TRACKING CLOUD ON THE INTERNET USING A CLOUD INFRASTRUCTURE

Bill Karakostas
Centre for HCI Design, School of Informatics, City University, London, U.K.

Keywords: Cloud computing, Intelligent cargo, Transport logistics, Internet of things, REST web services.

Abstract: In this paper we identify requirements for cargo management, and propose a Cloud based infrastructure that allows cargo tracking and monitoring in a transportation chain. The Cloud infrastructure provides services for cargo registration, identity management and notification support using simple and uniform REST based protocols.

1 BACKGROUND

Cargo (or 'freight') refers to goods carried between two destinations, usually, for commercial reasons, through a variety of transport routes (rail, land, ship, air) and means (boxes, packages, containers,…) carried by cargo ship, cargo airplane, rail, truck etc. Apart from the senders and receivers of cargo, there are several other stakeholders in the cargo transportation process, including the cargo carriers, insurers, authorities etc. Some of these stakeholders are active participants in the process while others are indirectly involved, but can still influence the outcome of the process. Customs or port authorities for example, while not directly participating in the movement of cargo, can prohibit a cargo from entering their jurisdiction, or confiscate it if it violates certain regulations.

Consistent management and tracking of cargo across transportation chains, requires coordination between the involved shippers, logistics services providers, authorities and other stakeholders. Information pertinent to cargo management involves aspects such as the origin and destination, contents, and status such as its current location of the cargo. Many applications and systems such as logistics execution systems (LES) have been developed for cargo management. Technologies for cargo location tracking such as RFID tags, location devices (GPS), presence sensors, and others have been also developed and integrated in the above systems (Dexler, 2008).

Despite such technological advances, some activities of cargo management are still performed manually, and there are misalignments between the different systems of the participants, as well as lack of transparent, up to date and accurate information about the cargo throughout the transportation chain. In other words, truly globally accepted standards for specifying cargo types, shipment points and load units (such as pallets, containers and so on) are still missing.

In this paper we identify the requirements for cargo management and we propose a Cloud based infrastructure that allows cargo tracking and monitoring across a transportation chain. The rest of the paper is organised as follows. Section 2 identifies business requirements for cargo tracking and monitoring. Section 3 proposes a Cloud based infrastructure that realises the previously identified requirements. The final section of the paper discusses how the approach described in this paper can contribute towards the realisation of the concept of 'intelligent cargo.

2 BUSINESS REQUIREMENTS FOR CARGO TRACKING

Systems for cargo management and monitoring need to include the previously identified stakeholders in the cargo management process, either as active participants, observers or both. At some point, a new stakeholder may become the active manager of the

Karakostas B..
TRACKING CLOUD ON THE INTERNET USING A CLOUD INFRASTRUCTURE.
DOI: 10.5220/0003646403880392
In *Proceedings of the 6th International Conference on Software and Database Technologies* (IWCCTA-2011), pages 388-392
ISBN: 978-989-8425-76-8

process. When, for example, the cargo leaves the shipper (customer) and becomes the responsibility of the carrier (transporter), the later becomes the active controller of the process, while the former becomes an observer who wants to keep track of status of the process.

Inter-organisational processes such as cargo transport and management have been the target of e-business technologies and systems such as EDI and EDIFACT for the best part of the last three decades. More recent e-logistics systems are XML based and provide Internet and web based services for freight transportation and management.

The problem that such systems face is that they represent the interests of a single stakeholder. Even when such systems provide interfaces to the other stakeholders through portals, APIs, or web services, such interfaces are controlled by a single stakeholder, usually a large transport service provider. Even community oriented cargo management systems are also effectively limited in this respect, because it is difficult to accommodate every potential stakeholder in the cargo management process.

The cargo business is characterised by a large number of smaller operator companies and by the lack of global IT standards. Multiple systems, interfaces and protocols must therefore coexist and interface with each other. A truly universal cargo management infrastructure can only be built on the principles of decentralisation, and peer to peer relations rather than on (portal or other based) centralised architectures.

