Volume 7 • Issue 4 • 2015
pages: 54-64

Application of Internet of Things in Logistics – Current Challenges

received: 21 September 2015
accepted: 30 September 2015

Paweł Tadejko

ABSTRACT
In this paper, some aspects of modern logistics related to the Internet of Things technology were studied. Internet of Things can overcome shortcomings of some areas of logistics, for example monitoring, production management, efficiency of logistics operations, information, exchange and communication, modeling supply chains, intelligent information collection and security. This paper describes some principles and characteristics of Internet of Things, and briefly discusses the application of it in modern logistics. Logistics has come to a new stage with the development of Internet of Things technology. The current application areas and future prospects of this technology are analyzed in this paper. Difficulties encountered in the implementation show that the IoT technology needed to be further improved. However, despite many difficulties, experts believe that the key are not problems of costs, standards and techniques, but the formation of a profitable business model in the logistics industry.

KEY WORDS
Internet of Things, modern logistics, standardization, architecture, security, privacy, interoperability

DOI: 10.12846/j.em.2015.04.07

Corresponding author:

Paweł Tadejko

Bialystok University of Technology
Faculty of Computer Science

e-mail:
p.tadejko@pb.edu.pl

Introduction

Internet of Things (IoT) represents the next step towards the digitization of our society and economy (Rose, 2015), where objects are interconnected through communication networks and exchange information about their status and/or the surrounding environment (Fig. 1). Paradigm „always connected" is one of the feature of IoT. Technology can be very useful in logistics where every object is uniquely identified, and accessible to the network, its position and status known, and where we have special software services.

Modern logistics includes a lot of characteristics, such as systematic industry, combination of logistics and information technology, technology modernization, integration of supply, integration services, a full service and network architecture of logistics system (Chuanyu, 2009; Shaoai, 2009).

The key technology of each path are: sensors, intelligent chips and wireless transmission network. Therefore, the core is identification device, which means using some technique through the internet protocols to achieve automatic recognition and communication. Nowadays the most popular device is RFID (Radio-Frequency Identification). Over the last decade RFID went on to become a useful tool in retail, logistics, healthcare and a handful of other enterprise sectors (Bisk Education, 2012; Harropm, 2006; Das, 2015).

Reports suggest that RFID is fast taking over the world, but the recent Beacon technology may change this situation by giving for businesses new possibilities. However, the market for RFID tags and systems will rise rapidly in the next decade, because RFID devices still have some advantages over Beacons (Girish, 2015).

Internet of Things systems require each device to be embedded with a unique digital tags with its detailed specifications. Using the special system to read or write the information, and then through wireless data communication network send to other

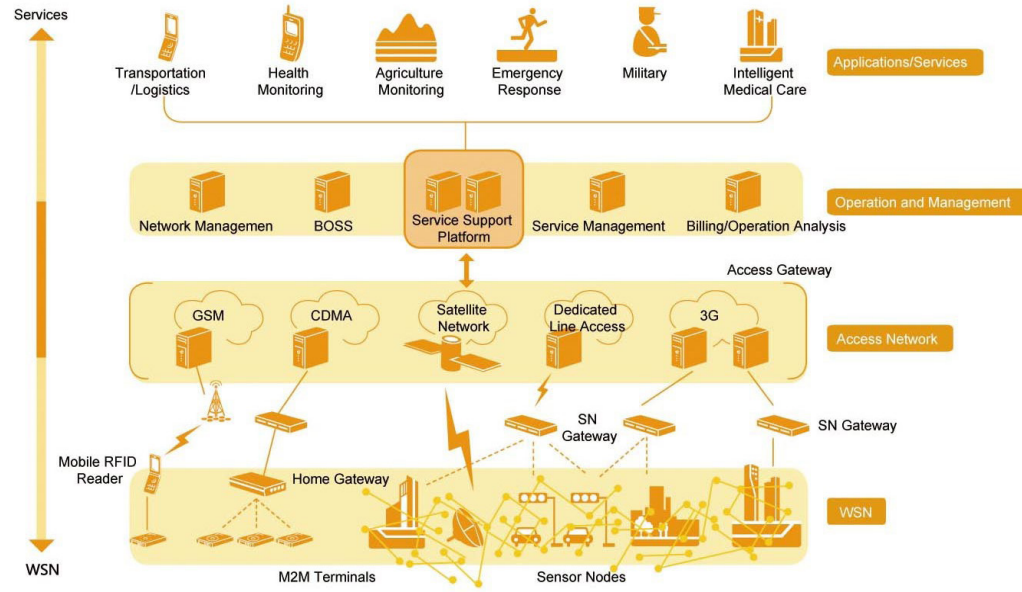

Fig. 1. Framework of the Internet of Things and surrounding environment
Source: (Wanpeng, 2010)

systems. The Internet of Things requires new level of interoperability. This means that IoT requires standards to enable horizontal platforms that consist of special middleware in fields of communication, operation, and programming across devices of different manufacturers, or even industry.

