View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by UPCommons. Portal del coneixement obert de la UPC

OmniaScience
Journal of Industrial Engineering and Management
JIEM, 2013 – 6(1):163-174 – Online ISSN: 2013-0953 – Print ISSN: 2013-8423
http://dx.doi.org/10.3926/jiem.668

A transportation security system applying RFID and GPS

Ruijian Zhang
Purdue University (USA)
zhang45@purdue.edu

Received October 2012
Accepted February 2013

Abstract:

Purpose: This paper is about developing a centralized, internet based security tool which utilizes RFID and GPS technology to identify drivers and track the load integrity.

Design/methodology/approach: The system will accomplish the security testing in real-time using the internet and the U.S. Customs' database (ACE). A central database and the interfaces and communication between the database and ACE will be established. After the vehicle is loaded, all openings of the tanker are sealed with disposable RFID tag seals.

Findings/value: An RFID reader and GPS tracker wirelessly connected with the databases will serve as testing grounds for the implementation of security measures that can help prevent future terrorist attacks and help in ensuring that the goods and products are not compromised while in transit. The system will also reduce the labor work of security check to its minimum.

Keywords: Modeling of Cargo Transportation, Radio Frequency Identification (RFID), Global Positioning System (GPS), Automated Commercial Environment (ACE)

1. Introduction

United States border security has become a major concern in the recent past. In order to enhance border security, a system must be put in place to allow the tracking of shipments from origin to destination. U.S. Department of Homeland Security requests proposals of cargo transportation security tools for U.S. Customs and Border Protection (CBP).

This project is to develop a centralized, internet based security tool which utilizes RFID and GPS technologies to identify drivers and track the load integrity. The system will accomplish the security testing in real-time using the internet and the U.S. Customs' database (ACE) (Auto-ID Center, 2011). A central database and the interfaces between the database and ACE will be established. After the vehicle is loaded, all openings of the tanker are sealed with RFID tags (E-seals). Then the RFID antenna and tag reader received and transmitted the signal, wirelessly connected with the databases. Also the GPS tracker traced the cargo's location at any time and reported to the system when necessary. This will serve as testing grounds for the implementation of security measures that can help prevent future terrorist attacks and help in assuming that the goods & products are not compromised while in transit. The system will reduce the labor work of security check to its minimum. It will also help in online billing.

This technology's two main focuses are private companies and the government. It can be used by a company to expedite the shipment and receiving process, streamline the billing and invoicing process, and to automate potential Federal Government container tracking requirements. The government can utilize this technology for shipping container validation, verification of load integrity, potential notification of special scenarios such as late or lost shipments, and as a tool to interact with the U.S. Customs and Border Protection's ACE database for border control (Auto-ID Center, 2011; AIDC 100, 2011; Battelle, 2003; Lee, 2005).

This paper is organized in five sections. Section Two describes the requirement specification and requirement analysis. Section Three elaborates the system design and implementation. Section Four analyzes the marketing potential of this produce. Finally, Section Five provides concluding remarks and the acknowledgements.

2. Requirement specification and analysis

The system (named Cargo Security System) consists of web-based software, servers, and databases. It accepts delivery orders from various employers and shippers, get them approved from the government if necessary, deliver them to the appropriate location and then send the response of successful delivery to the shipper or the source. A benefit of this system is that it will centralize all shipping system and will make it easier to track shipment from shipper to receiver safely with lesser amount of time needed.

The product is designed by keeping the track of cargo as viewed by the shipper, receiver and carrier. The product lets the shipper search and control his cargo through web. The carrier can create his own manifest and also go into the search details of the shipment and cargo. The product also includes the part which elaborates the significance of the government database (ACE) (Auto-ID Center, 2011). After creating a manifest the information is stored in the product database and the information is then sent to the government for authentication. The receiver can also search the cargo and will send the feedback to the shipper as soon as the cargo is received.

Shipper, carrier and receiver are the three user classes that are anticipated to use the product. From the technical point of view carrier has the privilege to view, edit and create the manifest. Each user class can search the information and view it. Only the valid users which have an authenticated password from the administrator can access the product.