Below, we identify requirements for a cargo management infrastructure and classify them across the categories of *identity, context, and security/ privacy.*

2.1 Identity

One of the main problems in cargo management is associating a single identifier with the cargo throughout the transportation process, and making such identifier available to everyone authorised. This identifier is the connecting link between the physical (cargo) world and the information system world. As in other e-business/ecommerce applications, identity management is therefore a key part of effective cargo management.

Cargo often undergoes physical changes as it is moves through different locations and means of transportation. It can for example, be repackaged or moved to different load units such as tanks (liquid) cargo or containers (dry cargo). A cargo management infrastructure must associate an identifier with the cargo it identifies, and persist that identifier for any desired period of time, regardless of changes to the cargo, its attributes, or its location on the transport chain.

Proposals for such identifiers exist, for example in the form of GSIN (Global Shipment Identification Number). GSIN is the GS1 organisation's Identification Key, used to identify a grouping of logistics units that comprise a shipment from one consignor to one consignee (buyer) referencing a despatch advice and/or Bill Of Lading (www.gs1.org). Identifiers such as the GSIN can be implemented as bar codes, or included within messages used in EDI and other logistics systems.

The problems however with approaches like this is that they require all parties systems to conform to the same encoding format. Also, such identifiers do not satisfy privacy requirements, as the identity of the sender or recipient can be inferred from the cargo identifier. Finally such identifiers do not convey other information about the cargo such as status/context, nor they indicate a way as to how such information can be obtained.

Thus, we establish the requirement that a cargo identifier needs to act as a direct key to an information source, e.g. a record, file, document etc. that contains cargo information. By 'direct key' we mean that there should be no need to obtain additional keys to access cargo information. Instead, the cargo identifier should yield access to the values of cargo properties and context variables (see next section).

As said above, a problem with cargo management is that cargo can change its physical characteristics as it is moved between different containers or gets repackaged. The ability for an identifier to persist independently from the loading unit containing the cargo is therefore essential.

2.2 Context

Cargo can be described by static properties (attribute variables) and dynamic properties that comprise its *context.* Cargo attributes are fairly static through the life of the cargo and include properties such as product code, description and values for its physical properties such as dimensions, weight etc.

Cargo's context is all the other entities that are associated with the cargo at some point in time. Since this set of entities is potentially enormous, for practical purposes, we need to restrict it to a more manageable subset that consists of other uniquely identified entities. Effectively then, context is

defined by entities that are related to the tracked cargo entity via a *containment* association. Thus, a cargo can be carried in a container (which is a uniquely identified entity) that in turn is carried by a truck (another uniquely identified entity), that is transported in a ro-ro ship (yet another uniquely identified entity).

Users should be able to employ context information to search for a particular cargo. Suppose that a user knows the identifier of the ship that carries the cargo but has no other searchable information about the cargo. Performing a search based on the ship's identifier will yield potentially a very large number of cargo items ('search hits'). The number of search hits will be significantly lower when we search using the truck's identifier, and even lower when searching by container identifier (assuming a container carries several cargo items).

Thus, another requirement refers to the ability to search for a cargo item by context, which however for practical performance reasons, needs to be restricted to a small subset of entities related to cargo. Searches should give indication of the number of potential 'hits' that a search by a particular cargo is likely to result in (similar to Google's number of search hits).

2.3 Security and Privacy

Identifiers play also a key role in security and privacy. In e-business, security requirements frequently require being able to verify the identity of the parties to a transaction. At the same time, privacy requirements often require that the parties not disclose any more information than necessary for the transaction.

Updating cargo information is essential, as such information may need to be corrected or updated, due to changes in context such as time, location and association with other entities.

One way to enforce security is to implement *views* of the cargo entity that only suitable authorised stakeholders have access to. Thus, a view can be defined for the cargo recipient, while another view can be defined for a Customs authority. However, these views must be audited for correctness ensuring that they only convey authorised information and cannot be altered without authorisation,

Another privacy requirement is that it should not be possible to infer information about cargo properties or stakeholders from the cargo identifier alone. Thus, it should not be possible to infer for example, who the shipper or received is, nor the contents of the cargo, from the identifier name, alone.