For the past six years, the European Commission has been cooperating actively towards the development and further deployment of the IoT technology. In March 2015 body initiated the creation of the Alliance for Internet of Things Innovation (AIOTI), (AIOTI, 2015). This alliance flags the intention of the European Commission to work closely with all stakeholders and actors of the Internet of Things. Very important role in this scenario plays new idea – the Digital Single Market. DSM (DSM, 2015), adopted in May 2015, leads Europe a step further in accelerating developments on IoT. The DSM consolidates initiatives on security and data protection, which are essential for the adoption of this technology. Most importantly, it announces an initiative on the Data economy (free flow of data, allocation of liability, ownership, interoperability, usability and access) and promises to tackle interoperability and standardisation.

The Internet of Things in the physical world is basically a network of digitally enabled communicating devices, products and services. Domestic appliance, cars, stores, and bus stops, everything will soon have not only connection to the Internet, but also special software with services on board. Research firm Gartner predicts that by 2020 we will have 26 billion smart and connected products in use. This translates to an average of 3.3 devices per person (without smartphones and tablets). What are devices capable of? Nowadays, most systems simply transmit pre-programmed data, but there are devices that transmit data about what they are able to sense and there are „things" that can autonomously respond to changes in their environment. These higher level of interoperability presents a new range of consumer touch points and opportunities for personalization and hybrid shopping in retail. This means that offline retail stores are increasingly moving towards the cloud as well. This calls for designing hybrid customer journeys that work simultaneously offline and online (Bosavage, 2015).

1. Development of the IoT – Application in Logistics

The rapid development of modern logistics used platform based on the RFID technology is the results from few things. RFID technology is a simple, cheap and secure solution. Internet of Things can go beyond it because can provide accurate flow of information of products in market to provide a reliable basis for logistics market analysis, forecasting and decision-making (Ruan, 2012).

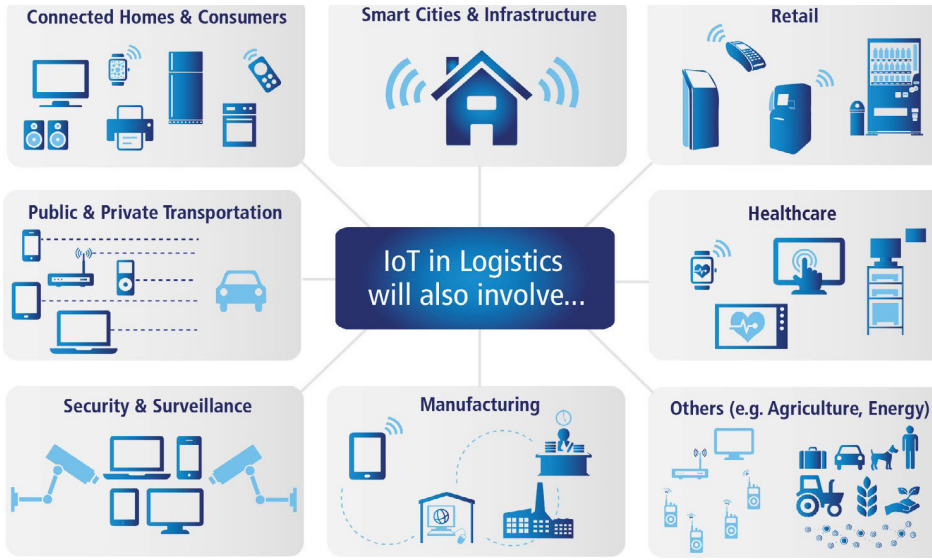

Fig. 2. The Internet of Things Ecosystem
Source: (Improving T&L, 2015).

Internet of Things is a network connecting anything with the Internet to exchange information and communication, to realize intelligent searching source, identification, location, tracking, monitoring and management. IoT and related technologies have strong connection with service-oriented architecture – SOA (Yuqiang, 2010). The facts makes the recommendations for designing a new-type logistics business processes by applying the IoT technology based on the supplying chain perspective. The IoT has many positive impacts on every stage in the global logistics supply chain, starting from the manufacturing stage all the way, to the retail stage (Fig. 2). It makes better visibility of supply chain, tracks deliveries in real time, improve a data accuracy and thus provides the ability of faster exception management.

Standardization of technologies related to IoT is very important, as it will lead to better interoperability, thus lowering the entry barriers. Currently, many manufacturers are creating vertical solutions (a slice in the IoT application space), using their own technologies and inaccessible services. Standards need to be created to change this „Intranet of Things" into the more complete „Internet of Things". As yet, no holistic approach to IoT has been proposed; coherent concepts that unify IoT do not exist, leading to silo solutions that do not support interoperability (Rose, 2015; Bassi, 2013). This approach is an extension of the single device-to-cloud communication model, where „IoT devices upload data only to a single application service provider".

