Emerald Internet Research

The internet of things: a security point of view

Journal:	*Internet Research*
Manuscript ID	IntR-07-2014-0173.R2
Manuscript Type:	Research Paper
Keywords:	Internet of Things, Security Requirements, Multi-layer Security Architecture

The Internet of Things: A Security Point of View

1 Introduction

The emerging Internet of Things (IoT) is believed to be the next generation of the Internet and will become an attractive target for hackers (Li et al. 2014a; Li et al. 2014c; Roman et al. 2011), in which billions of things are interconnected. Each physical object in the IoT is able to interact without human interventions (Bi et al. 2014; Li et al. 2014d). In recent years, a variety of applications with different infrastructures have been developed, such as logistics, manufacturing, healthcare, industrial surveillance, etc (ITU 2013; Pretz 2013). A number of cute-edging techniques (such as intelligent sensors, wireless communication, networks, data analysis technologies, cloud computing, etc.) have been developed to realise the potential of the IoT with different intelligent systems (Bi et al. 2014; Tan et al. 2014). However, technologies for the IoT are still in their infant stages and a lot of technical difficulties associated with IoT need to be overcome (Li et al. 2014c). One of the most significant obstacles in IoT is security (Li et al. 2014c), which involves the sensing infrastructure security, communication network security, application security, and general system security (Keoh et al. 2014). To address the security challenges in IoT, we will analyse the security problems in IoT based on four-layer architecture.

1.1 Overview

The concept of IoT was firstly proposed in 1999 (Li et al. 2014c) and the exact definition is still subjective to different perspectives taken (Hepp et al. 2007; ITU 2013; Li et al. 2014c; Pretz 2013). The IoT is believed to be the future Internet for the new generation, which integrates various ranges of technologies, including sensory, communication, networking, service-oriented architecture, and intelligent information processing technologies (Council 2008; Li et al. 2014c; Lim et al. 2013). However, it also brings a number of significant challenges, such as security, integration of hybrid networks, intelligent sensing technologies, etc. Security is the chief among them, which play a fundamental role to protect the IoT against attacks and malfunctions (Roman et al. 2011). Traditionally, the security means cryptography, secure communication, and privacy assurances. However in IoT security encompasses a wider range of tasks, including data confidentiality, services availability, integrity, anti-malware, information integrity, privacy protection, access control, etc (Keoh et al. 2014).

As an open eco-system, the IoT security is orthogonal to other research areas. The great diversity of IoT makes it very vulnerable to attacks against availability, service integrity, security and privacy. At the lower layer of IoT (sensing layer), the sensing devices/technologies have very limited computation capacity and energy supply and cannot provide well security protection; at the middle layers (such as network layer, service layer), the IoT relies on networking and communications which facilitates eavesdropping, interception and DoS attacks. For example, in network layer, a self-organized topology without centralized control is prone to attacks against authentication, such as node replication, node suppression, node impersonation, etc. At the upper layer (such as application layer), the data aggregation and encryption turn out to be useful to mitigate the scalability and vulnerability problems of all layers. To build a trustworthy IoT, a system-level security analytics and self-adaptive security policy framework are needed.

1.2 State-of-the-art

The IoT is an extension of the Internet by integrating mobile networks, Internet, social networks, and intelligent things to provide better services or applications to users (Cai et al. 2014; Gu et al. 2014; Hoyland et al. 2014; Kang et al. 2014; Keoh et al. 2014; Li et al. 2014a; Li et al. 2014b; Tao et al. 2014; Xiao et al. 2014; Xu et al. 2014a; Xu et al. 2014b; Yuan Jie et al. 2014). The success of IoT depends on the standardization of security at various levels, which provides secured interoperability, compatibility, reliability, and effectiveness of the operations on a global scale (Li et al. 2014c). The importance of IoT has been recognized as top national strategies by many countries. The IoT European Research Cluster (IERC) sponsored a number of IoT fundamental research projects: IoT-A was launched to design a reference model and architecture for IoT, while the ongoing RERUM project focuses on IoT security (Floerkemeier et al. 2007; Gama et al. 2012; Welbourne et al. 2009). The Japan government proposed u-Japan and i-Japan strategies to promote a sustainable ICT society (Ning 2013). In US, the ITIF focuses on new information and communication technologies for IoT (He et al. 2012; Xu 2011). The South Korea conducted RFID/USN and "New IT Strategy" program to advance the IoT infrastructure development (Xu 2011). The China government officially launched the 'Sensing China' programme in 2010 (Bi et al. 2014).

Technically, a very diverse range of networking and communication technologies is available for IoT, such as WiFi, ZigBee (IEEE 802.15.4), BLE (Low energy Bluetooth), ANT, etc. More specifically, the IETF has standardized 6LoWPAN (IPv6 over Low-Power Wireless Personal Area Networks), ROLL (routing over low-power and lossy-networks), and CoAP (constrained application protocol) to equip constrained devices (Cai et al. 2014; Chen et al. 2014; Esad-Djou 2014; Gu et al. 2014; Hoyland et al. 2014; HP Company 2014; Kang et al. 2014; Keoh et al. 2014; Li and Xiong 2013; Li et al. 2014a; Oppliger 2011; Raza et al. 2013; Roe 2014; Tan et al. 2014; Wang and Wu 2010; Xiao et al. 2014; Xu et al. 2014a; Xu et al. 2014b; Yao et al.