The shipper will log on the system with a password and an ID provided by the administrator. The shipper will enter all the required information into the system for the carrier and the receiver. The carrier will now look at the information logged on and will make sure that there is no illegal means. A manifest will be created. Furthermore, an approval from the government is required. After the approval is made then the cargo will be shipped. Carrier will take the cargo to the receiver and will take the affirmation. Receiver will check the shipment ID and all the sent information about the cargo through shipper and then the receiver will send a feedback to the shipper about whether or not the cargo is intact or not. If there is a problem the receiver will notify both the carrier and the shipper and if there is no problem then the receiver will leave a positive feedback in the system (AIDC 100, 2011).

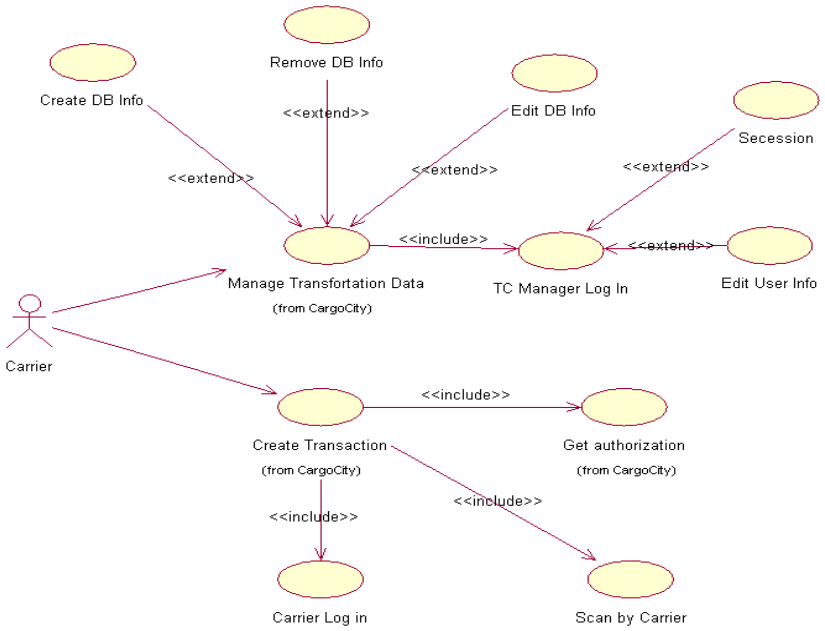

Figure 1. Use-case diagram shows the required activities of carrier

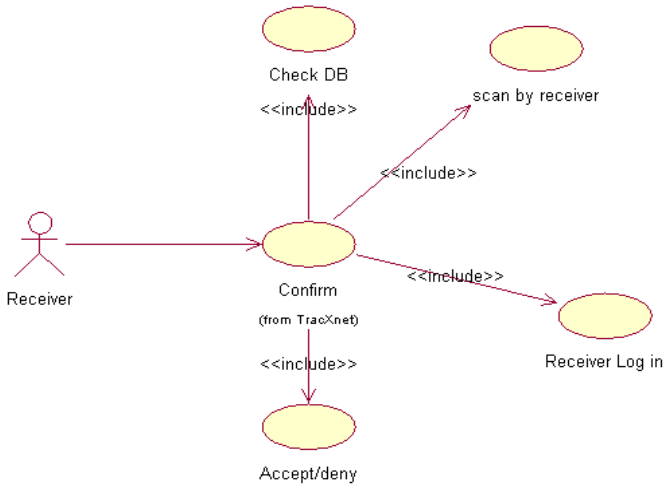

Figure 2. Use-case diagram shows the required activities of receiver

System security is an attribute that has the highest priority in the whole design of the product. The security is not only important from the programming point of view but also from the legal issues of national importance. The shipper will ship the cargo through a carrier by packing and sealing the whole stuff. The shipper needs to make sure that there is a proper record of all the shipment taken being approved by the government. The carrier needs to make sure that there is no falsehood being adopted while carrying the carriage to the receiver. Moreover, the receiver also needs to understand the security policy and should check the RFID tag in the E-seal based on the information received (Battelle, 2003; Lee, 2005).

