensuring the security of the marketplace

4.2 Registry

The IoT Marketplace includes a registry which contains relevant information about all registered users (buyers, sellers, brokers); all available sensor data and actuator streams; information about their ownership, conditions for use, and pricing; completed and ongoing transactions agreements and payments including currently authorized users.

Ownership of Data and Devices: to represent and manage the ownership of data and devices that can be accessed in the market, the registry includes information about

- physical ownership of devices and data
- access right (read, write, modify, resale, etc.)
- licensing (public, semi-public, private),
- ownership management, allowing for unique identification of data and device owners
- sensor data and actuator naming

Information stored in the registry is used to populate the various user interfaces, e.g. to show buyers what devices and data streams are available, to identify their pricing and policies for use. The information in the registry provides necessary input to the recommendation system (see below). The information in the registry is also used to determine authorization for data routing, e.g. to ensure that sensor data from a seller is only available to users that have paid for it. Information regarding ratings and trust in buyers and sellers are also stored in the registry.

4.5 Recommendation System

In the I3 marketplace, Buyers will seek to find raw data which they can leverage once it is acquired. By accessing these assets as they pursue their own IoT business initiatives, Buyers will be able to better understand their data's value and utilization thereby allowing them to align their business cost-model with their business revenue model (buying data as needed). This new capability may also allow them to create new value-added business models that will further enhance their applications' value-proposition driven by the selective purchasing and accessing sensors.

The quantity and variety of data collected via existing IoT systems (much of that data is now held by third parties) can make it difficult for Buyers to find the data they want. This IoT marketplace has the potential to enhance the value of this existing historic data by allowing the data owners to market their data in an open and vibrant data marketplace. Based on the data owners understanding of their data and combining this data with other new or historic

data, data owners will create new opportunities for the data they already hold. By establishing such a system, users can more readily and reliably identify and trade useful data set for their own purposes.

To identify data set for a potential trading, IoT marketplace maintains an advanced directory service for participating users to search for data, applications, and services. Directory requires three fundamental representations: 1) Description of IoT data - physical and technical description of data item such as type, size, location, generation time, access method, ownership, etc., 2) Seller's requirement (Seller properties) such as what to sell (IoT data description) and how to sell (price and licensing), e.g., public, semi-public, private, access right (read, write, modify, resale, etc.), and 3) Buyer's requirements (Buyer properties) such as what to buy (IoT data description) and how to buy (price and licensing). The marketplace will provide a standardized way to handle the above data.

Based on the above representations, I3 directory provides two methods to identify matches among Sellers' and Buyers' interests. A straightforward method is listing: Data should be properly listed and/or categorized to be easily found by human users with various search features. This might be sufficient in a small market. However, as the number of users grows and the amount of heterogeneous data becomes large, a simple list may not be effective while automatic searching and recommending will get more practical by saving human user's valuable time. Considering the complexity of matchmaking many data items, sellers, buyers, and brokers, it would be helpful to provide a systematic recommendation for users.

In the I3 context, one can consider three different recommendation scenarios. First, recommending data items to Buyers. This scenario occurs when a Buyer searches for data items prior to purchase, and hence the recommendation service is provided to the Buyer. Since the descriptions of IoT data and Seller's/Buyer's requirements can be represented with feature vectors, we use the *content-based recommendation* approach for this scenario, which utilizes the features of the items to be recommended. In particular, for IoT applications, spatial and temporal aspects of the sensors are important, thus we use the recommendation algorithms focusing on these features building on our experience in managing spatiotemporal data. The second scenario is to recommend potential Buyers to Sellers. When a Seller is interested in selling data items, the recommendation service would suggest some potential Buyers to the Seller. This is similar to the case 1 recommending similar data items to Buyers.

When a Buyer wants to buy more similar data items after application is started and growing, a different kind of search for similar data items might be needed. This is especially interesting for human sensors when we assume dynamic nature of human behaviors (which will be described in the following section) and ad-hoc participation (join/leave) of people. For this kind of recommendation, we use *collaborative filtering* systems to recommend data items based on similarity measures between users and/or items. Collaborative filtering works based on the assumption that if user x interests are similar to user(s) y interests, the items preferred by y can be recommended to x. The items recommended to a user might be those preferred by similar users.