Many industries and business sectors try to use the possibilities of data-driven technology, but companies in transport and logistics are way ahead. By their very nature, the logistics providers that move objects by modes of transport have widely distributed networks and take part in rapid information distribution about states of devices. As a result, they were quick to see the benefits of new kinds of sensors, connection technology and service oriented architecture.

Using mobile technologies and the Internet of Things, enterprises can accelerate productivity, profitability and operations with solutions designed specifically for their processes. Building solution where enterprises can connect all devices across a distributed network, capture and share their mission-critical data, allowing them to show real-time view of all operations (Tab. 1), (Boost to C&L, 2015). By leveraging convergence of the above mentioned trends, transportation and logistics can dramatically improve the following areas:

- End-to-End Visibility – complete visibility facilitates more effective, timely decisions and reduces delays through quicker detection of issues;
- Warehouse and Yard Management – with IoT-enabled mobile devices designed to track inventory data, equipment and vehicles, enterprises can give their physical assets a digital voice;
- Fleet Management – with mobile scanners, computers and RFID systems alone, enterprises can gain visibility into their assets and better streamline operations to keep their fleet moving.

Tab. 1. Transport and Logistics Internet of Things framework

Improvement Area	Improvement Area Description
Sensing and shaping	• Information capture across various nodes of a supply chain • Environmental monitoring aspects
Adaptive supply	• Interpretation of captured information; • Decision aid based on analytics; • Act on changed environment to orchestrate connection across supply chains
New business opportunities	• Continuous improvement based on continuous captured information • New business model generation possibilities based on X-as-a-service • Ecosystem partnership to enable wider market reach with lower levels of investment

Source: author's elaboration on the basis of (Deloitte University Press, 2015).

Companies in this sector made use of data-driven technologies related to the Internet of Things in many ways. Specific applications include the real-time tracking of shipments, warehouse-capacity optimization, predictive asset maintenance, route optimization, improved last-mile delivery, and more. But there are many more capabilities of IoT applications for transport and logistics providers. Through a rapidly increasing number of connected devices, embedded sensors, and analytics technologies, companies in the sector can enjoy unprecedented visibility into almost every aspect of their business, from operations to finance (Koomey, 2012). This real-time visibility will allow transport and logistics providers to explore more effectively and intelligently their rich and complex database, leading to more efficient use of resources, better engagement with customers, and more informed decision making.

Beacon technology consist of a device with special software and can help drive shoppers to those „smart" shelves. One of the most important advantages IoT that shops have is the tremendous amount of customer information they can mine and analyze to provide more tailored and streamlined shopping experiences. Beacons can may offer more targeted (personalized) content onto displays of our mobile devices within the stores whenever they are triggered. Inside a smartphone app, shoppers can define personal shopping preferences – for example, food preferences and allergies. Every time when they enter a store, their phones will connect via Bluetooth to smart displays located underneath products on store shelves. Beacons can be a big part of the near future of retail. Beacons are not the same as RFID, because can interact with environment and can also collect the data.

Machine-to-Machine (M2M) communication has attracted considerable attention in research and from the perspective commercial operators offer services within the domains of fleet management, logistics, home automation and so on. Domain of Internet of Things is starting some kind of revolution of M2M (Alam, 2013). The M2M solutions provided today mostly reside on vertical platforms – silo solutions – servicing only one specific vertical system. IoT is much broader when considering wireless with wired connectivity. Looking at IoT it is lacking behind M2M with only few business cases such as systems of RFID tags in supply chain management and logistics. New IoT platforms on the market today are better addressing the market problems from a M2M silo architecture perspective (Alam, 2013).

2. Main challenging domains of the IoT

For IoT to achieve its vision, a number of challenges need to be overcome (Croll, 2015; Wanpeng, 2010; Bauer, 2015). These challenges range from applications, contextual to technical. A world where all things are connected, communicating information and data about its local environment are send to a distributed cloud computing opens the door for less security and privacy. There are new areas where privacy needs to be protected. Principles of data confidentiality and security must be safeguarded. Governance in the IoT is crucial.

The idea of a globally interconnected continuum of devices based on RFID technology has considerably been extended to the current vision that envisages a plethora of heterogeneous objects interacting with the physical environment. Today, a large number of different means are used to enable communication between heterogeneous devices.

One significant aspect in IoT is the large number of devices being connected to the Internet, each one exchanging data. Finding ways to reliably store and

Tab. 2. Major challenge areas of Internet of Things

Challenge Area	Challenge Area Description
Privacy and Security	IoT presents significant challenges in terms of who can see what with which credentials Millions of devices will create a whole new security landscape as enterprises attempt to protect themselves, it will also create new opportunities for operational technology security providers
Standardization and Interoperability	How do we make sure that the hugely diverse technology platform continues to act in a platform manner? Appropriate standards, reference models, and best practices also will help curb the proliferation of devices that may act in disrupted ways to the Internet
Large data sets – „big data"	There are many of the key challenges similar to large scale data. How do we deal with the data stream of billions of „actors"? How do we ensure the data remains usable? Where is all the data provided by those processors going to be stored and what are the problems around them – processing, analysis, data exploration?