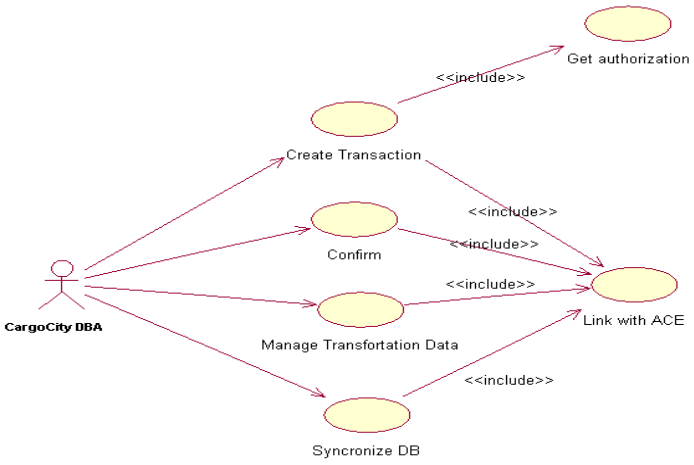

Figure 3. Use-case diagram shows the required activities of database administrator (DBA)

Cargo Security System is a product that goes hand in hand with security. Software architects need to pay special attention to the fact that no one should be able to access the product

without the authentication provided by the administrator. They have to make sure that there are no provisions for unauthenticated and unregistered cargo and user classes. The following three use-case diagrams in Figure 1 - 3 show the required activities of three actors: carrier, receiver, and the database administrator of the Cargo Security System.

3. System design and implementation

In order to help protect border security, it is essential that a system is put in place to enable tracking of dry and liquid bulk tank shipments from origin to destination. This project is to develop a centralized, internet based security tool to aid in the identification of drivers and the tracking of tanker truck load integrity. Cargo Security System will accomplish the security testing in real-time using the internet and the U.S. Customs' database (ACE). A central database, and the interfaces between the database and ACE will be established. The system is founded on the twin concepts of "central information storage" and "blind confirmation". This involves driver and load information that is centrally stored and controlled by the system as an unbiased third party and verified with end users on a "need to know" basis. The system will verify driver, tractor and trailer identification. It also tracks the integrity of load by verifying the e-seals that are put on the vehicle's opening.

We applied RFID technologies in Cargo Security Systems (Lee, 2004; IBM Corporation,2004; Denning, 2004; Richardson, 2004). This is an automatic identification method (Chen & Lee, 2007; McQueary, 2004; Waldner, 2008), relying on storing and remotely retrieving data using devices called RFID tags, which is placed as e-seals to the cargo transportation vehicles (Figure 4):

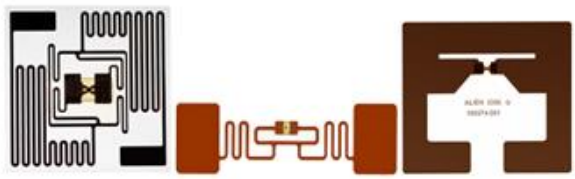

Figure 4. RFID tags

In Cargo Security System, the vendors place RFID tags on all shipments for the purpose of identification using radio waves. These tags were used as E-seal (Figure 5). We applied "ISO 18185", which is the industry standard for electronic seals for tracking cargo containers using the 433 MHz and 2.4 GHz frequencies.

Passive tags, among the three general varieties (passive, active, and semi-passive), were chosen for Cargo Security System, because passive tags require no internal power source and they are only active when a reader is nearby to power them. That property makes tags more

stable, which is important for cargo transportation. Our E-seals contain two parts. One is an integrated circuit for storing and processing information, modulating and demodulating a RF signal. The second is an antenna for receiving and transmitting the signal. E-seals have no internal power supply, the minute electrical current induced in the antenna by the incoming radio frequency signal provides just enough power for the CMOS integrated circuit in the tag to power up and transmit a response. The transmitted response received from an E-seal will be a 128-bit unique ID number that will correspond to the cargo's ID number within the Cargo Security Systems database.