4.6 Ratings and Trust

For an effective marketplace, it is important for all parties to have a level of trust in each other. As noted above, all users of the system have an opportunity through their respective interfaces to rate other users they may have interacted with. E.g., buyers can rate sellers, sellers can rate buyers, etc. Input for ratings may be provided in the form of numerical scores (or stars), response to survey questions, and qualitative textual reviews. These inputs provide the basis for building trust through reputation. E.g., sellers that provide high quality data are likely to have a higher rating / reputation, causing buyers to trust them more. Other mechanisms for building trust may be included in the marketplace. They could incorporate, for example, a way for buyers / sellers / brokers to demonstrate third party certifications with respect to policies or mechanisms they have in place to ensure validity, integrity, confidentiality, privacy, security. Users with simple, transparent, third-party verified data use policies may be able to present these as a way to build trust as well.

4.7 Billings and Payment

The marketplace may incorporate different mechanisms of payment (e.g., advance payment, pay-as-you-go, payment at predetermined intervals) and modes of payment (e.g., credit card, digital or online currencies, check, etc.). Information from the data and access metering mechanism (see below) will be used in conjunction with the biling and payment agreement stored in the registry to determine how much a buyer should be charged and when, and how billing should take place. The marketplace operator may realize revenue in the form of a percentage or fixed commission off each transaction or a one-time fee for listing each sensor/actuator stream, or for user registrations, or some combination of these. Incentive mechanisms offered by the sellers and the operator such as discounts and coupons will also

be taken into account in the billing and payment system.

4.8 Real Time Data Routing Middleware

The IoT Marketplace includes a data routing middleware that allows data from sensors to be routed to authorized applications, and control signals from authorized applications to be routed to corresponding actuators, in real-time. In case of high bandwidth or particularly sensitive data, the middleware may potentially route through pointers to addresses of relevant data sources (e.g., URL's or IP address + port numbers) instead of the raw data itself, allowing for the data itself to be directly communicated between the seller and buyer through an external channel (such an approach may not allow for data metering, provision of privacy, and implementation of brokering and trust mechanisms, however, and as such may not be a preferred instantiation for the marketplace).

The middleware can be implemented, for instance, using a publish-subscribe broker such as MQTT. In this case the data is sent from relevant devices and sensors in the form of publish messages with corresponding topic names, and applications must sent subscribe messages along with necessary credentials to be connected with them. The broker would check with an authentication plugin to ensure that the subscriber is authorized before sending on the published messages to the subscriber. As MQTT allows for one to many communication, a single buyer may implement subscription messages from applications running on multiple devices to get the corresponding data on multiple devices (assuming it is allowed by the purchase agreement). Likewise, the middleware may allow for many to one communication or many to many communication, allowing multiple sensor devices belonging to the same owner / seller to send data to one buyer and application or multiple applications belonging to the same buyer or even multiple buyers simultaneously. Actuator devices would send subscribe messages to the broker, and authorized applications would then be allowed to send control and actuation signals to that device in the form of publish messages.

The middleware may also implement mechanisms for interoperability with different types of communication and middleware systems and IoT applications, such as CoAP, MQTT, Websockets, XMPP, or proprietary systems such as PubNub, RTI, and proprietary IoT Cloud systems.

The data sent through the IoT marketplace may be encrypted end to end, with the buyers being able to unencrypt the data based on keys that they obtain after payment / agreement to usage policies. In a different model, the data may be encrypted from sellers to the marketplace and from the marketplace to the seller, with unencrypted data on the platform allowing for the implementation of sensor fusion, aggregation and other privacy mechanisms.

4.8.1 Data Access beyond Real-Time Streaming: For certain applications it may be desirable to allow buyers to access not only real time IoT data but also historical or archived repository data. In such cases the real-time middleware or other software may allow for the exchange of pointers and addresses to the relevant repository. The marketplace operator

may also choose to configure their own repository to store such archival data (assuming it is allowed by the corresponding seller(s)).

Note that a key idea in the I3 IoT Marketplace is to separate any data repositories from the relationship brokering. I3 systems can be run as independent data market places or they can be usable by other existing IoT platforms.

4.9 Authorization

Once a data or actuation product is purchased by a buyer, access to the corresponding data or actuation access stream is provided by the platform. This may be implemented in the form of an entry in an authorization database, that is used by an authentication plugin connected to

the real time middleware (e.g., to determine if a particular subscribe (publish) message from an application comes from a buyer that has paid for the corresponding sensor data (actuator access) stream). Through API's (see below), buyers and sellers can present the relevant keys and credentials in order to be authenticated by the IoT marketplace middleware. The authorization may implement different granularities of access and allow certain users to only access a sensor stream at a particular frequency.