Source: author's elaboration on the basis of (Alistair Croll – O'Reilly Radar, 2015; Wanpeng, 2010; Bauer, 2015).

interpret the masses of data through scalable applications remain a major, not only technological, challenge (Tab. 2).

We can also show fields of challenges from other point of view. The concept of the IoT is the multidisciplinary study that involves the research in the fields of hardware, communication, networking, data flow and software engineering (Tab. 3).

The individual's trust in the IoT should be fundamental and complete, knowing that information will not impact negatively on any individual or society. Factories and industrial facilities will use the IoT in completely different ways. Considering the advantages of IoT, overall architecture of the IoT -enabled manufacturing execution system provides a new paradigm by extending the IoT to manufacturing field. Under this architecture, the manufacturing things, information sharing fleet management and other can be embedded with sensors to interact with wide range of sensors and other IoT systems. The real-time data driven monitoring and optimization for IoT-based sensible systems can be achieved to improve productivity and quality, reduce the wastes of manufacturing resources, cut the costs in logistics, reduce the risk and improve the efficiency in transportation, and improve the responsiveness many tasks (Zhang, 2013).

2.1. Device discovery standards and Protocol translation

The way IoT devices are discovered, managed, data is reported and authentication is done should be interoperable using standard protocols. Ideally, any IoT device should be able to communicate with any application or service. Devices but also applications as well need to talk to each other (Bosavage, 2015). Checking the weather, doing banking operations, looking at my Endomondo runs, getting my medical information. The source of data are not only devices but everything you interact with. They enable devices to be discovered, they broadcast their capabilities and interact with others in standard ways (Schneider, 2013; Bassi, 2013). The IoT needs many protocols. Perhaps it is easiest to categorize them along a few key dimensions: Quality of Service, addressing, and application. We have devices speaking MQTT, some XMPP, some CoAP, some DDS, some proprietary

Tab. 3. Major fields of challenges of Internet of Things

Field od Challenge	Fields of Challenge Description
Technology level (Interface between the real and digital worlds)	Challenges linked to the integration of smart 'network enabled' objects under strong energy and environment constraints, communication technology – wireless technologies
Network level (Data and Transmission)	Challenges linked to the massive secure and dynamic and flexible networking and the ubiquitous service provision
Application level (Intelligence level)	Challenges linked the data flow and service discovery where data collected by individual smart 'network enabled' objects such as wireless sensors are enquired by distributed users

Source: author's elaboration on the basis of (Croll, 2015; Wanpeng, 2010; Bauer, 2015).

protocols. Inside those the data format may even be different. Translating those protocol to something standard either through JSON, XML or RESTFul APIs is going to be key (Schneider, 2013).

2.2. Interoperability – Fragmentation and Silos

Interoperability is a critical source of value in IoT systems. One of the most important things of interoperability in generating maximum value from IoT applications. Much of the data collected by sensors today is used to monitor discrete machines or systems. Individual equipment manufacturers collect performance data from their own machines and the data can be used to schedule maintenance. Interoperability would significantly improve performance, costs, effectiveness by combining sensor data from different machines and systems to provide decision makers with an integrated view of performance across an entire factory or between different systems.

The Internet of Things is becoming the Internet of Everything, connecting people, processes, data, and things at unprecedented scope and scale. Despite the many concerns around privacy and security, a poll by IoT Nexus found that interoperability was seen as the biggest challenge to the IoE by 77% of respondents. Research by McKinsey suggests that 40% of the value of the IoE will need to be unlocked via interoperability (Manyika, 2015). Given the potential benefits, and the previous interoperability challenges faced by IT, it may seem surprising that it continues to be a problem. Main reason for that is a lot of the applications that have been created. Most of them have been created as a stand-alone systems and often it is in their interest not to build open systems. Great examples are Smart Cities and Transport and Logistics solutions. Design IoT solutions should use IoT Architectural Reference Model or something similar concepts (Bassi, 2013). The Lighthouse Project IoT-A proposes the creation of an architectural reference model for the IoT as well as the definition of a set of key building blocks to lay the foundation for a ubiquitous IoT (European Lighthouse Integrated Project, 2013).

2.3. Security

Security and privacy protocols are very important issues when it comes to the Internet of Things space. There are some wide known standard like Online Trust Alliance (OTA) published a draft trust framework specifically for Internet of Things devices that entails specific best practices for data privacy and protection manufacturers should follow. The Framework is a comprehensive global initiative that provides guidance for device manufacturers and developers to enhance the security, privacy and sustainability of connected home devices, wearable fitness and health technologies, and the data they collect (FTC Staff Report, 2015).