Figure 5. E-seals

In Cargo Security System, "triple layer securities" has been created. The first security layer is the information pair that is stored with the CBP ACE database. That information pair is the "e-manifest", which stores and bounds a ciphered E-seal number with the cargo information which includes manifest, driver, passenger etc. The second security layer resides with the backed information pair stored in the Cargo Security System database. The third security layer is the secured transmission of the e-seal's ID. When a shipment of cargo crosses the border, E-seal wirelessly transmit a 128-bit unique ID number which is hard coded into the E-seal as part of the manufacturing process. The unique ID in the E-seal cannot be altered, providing a high level of security and authenticity to the E-seal and ultimately to the items the E-seal may be permanently attached or embedded into. When cargo is about to be delivered to a warehouse, installed readers will be reading information inside E-seal, and possibly compare the E-seal's information with one stored on the Cargo Security Systems database or ACE (Figure 6).

Due to the fact that there will possibly be many E-seals associated with a cargo's container, the readers may need to select which E-seal is to be read from among many potential e-seals, or the readers may wish to probe surrounding devices to perform inventory checks. Cargo Security System implements a tree-walking singularize algorithm, resolving possible collisions and processing responses one by one. We applied a secure tree-walking algorithm such as Class 0 or Class 1 UHF.

We built a RFID middleware, which is used to finish information manipulation and communicate through the reserved ports between Cargo Security System and the RFID hardware. Unlike most of the current enterprise RFID applications in the United States which have supplied a middleware between the legacy systems and new added RFID technologies, we built a middleware by use of the API (application program interface) which is suited with our system's java platform, rather than using an existing commercial middleware. This middleware has sufficient functions for RFID manipulation and is well-connected with the Cargo Security System.