4.10 Metering

The real time data routing middleware in the marketplace is instrumented so that the amount of data or actuator access consumed by each application and buyer is logged and recorded, for billing purposes. Usage parameters tracked and metered for billing purposes may include:

- Data access/trading: amount, frequency, type: (reading/susbscribing or writing/publishing, unformatted or formatted)
- API access: number of calls for plain data access, for data processing, for data analysis

4.11 Privacy Mechanisms

The marketplace may include privacy mechanism in conjunction with the data routing middleware. These include providing different versions of sensor data streams for different levels of authorization, such that users with highest access level get original, unfiltered data, while users with a lower level of access may get a noise-added or downsampled or aggregated or anonymized or otherwise filtered data stream. Brokers may compete to provide sellers with suitable privacy algorithms for anonymizing the raw data. Privacy mechanisms may also be applied to actuation, where the buyer may only be guaranteed that one among a set of actuators is activated or controlled but not given detailed information about which particular one is activated or controlled.

4.12 Data Formats

The marketplace will allow sellers, buyers, brokers to do transactions over different Types of Data, to represent, manage and communicate different categories of data

- structured sensor data,
- structured actuator data
- variable data (limited length video or audio)
- streaming data (always on video or audio)
- logical data (that may be manually entered by device owners).

The marketplace allows data and actuator access providers (the sellers) to describe the structure, format and naming of the data from their sensors in a manner that would make it useful for the application developers (buyers). The marketplace operator may also configure a particular set of standard data formats (either as an option or required, depending on marketplace needs).

4.13 API's and SDK's

The IoT marketplace will provide application programmer interfaces (API) and software development kits (SDK) for application developers, device owners, as well as third-party brokers.

- The API's provide a set of functions and tools for IoT sensor data and actuator accessing, processing, analysis for IoT data and actuator access trading and application development.
- The API's make it possible for applications to communicate with the data routing middleware in an authenticated manner and through that to the end devices, and for devices to authenticate themselves and contribute data and availability information to the middleware
- The API's may also provide functions to specify the static / dynamic pricing of data and programmatic access (as opposed to graphical user interface access for human users) to the buyer/seller/broker interfaces, rating mechanisms, recommendation engine
- The API's may allow sellers and brokers to specify particular filtering mechanisms to be implemented on the middleware, to ensure privacy of sensor data
- The API's may provide for interoperability between different application layer protocols such as those based on MQTT, CoAP, Web Sockets, XMPP, or even proprietary commercial solutions such as PubNub, RTI, etc.
- Technical broker can potentially develop their own API functions and sell them (as a form of service) in the IoT marketplace. Thus, not only data access and trading, but also any data processing and analytics can be easily incorporated in the store, which can make the market bigger. For example, a buyer wants to buy a set of data but the data needs to be transformed to a specific form but neither seller nor buyer know how to do it. A technical broker who has the requested technique can provide an API to do the transformation.
- The API's may provide for automated data formatting and comprehension of standardized and structured sensor data and actuator commands
- The API's may provide for encryption of sensor data and actuator control signals (either end to end from the devices to the marketplace and from the marketplace to the applications).

- SDK's implementing the APIs may be provided for several different programming languages and environments to enable app developers, device owners and brokers to quickly connect their systems to the I3 IoT marketplace.

5. Novel Features of IoT Marketplace

Comparing to the state-of-art IoT solutions, IoT Marketplace is fundamentally innovative in attempting to create a democratic marketplace for sensor data and actuator access that brings together multiple device owners, application developers and brokers under a common platform. It supports the following novel features:

- Provides the ability to post, search, share, and trade IoT data/services among stakeholders such as Sensor/Data Actuator Owners (Sellers), Application Developers (Buyers), Brokers (both business and technical).
- It brings together a comprehensive set of mechanisms to facilitate the marketplace, including:
  1) mechanisms for application developers to search, find, browse available data sets of relevance to them (comprehensive directories)
  2) a recommendation system to bring relevant data and devices to the attention of application developers
  3) mechanisms for incorporating rating and reputation for owners and the users
  4) mechanisms for application developers to apply for data and actuator use (if necessary), agree to licensing terms, negotiate prices and access
  5) mechanisms to control the data flow: it provides a way to provide real time streams, store archival data, as well as facilitate access to data archived or streamed from other platforms
  6) mechanisms for metering the use/access of data from sensors and capabilities of actuators (through API calls) from the application
  7) mechanisms for potentially anonymizing sellers and users and for privacy-sensitive provision of sensor data and actuator access
  8) mechanisms for the broker to offer discounts / incentives for owners and users to join and participate in the market
  9) cryptographic mechanisms for providing confidentiality of data
- Pricing models of market operation for both data and actuator calls:
  1) pricing based on metadata, metered data
  2) pricing through API calls, whether data goes directly from owner to user or through the IoT marketplace middleware