According to a press release, this framework could pose as the building blocks of a certification program among manufacturers of IoT devices. To address the problem Online Trust Alliance established the IoT Trustworthy Working Group (Online Trust Alliance, 2015), as a vendor neutral multi-stakeholder initiative. The group recognizes that „security and privacy by design" must be a priority of product development. Sustainability incorporates the life-cycle issues related to transfer and processing of collected data.

2.4. Privacy

Furthermore Internet of Things technology enables a whole new context for smart objects. Even RFID putting an identification label into every object, but Beacon enables a smart system to collect the data interact and exchange information. Information retrieved from such an object, turns it into a potential smart objects. If security problems are suitably treated, they will most probably be able to connect to the global Internet. This way, one can get an ubiquitous framework to access, monitor and control many systems of those smart devices over an Internet (FTC Staff Report, 2015).

There is a special field of IoT – Mobile Health (mHealth) with rapidly growing sector stemming out of the convergence between healthcare and ICT (European Data Protection Supervisor, 2015; Harropm, 2006). It includes mobile applications designed to deliver health-related services through smart devices often processing personal information about health, lifestyle and well-being information. Medical context enables a rapid and precise identification and quick access to Personal Health Records over an IoT. The use of smartphones with Internet access turns this whole context into many mobile healthcare systems. The mHealth market is complicated because many public and private operators are active at the same time, for example app

developers, devices manufacturers and advertisers, and there are many business models with fast changing conditions (Mobile Health – Reconciling, 2015).

2.5. Collecting IoT data – really Big Data

Companies need to collect most of the data because that is relevant to their business and that is a seriously challenging task. Furthermore they need to filter out redundant data and also protect the data from getting attacked. This requires highly efficient mechanism that includes software and protocols (Croll, 2015).

The most common data collection tool is the devices with special sensors. Data collection process in field of IoT also requires particular protocols. Message Queue Telemetry Transport (MQTT) and Data Distribution Service (DDS) are two of the most comprehensive protocols. Both protocols can help devices connect with real-time machine-to-machine (M2) networks. MQTT collects data from multiple devices and puts the data through the IT infrastructure. On the other hand, DDS distributes data across devices.

IoT deployments will generate large quantities of data that need to be processed and analyzed in some cases real time. Processing large amount of data in real time will increase workloads of data centers, leaving providers facing new security, capacity and analytics challenges. This is where knowledge discovery in databases and data mining technologies come into play. These technologies (called sometimes machine learning or deep learning) provide possible solutions to find out the information hidden in the data of IoT. Next knowledge can be used to enhance the performance of the system or to improve the quality of services (Tsai, 2014).

2.6. Legal, Regulatory and Rights

The use of IoT devices raises many needs of regulations and legal questions as well as amplifies existing legal issues around the privacy and personal data processing. The questions are wide in scope, and the rapid rate of change in IoT technology outpaces the ability to adapt. Gartner said cybersecurity and privacy concerns are the main obstacles to IoT adoption. A report by the U.S. Federal Trade Commission enumerated the risks of a standard-less IoT: enabling unauthorized access and use of personal information, facilitating attacks on other systems and endangering personal safety (Cline, 2015).

Companies need to get ahead of the inevitable fearmongering and back a minimum set of privacy standards that addresses the core concerns of IoT users. Other industries have successfully taken a similar self-regulatory approach, such as the mobile-marketing industry's „Mobile Application Privacy Policy Framework", automaker industry's „Consumer Privacy Protection Principles for Vehicle Technologies and Services" and agribusiness sector's „Privacy and Security Principles for Farm Data".

In October 2014, Europe's Article Working Party (WP) published Opinion 8/2014 on the Recent Developments on the IoT. While the Opinion is based on the current Data Protection Directive 95/46/EC, many of the legal solutions and recommendations are taken from concepts proposed in the draft EC data protection regulation (95/46/EC, 1995; 2002/58/EC, 2002). The Opinion establishes that European data protection law applies even if the data controller is outside of the European Union.

The US regulator has adopted similar non-binding guidance. In January 2015, the Federal Trade Commission (FTC) released a report on „The Internet of Things: Privacy and security in a connected world" (FTC Staff Report, 2015), which provides a „series of concrete steps that businesses can take to enhance and protect consumers" privacy and security.

2.7. Issues strictly addressed to Transport and Logistics

Some techniques based on IoT can help manufacturing execution system to solve real-time data driven optimization among each manufacturing system layer. Most key components of T&L systems can be designed to track and trace the real-time information of the manufacturing things such as operators, machines, pallets, materials and so on. The dynamical optimization of the production process could be possible in new way if we can use the real-time manufacturing information coming from IoT sensors. The objective of dynamical optimization is to analyze and quickly adjust the production control parameters based on information from IoT devices. The most important challenge is how to establish an reference architecture for IoT-based manufacturing execution system to apply the conception of IoT to manufacturing field and build up a referenced real-time information capturing and integration framework (Zhang, 2013).