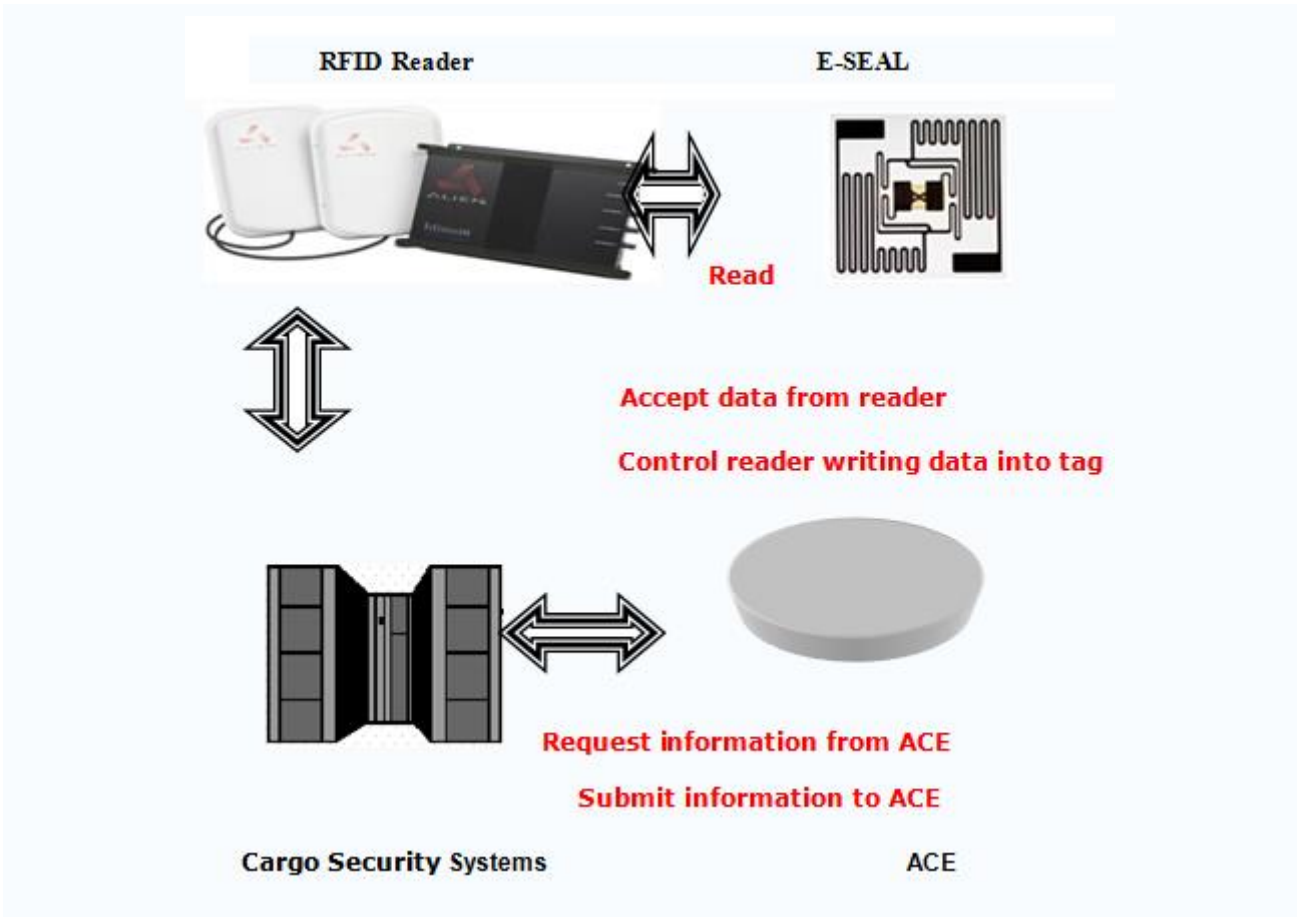

Figure 6. Cargo Security System structure

After the vehicle is loaded, all openings of the tanker are sealed with E-seals. At the time of departure, the security E-seals are read by the RFID wirelessly. This information, along with the driver's ID, the tractor ID and the trailer ID, will be transmitted in real time over a secured internet link to the Cargo Security System database. The driver may then proceed to the destination. When pass the border of United States or upon arrival of the destination, the RFID facility will read the E-seals wirelessly. The system will then prompt the official of the U.S. CBP or the receiver with an online photo in real-time to verify the driver's identity. Upon verifying each of the remaining security E-seals, the load is looked up in real time over the internet on the database. The system will generate "OK" or "Not OK" status messages to confirm the

integrity of the shipment. After successful verification of all E-seals, the official of the U.S. CBP may allow the cargo to pass the border or the receiver may accept the shipment and allow the vehicle to be unloaded. The RFID facility wirelessly connected with the databases will serve as testing grounds for the implementation of security measures that can help prevent future terrorist attacks and help in assuming that the goods & products are not compromised while in transit.

We applied GPS technology for tracing cargo transportations so that the related parties could know the current position where the cargo is. An interface enabled GPS devices communicating with the GPS tracker hardware to update current location of the cargo. The security system can track, monitor, and manage each cargo remotely in real-time, at all time. Currently, the system could track up to 500 cargo transportations on a single map, easily communicate with and reroute vehicles from the related parties through Internet. Through the location management of the GPS tracker, the server inserts the locations of cargos on real time into the database and shows them on a map at the front end. Visualization of historical data for particular cargo transportation could be superimposed on an interactive map. The best functionality is that we combined the leverage of RFID and GPS technologies into one system.

Modeling of cargo transportation is very important for this system. The project is split to four modules: database; RFID; GPS; interface and the communication through Internet. The database module is the module which defines what, how, and where to store the cargo information in the database. The tool we use for developing the database module is the state-of-art database software, IBM Rational Rose. The RFID module automatically verifies driver, tractor and trailer identification through visualized ID recognition. It also tracks the integrity of load by verifying the E-seals that are put on the vehicle's opening. The GPS tracker module traced the cargo's location at any time and reported to the system when necessary. The interface module includes the electronic formats of forms which transportation companies report to U.S Customs on the border, and the user interface dialogs between drivers, transportation company staffs and the database. The communication between our database and the U.S. Customs' database is through Internet.