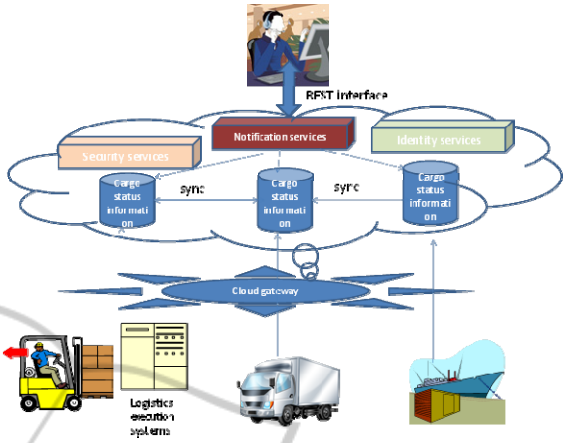

Figure 1: Cloud Infrastructure architecture.

3 A CLOUD INFRASTRUCTURE FOR CARGO TRACKING

In this section we propose a Cloud infrastructure for cargo monitoring. We use the term 'Cloud' to mean that the users of this infrastructure do not need to know where the cargo tracking services they use originate from, as they appear to originate 'somewhere on the Internet' (Vaquero et al, 2009).

As shown in Figure 1, the Cloud based cargo monitoring infrastructure is realised by a number of technologies such as sensor (e.g. RFID and GPS) networks that track cargo context, as well as by logistics execution systems that track movement of cargo in and out of warehouses. Such systems can update cargo status information through Cloud gateways. Gateways are points where a system that handles the physical cargo can access the Cloud and upload status updates. These updates are uploaded to clusters of replicating online databases that implement a common interface that follows the REST philosophy for manipulating resources on the Web (Fielding, 2000).

In addition, the above infrastructure provides identity management and security services. The company that registers a cargo with the system is issued with a global identifier (UUID) that is guaranteed to persist throughout the cargo transportation process. Authorisation keys are issued by the Cloud infrastructure allowing varying levels of access to information about the cargo. Thus a transport service provider is authorised for certain items of information such as the type of

cargo, but perhaps not the exact contents of the cargo. Cargo information can be accessed by using such identifiers and keys through any HTTP based systems, without needing to log on to dedicated portals or other proprietary systems browsers. Since they are based on the http protocol, all cargo tracking services can be invoked using a URI syntax such as

http://TOP LEVEL DOMAIN/<SERVICE NAME>/<SERVICE PARAMETERS>

where the top domain name is a fixed (unchangeable) URI that is assigned to the Cloud infrastructure by an authority such as ICANN. *<SERVICE NAME>* could be further qualified into subdomains if the potential space of cargo related services is large. A Cloud based directory of services should also provide information about the available services and be searchable using service metadata.

Directory search parameters can include the unique identifier of the cargo, and optionally the name of one of its properties (attributes/context variables).

For example, information about a cargo with UUID

"6E09886B-DC6E-439F-82D1-7C83746352B"

can be accessed using the following HTTP GET operation

GET

http://.../cargo/status/6E09886B-DC6E-439F-82D1-7C83746352B

This will yield a data structure such as in Table 1. This contains important information about the cargo such as sender and receiver, type and current status. Note that this representation is in JSON format (assuming it to be the default format of the Cloud infrastructure). Alternative representations e.g. in XML could be requested using syntax such as the following

GET

http://.../cargo/status/6E09886B-DC6E-439F-82D1-7C83746352B/_asXML

3.1 Cargo Registration Services

A user such as a shipper should be able to register a new cargo with the Cloud infrastructure by supplying the required parameters (using am HTTP PUT command) to the cargo registration service.

As explained above, the Cloud service should return a unique identifier for the cargo in the form of a UUID, i.e. an identifier that is guaranteed to be unique in the context of the transportation chain. The service also will supply the cargo owner with a digital key that certifies its ownership and is used to authenticate and authorise further operations.