However, although companies are aiming to implement IoT-based manufacturing models, there are still some other risks that prevent companies from widely using amount of collected data. These barriers are basically related to the lack of security services and standard and effective data management with desired level of protection of sensitive information (Ortiz, 2013).

Next issue is connected with traditional IP networking and the QoS level, because guarantees provided with current solution will no longer suffice compared to requirements of IoT nets of sensors. Most M2M systems and IoT solutions are currently should be implemented over transportation layer with special new application protocols connected with the network layer. This becomes a critical use cases when we talks about special uses, such as connected vehicles and telemedicine where latency and the guarantee of delivery are essential. Therefore, this kind of solution should to consider multilayer architecture of whole system as an integral part of the end-to-end solution, not only as network transport medium (Alam, 2013).

Another, one of the scientific and technical challenges in the design of the IoT systems is the dedicated architecture design, which enables the interconnection of trillions of smart devices. Modern wireless technology like WiFi, GSM 3G/LTE nets are only transport medium. Smart devices or RFID sensors will use wireless technology as smart network but we need some standards for „network enabled" objects in IoT architecture for logistics management.

Logistics has always been considered as an most important element in emergency response operations. Technology can help to manage rescue equipment, vehicles and on-site staff as well as food, medicine and general living goods. The emergency response operations require the participation of a wide range of organizations with a lot of equipment. Extensive information and resource sharing help to better cooperation between separated organizations. The results of using smart IoT systems include better resource allocation, cooperation among multiple participants, faster and accurate situation analysis, complete visibility of response forces, and their capability. These benefits looks like as emergency response specific, but there is a room for wide range of logistics management applications based on IoT applications and systems (Xu, 2013).

As we see, in general, scientific and technical challenges in the development of the IoT solution for transport and logistics require different systems and competencies: challenges of interconnecting massive smart 'network-enabled' objects, networking smart objects with external networks, and challenges of data storage, data discovery and data sharing.

Conclusions

IoT is a very complicated matter and we need to make standards in many areas, most importantly in privacy and security. We also need standards for interoperability. The applications and devices will have to be compliant to these standards. Otherwise, there will be a weak link that compromises the whole idea of „connected world". More devices are becoming embedded with sensors and gaining the ability to collect and exchange data. The resulting information networks promise to create new business models. But the predictable pathways of information are changing.

The physical world itself is becoming a type of information system where sensors embedded in physical objects are linked, often using the same Internet Protocol (IP) that connects the Internet. These networks generate large volumes of data. Often in the single device-to-cloud model, the data each IoT system produces is processing in a private stand-alone data silos. Every major IT company wants to build their own IoT platform, meaning that each one is developing its own set of standards. Is it too late to save the IoT from becoming broken into useless pieces or can the industry work together to build a true Internet of Everything?

We need an effective back-end data sharing architecture that would allow the companies to easily access, exchange and analyze the data in the cloud. Solutions designed with the IoT Architectural Reference Model (ARM) allow users to move their data when they switch between IoT services, breaking down traditional data silo barriers. The ARM provided aims to connect vertically closed systems for creating open systems and integrated environments or platforms. Industry can capitalise on the benefits of developing this kind of „Internet of Consumer-oriented Things" platforms that closely involve the telecom, hardware, software and service industries.

IoT-A, the European Lighthouse Integrated Project has created the proposed architectural reference model for IoT solutions. Using an experimental paradigm with the definition

of an initial set of key building blocks, IoT-A combined top-down reasoning about architectural principles and design guidelines with simulation and prototyping in exploring the technical consequences of architectural design choices.

However, we must face the biggest problem of IoT. Security as an important requirement for growth in IoT systems. One called it the „critical enabler", claiming that many developers and companies initially underestimate its importance when creating IoT devices. He noted, „Security is not a key issue while your application or product has not reached scale, but once you are at scale and maybe have a first incident, it becomes the most important problem" (Bauer, 2015). Recent hacks on online car systems also highlight the importance of addressing security challenges for connected devices, vehicles, and buildings.

Ensuring security will not be easy, given the numerous stand-alone applications, each with its own special features. For instance, fitness wearables might only require relatively basic security measures that ensure consumer privacy, such as software-based solutions. But IoT applications that control more critical functions, including vehicles, medical electronics and industrial automation, need much higher security level, including sometimes hardware-based solutions.