The project is implemented on Intel Core 2 Duo processor with IBM Rational Suite as component based software development tools. The languages and tools we employed also include: Java, Html/JavaScript, JSP, JDBC/ODBC, and Tomcat4.1 for compile JSP files. We apply ANSI X.12 as information communication standards connecting between the Cargo Security System database and ACE. The system is described in Figure 7 below.

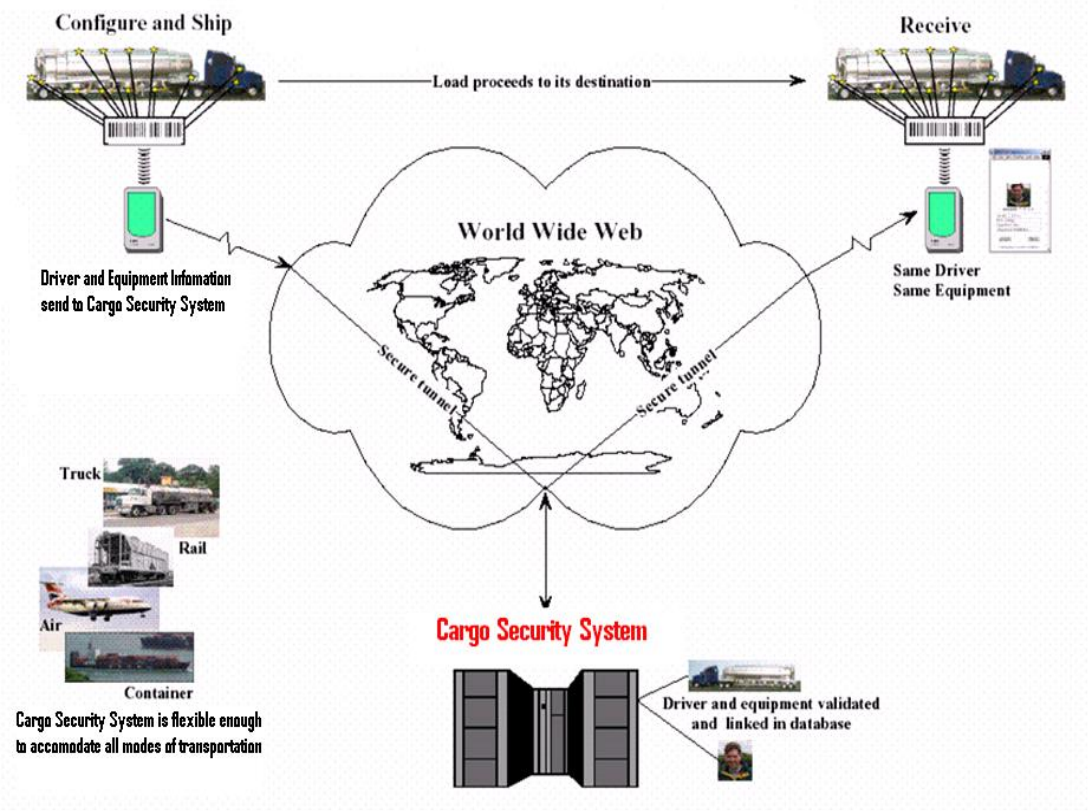