Table 1: Cargo information structure.

```
{
"UUID" : "6E09886B-DC6E-439F-82D1-7C83746352B",
//the global unique identifier of the cargo
"consignor" : { "GLN" : 7300011234566},
//the GLN identifier, according to GS1 standard
"consignee" : {"GLN" : 7365566156190},
//same as for consignor
"consignment identification" : { "GINC" : 7365566156191234513}
// again according to GS1 standard
"pick up Date Time" : "200907151500-200907161200",
"cargo type" : {"UN/CEFACT" : "31"},
// Bottle gas according to UN/CEFACT classification
"transport payment method" : "WE"
//  (paid by buyer)
"total gross weight" : {"KGR" : 1500},
// weight in kilograms
"total gross volume" : {"MTQ" : 10},
// volume in metric tons
"status" : "dispatched",
...
}
```

3.2 Notification Services

Authorised users should be able to register with notification services for the cargo that they wish to track. A number of parameters should be attached to the service request that relate to cargo attribute or context variables such as location. The following example shows a request for notification for cargo with id: *6E09886B-DC6E-439F-82D1-7C83746352B*, when the cargo status becomes 'delivered'

```
http://.../notifications/6E09886B-DC6E-439F-82D1-7C83746352B?status=delivered
```

The Cloud infrastructure can operate several types of notification services, for example email,

SMS or URL callback ones.

3.3 Authorisation and Authentication Services

The owner of the cargo (i.e. the shipper, agent etc.) shall be granted full read access to the tracked cargo information including its attributes and context variables. Other users will be granted partial information based on their role in the transportation process. When another organisation takes over the handling of cargo, it shall be supplied with the UUID of the cargo (which, as said earlier, does not give access to cargo information unless the requester has a suitable key) as well as a digital key authorising operations (GET, PUT, DELETE) to certain cargo context variables. Thus, a carrier company is given permission to access (GET) cargo information such as physical properties (size, weight) and to modify (POST) context variables such as 'contained in' and 'status'.

National authorities such as port authorities and customs shall be given by the Cloud permanent keys that have read access to cargo information, if the cargo's destination or intermediate stop involves their jurisdiction.

Users who attempt to access or modify cargo information without sufficient authorisation shall be met with a HTTP 401 type error.

4 DISCUSSIONS AND FURTHER RESEARCH

Recent research in transport and logistics has proposed the concept of *intelligent cargo* (Schumaker et al, 2010). Intelligent cargo has the ability to self-identify, to detect its physical and organizational context, and to play an active role in transport processes, either by using own computational resources or by connecting remotely to web services platforms.

The infrastructure outlined in this paper contributes towards the realisation of the concept of intelligent cargo. In the Cloud architecture, the location of the services is transparent to their consumers, in other words users who wish to track the status of a cargo do not need to know which system holds such details. With current progress in embedded computer and network systems and sensors, the cargo tracking services described in the previous section could be implemented directly by the cargo itself (i.e. by a computer system embedded in the palette or container of the cargo), rather by some external logistics systems. Cargo could then communicate directly with its context entities (e.g. with containers, trucks etc.) using near field communications (e.g. RFID) and collaborate with them to carry out the transportation process. Of course, resilience and availability of such services are prerequisites, and the Cloud should provide additional functionality for service replication and backup.

In summary, this paper highlighted a Cloud infrastructure that will overcome current limitations of cargo management and allow seamless access to information and services about cargo to a large, heterogeneous and dynamic transportation chains.

ACKNOWLEDGEMENTS

Research reported in this paper has been partially supported by EU project E-freight (www.efreightproject.eu)

REFERENCES

Dexler, P. (2008) RFID Technology Can Help Manage Fleet Loads. *Business Fleet*, March 2008.

Fielding, RT (2000) *Architectural Styles and the Design of Network-based Software Architectures*. Ph.D dissertation, University of California, Irvine.

GSIN (Global Shipment Identification Number)
Available from http://www.gs1.org/barcodes/technical/idkeys/gsin

Schumaker, J., Gschweidi M., & Rieder, M. (2010) EURIDICE – An enabler for intelligent cargo for the logistics sector. *Journal of Systemics, Cybernetics and Informatics* (volume 8 - number 2 - year 2010, pages: 18-28)

Vaquero, L. M, Rodero-Merino, L , Caceres, J. & Lindner, M. (2009) A Break in the Clouds: Towards a Cloud Definition *ACM SIGCOMM Computer Communication Review*, Volume 39, Number 1, January 2009