Privacy and protection of personal data are fundamental rights under Articles 7 and 8 of the EU Charter of Fundamental Rights. In addition there are specific rules currently applicable to mHealth laid down in the Data Protection Directive (95/46/EC, 1995) and the ePrivacy Directive (2002/58/EC, 2002). Completing the Digital Single Market is one of the top priorities of the European Commission. The digital technologies are transforming our world. But existing barriers online mean citizens, businesses and governments cannot fully benefit from digital tools. If citizens do not trust online services, they will not benefit from all the opportunities.

The European Commission's proposals for a comprehensive reform of the EU's 1995 Data Protection Directive aim to strengthen privacy rights and boost Europe's digital economy. The Commission's proposals update and modernize the principles enshrined in the 1995 Directive, bringing them into the digital age and building on the high level of data protection which has been in place in Europe since 1995. A clear definition of personal data will be established in the regulation to ensure harmonized implementation of the rules across the EU. The legislation is technologically neutral: this means that it will not go out of date, enabling innovation to continue to thrive under the new rules.

The current stage, known as the „trilogue", involves negotiations between the three European institutions to reach an agreement on the final text. There are many specific disagreements, but overall the Parliament's approach has been focused more on the rights of data subjects, whereas the Council wants to take approach which leaves many of the details up to national law. This may reflect the preference of some member countries, but it does risk the GDPR failing in its stated goal of harmonizing data protection rules across the EU.

While the EU had presented a strategy on cloud computing, data and the DSM, there had been little focus on IoT since the 2009 action plan. Opening the discussion on IoT policy during a debate in Brussels (Moss, 2015), Thibaut Kleiner said the EU was at a „key moment in policy in relation to IoT". Kleiner questioned if a „horizontal data approach" was needed, asking, „Do we need essential elements in terms of privacy in general or something specific for IoT?" Some important privacy questions may be covered in general, but „others deserve attention in terms of policymaking and possible legislation", he told the event. Kleiner noted that the IoT had been mentioned in the EU's recently unveiled digital single market (DSM) strategy, with its potential in helping build a telecoms single market among the aspects highlighted. In addition, some of Europe's largest tech and digital companies, launches the Alliance for Internet of Things Innovation (AIOTI) to strengthen links and build new relationships between the different IoT players (industries, SMEs, startups) and sectors.

The widespread adoption of the Internet of Things will take time, but the time line is advancing thanks to improvements in underlying technologies. Advances in technology and the greater standardization of communications protocols make it possible to collect data from sensors almost anywhere at any time. While consumers stand to reap the greatest benefits from the Internet of Things, they will have to balance potential benefits with privacy concerns. Business users of IoT technology will need to change their systems and organizations in order to make the most of the Internet of Things. They will need to invest in capabilities, culture, and processes as well as in technology. Policy makers also have an important

role in enabling the Internet of Things by leading and encouraging standards that will make interoperability and widespread adoption possible. Industry players know that a successful adoption of industrial IoT requires a rich network of partners to help companies put together all the pieces of the puzzle. From device makers to developers who can write software applications and to service providers who connect things to mobile devices and the cloud. In order to meet the needs all of the players in industrial IoT, interoperability needs to be top priority.

Literature

AIOTI (2015), The Alliance for Internet of Things Innovation (AIOTI), European Commission

Alam M., Nielsen R.H., Prasad N.R. (2013), The evolution of M2M into IoT, Communications and Networking (BlackSeaCom), First International Black Sea Conference, pp. 112-115, DOI: 10.1109/BlackSeaCom.2013.6623392

Bassi A., Bauer M., Fiedler M., Kramp T., van Kranenburg R., Lange S., Meissner S. (2013), Enabling Things to Talk: Designing IoT solutions with the IoT Architectural Reference Model, Springer Berlin Heidelberg, pp. 163-211

Bauer H., Patel M., Veira J., Internet of Things: Opportunities and challenges for semiconductor companies, McKinsey Insights, http://www.mckinsey.com/insights/innovation/internet_of_things_opportunities_and_challenges_for_semiconductor_companies [30.10.2015]

Bisk Education, University Alliance, RFID Technology Boosts Walmart's Supply Chain Management, http://www.usanfranonline.com/resources/supply-chain-management/rfid-technology-boosts-walmarts-supply-chain-management/ [07.02.2014]

Boost to C&L, Supply Chain 24/7 Boost; Internet of Things Will Deliver $1.9 Trillion Boost to Supply Chain & Logistics Operations, http://www.supplychain247.com [16.04.2015]

Bosavage J., Sensors, Beacons and GPS: The IoT Is Here, http://www.retailpro.com/News/blog/index.php/tag/beacon/ [05.10.2015]

Chuanyu S. (2009), Analysis on the Interaction of both Computer Network and Modern Logistics, E-Busness Journal, pp. 44-45

Cline J., Computerworld, A privacy standard for Internet of Things suppliers, http://www.computerworld.com/article/3010626internet-of-things/a-privacy-standard-for-internet-of-things-suppliers.html [01.12.2015]