Figure 7. The system functionalities

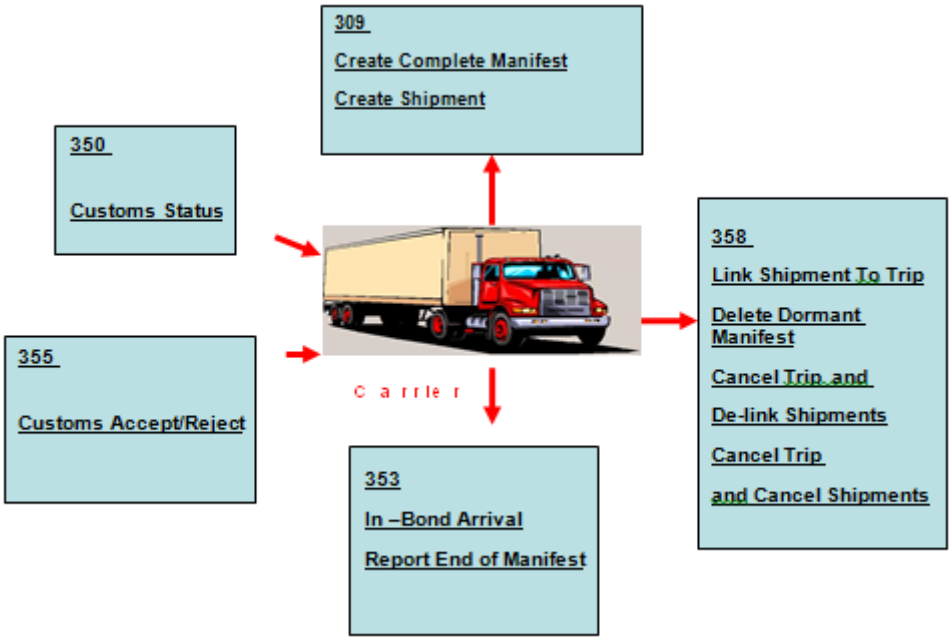

Figure 8. Manifest filing using EDI

Figure 8 shows the messages transmitted between our database and the U.S. Customs and Border Protection (CBP). Figure 9 shows the communication through the internet.

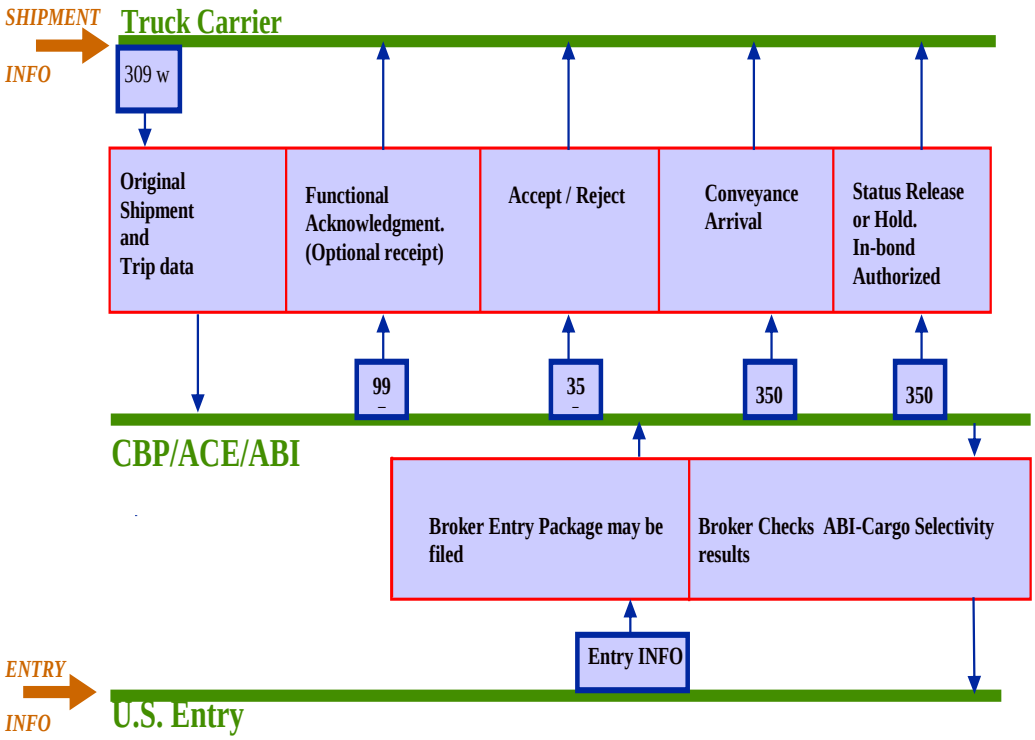

Figure 9. Communication through the Internet

The codes of the manifest filing using EDI are explained as following:

- Messages transmitted to the U.S. Customs and Border Protection (CBP).
  - 309 Complete Manifest or Preliminary Shipments
  - 358 Truck Manifest (Trip/Consist)
  - 353 Event Advisory Message (Trip Commit)
- Messages transmitted from the U.S. Customs and Border Protection (CBP).
  - 997 Functional Acknowledgement
  - 355 CBP Acceptance/Rejection
  - 350 CBP Status Information

4. Marketing potential of the system

The September 11th attacks and all the related catastrophic events are forcing all of us to take a very careful look at how we manage and take care of our security. As, United States being the center of all business activities in North America, many illegal activities are performed

across the border. Even the interstate and local businesses could be compromised during the transportation of goods. Therefore, U.S. Department of Homeland Security requests proposals of cargo transportation security tools for U.S. customs and border protection.

This technology's two main focuses are private companies and the government. It can be used by a company to expedite the shipment and receiving process, streamline the billing and invoicing process, and to automate potential Federal Government container tracking requirements [Auto-ID, 2011; AIDC 100, 2011; Battelle, 2003; Lee, 2005; Karkkainen & Ala-Risku, 2003). It will serve as testing grounds for the implementation of security measures that can help prevent future terrorist attacks and help in assuming that the goods & products are not compromised while in transit. The system will reduce the labor work of security check to its minimum. It will also help in online billing. The government can utilize this technology for shipping container validation, verification of load integrity, potential notification of special scenarios such as late or lost shipments, and as a tool to interact with the U.S. Customs and Border Protection's ACE database for border control.

5. Concluding remarks

In order to enhance border security, we have developed a centralized, web-based database system as a cargo transportation security tool, which utilizes RFID and GPS technology to identify drivers and track the load integrity. There is a great potential that this technology will be applied by the transportation companies and the U.S. government. It will make the security check and the shipment and receiving process faster and easier.

Acknowledgment

The project is sponsored by the Task Technology Innovation Grant of Purdue Research Foundation. Several groups of undergraduate and graduate students participated in the software development.

References

AIDC 100 (2011). Professionals Who Excel in Serving the AIDC Industry". Retrieved 2, August, 2011.

Auto-ID Center. (2011). The New Network. Retrieved 23 June 2011.

Battelle (2003). Federal Motor Carrier Safety Administration: Hazmat Safety and Security Field Operational Test Task 4: System Requirements and Design, July.

Chen, P.S., & Lee, J. (2007). RFID solution applying on freight container security management", Proc. Stockholm-Taipei 2007 International Conflict Management Conference, March 2007.

Denning, M. (2004). CBP and Rick Davenport, eCP: "ACE Development and Trade Engagement", June 30.

IBM Corporation (2004). Team Focus Facilitation Services: "U.S. Customs and Border Protection Trade Support Network, e-Manifest: Trucks", November 10.

Karkkainen, M., & Ala-Risku, T. (2003). Department of industrial and Management, Helsinki University of Technolog, Finland: Automatic Identification: Applications and Technologies.

Lee, H.L. (2004). Coping with Security Costs of Terrorist Threats to Supply Chain Management", Standford, U.S.A.

Lee, H.L. (2005). Higher Supply Chain Security with Low Cost: Lessons from Total Quality Management. *International Journal of Production Economics*, 96(3), Standford, U.S.A. http://dx.doi.org/10.1016/j.ijpe.2003.06.003

McQueary, S. (2004). Brown Line Inc.: "Participation of Smaller Carriers", American Trucking Associations EDI workshop, July.

Richardson, M. (2004). UPS: "How Large Carriers May Participate In ACE", American Trucking Associations EDI workshop, July 2004.

Waldner, J.B. (2008). *Nanocomputers and Swarm Intelligence*. London: ISTE John Wiley & Sons. 205–214. ISBN 1-84704-002-0. http://dx.doi.org/10.1002/9780470610978

.

El artículo está con Reconocimiento-NoComercial 3.0 de Creative Commons. Puede copiarlo, distribuirlo y comunicarlo públicamente siempre que cite a su autor y a Intangible Capital. No lo utilice para fines comerciales. La licencia completa se puede consultar en http://creativecommons.org/licenses/by-nc/3.0/es/