Croll A., O'Reilly Radar. The Internet of Things has four big data problems, http://radar.oreilly.com/2015/01/the-internet-of-things-has-four-big-data-problems.html [12.01.2015]

Das R., Harrop P. (2015), RFID Forecasts, Players and Opportunities 2016-2026, The complete analysis of the global RFID industry, IDTechEx, RFID Forecasts, Players and Opportunities 2016-2026, The complete analysis of the global RFID industry

Deloitte University Press, M. L. Shipping smarter: IoT opportunities in transport and logistics, http://dupress.com/articles/internet-of-things-iot-in-shipping-industry/ [15.09.2015]

Directive 2002/58/EC of the European Parliament – Directive on privacy and electronic communications

Directive 95/46/EC of the European Parliament on the protection of individuals with regard to the processing of personal data and on the free movement of such data

DSM (2015), Digital Single Market – Digital Agenda for Europe, The Digital Single Market strategy, European Parliament

European Lighthouse Integrated Project (2013), IoT-A – Internet-of-Things Architecture Project, European Lighthouse Integrated Project

FTC Staff Report (2015), Internet of Things: Privacy & Security in a Connected World, US Federal Trade Commission

GDPR (2015), European Commission, General Data Protection Regulation, European Commission

Girish D., RFID vs iBeacon (BLE) Technology, http://blog.beaconstac.com/2015/10/rfid-vs-ibeacon-ble-technology/ [20.10.2015]

Harropm P., IDTechEx, Rapid adoption of RFID in healthcare, http://www.idtechex.com/ [08.05.2006]

Improving T&L, Supply Chain 24/7, How the Internet of Things Is Improving Transportation and Logistics, http://www.supplychain247.com [09.09.2015]

Koomey J. (2012), The computing trend that will change everything, MIT Technology Review

Manyika J., Woetzel J., Dobbs R., Chui M., Bisson P., Bughin J., Aharon D. (2015), McKinsey & Company, The Internet Of Things: Mapping The Value Beyond The Hype, McKinsey Global Institute

Mobile Health – Reconciling (2015), European Data Protection Supervisor, Mobile Health – Reconciling technological innovation with data protection, European Commission

Moss M. (2015), Future of the Internet of things: EU at „key moment" in IoT policy debate, The Parliament Magazine

Online Trust Alliance (2015), ITWG, https://otalliance.org/initiatives/internet-things [20.10.2015]

Ortiz P., Lazaro O., Uriarte M., Carnerero M. (2013), Enhanced multi-domain access control for secure mobile collaboration through Linked Data cloud in manufacturing, World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2013 IEEE 14th International Symposium and Workshops, pp. 1-9, DOI: 10.1109/WoWMoM.2013.6583372

Rose K., Eldridge S., Chapin L. (2015), The Internet of Things (IoT): An Overview – Understanding the Issues and Challenges of a More Connected World, Internet Society

Ruan D.X., Wu D., Wu X.B. (2012), The Internet of things technology in logistics application: Stages, trend and drive modes. Management of Technology (ISMOT), 2012 International Symposium, Hangzhou, IEEE, pp. 452-455, DOI: 10.1109/ISMOT.2012.6679511

Schneider S., Understanding The Protocols Behind The Internet Of Things, Electronic Design, http://electronicdesign.com/iot/understanding-protocols-behind-internet-things [09.10.2013]

Shaoai W. (2009), Analysis on the relationship between Modern Logistics and Multimodal Transport New West 10, 37, 23

Tsai C.W., Lai C.F., Chiang M.C., Yang L.T. (2014), Data Mining for Internet of Things: A Survey. Communications Surveys & Tutorials, IEEE 16 (1), pp. 77-97, DOI: 10.1109/SURV.2013.103013.00206

Wanpeng F., Yu L. (2010), ZTE Technologies. Opportunities, Challenges and Practices of the Internet of Things. Retrieved from Opportunities, Challenges and Practices of the Internet of Things, http://wwwen.zte.com.cn/ [01.03.2010]

Xu R., Yang L., Yang S-H. (2013), Architecture Design of Internet of Things in Logistics Management for Emergency Response, Green Computing and Communications (GreenCom), 2013 IEEE and Internet of Things (iThings/CPSCom), IEEE International Conference on and IEEE Cyber, Physical and Social Computing, pp. 395-402, DOI: 10.1109/GreenCom-iThings-CPSCom.2013.85

Yuqiang C., Jianlan G., Xuanzi H. (2010), The research of Internet of things' supporting technologies which face the logistics industry, Computational Intelligence and Security (CIS) International Conference, pp. 659-663, DOI: 10.1109/CIS.2010.148

Zhang Y., Sun S. (2013), Real-time Data Driven Monitoring and Optimization Method for IoT – based Sensible Production Process, Networking, Sensing and Control (ICNSC), 2013 10th IEEE International Conference, pp. 486-490, DOI: 10.1109/ICNSC.2013.6548787