2013). Concerns over the authenticity of software and protection of intellectual property produced various software verification and attestation techniques often referred to as trusted or measured boot. The confidentiality of data has always been and remains a primary concern. Security control mechanisms have been developed to ensure the security of data transmission in wireless communication and in motion, such as 802.11i (WPA2) or 802.1AE (MACsec). In recent, the security standards for the RFID market have been reported in (Raza et al. 2012). For RFID applications, EC has released several recommendations to outline the following security issues in a lawful, ethical, socially and politically acceptable way (Di Pietro et al. 2014; Esad-Djou 2014; Furnell 2007; Gaur 2013; HP Company 2014; Raza et al. 2012; Roe 2014; Roman et al. 2013; Weber 2013):

- Measuring the deployment of RFID applications to ensure that national legislation is complying with the EU Data Protection Directive 95/46, 99/5 and 2002/58.
- A framework for privacy and data protection impact assessments has been proposed (PIA; No.4).
- Assessment of implications of the application implementation for the protection of personal data and privacy (No.5).
- Identifying any applications that might raise information security threats.
- Checking the information
- Issuing recommendations that concern the privacy information and transparency on RFID use.

But for IoT, the security problem is still a challenging area. Billions of devices might be connected in IoT and well-designed security architecture is needed to fully protect the information and allow data to be securely shared over IoT. New security challenges will be created by the endless variety of IoT applications(HP Company 2014; Roman et al. 2011; Roman et al. 2013). For example,

- Industrial security concerns, including the intelligent sensors, embedded programmable logic controllers (PLCs), robotic systems, which are typically integrated with IoT infrastructure. Security control on the IoT industrial infrastructure is a big concern.
- Hybrid system security controls. The IoT might involve many hybrid systems, how to provide cross-system security protection is crucial for the success of the IoT.
- For the new business processes created in IoT, a security is needed to protect the business information and data.
- IoT end-node security, how the end-nodes receive software updates or security patches in a timely manner without impairing functional safety is a challenging.

1.3 Security Requirements

In IoT, each connected device could be a potential doorway into the IoT infrastructure or personal data (HP Company 2014; Roe 2014). The data security and privacy concerns are very important but the potential risks associated with the IoT will reach new levels as interoperability, mashups and autonomous decision-making begin to embed complexity, security loopholes and potential vulnerability. Privacy risks will arise in the IoT since the complexity may create more vulnerability that related to the service. In IoT, much information is related with our personal information, such as date of birth, location, budegets, etc. This is one aspect of the big data challenging, and security professions will need to ensure that they think through the potential privacy risks associated with the entire data set. The IoT should be implemented in a lawful, ethical, socially and politically acceptable way, where legal challenges, systematic approaches, technical challenges, and business challenges should be considered. This paper focuses on the technically implementation design of the security IoT architecture. Security must be addressed throughout the IoT lifecycle from the initial design to the services running. The main research challenges in IoT scenario include the data confidentiality, privacy, and trust, as shown in Fig.1 (Di Pietro et al. 2014; Furnell 2007; Gaur 2013; Miorandi et al. 2012; Roman et al. 2013; Weber 2013).

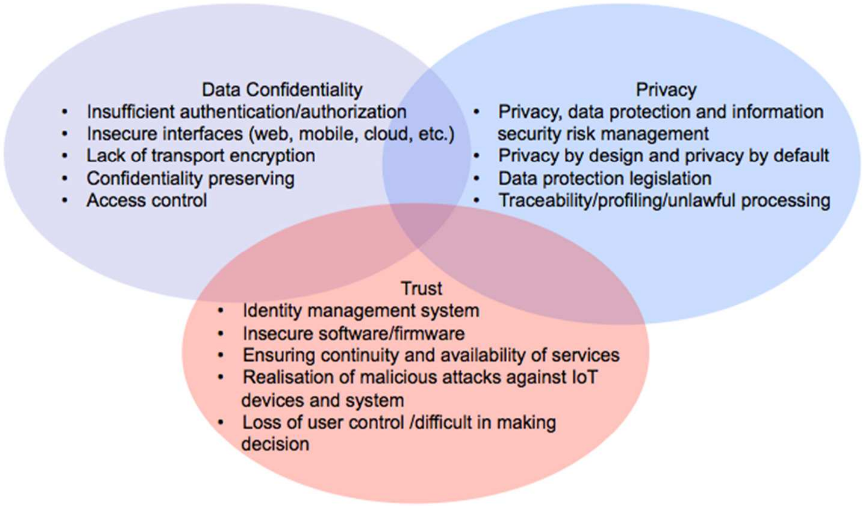
Data Confidentiality
• Insufficient authentication/authorization
• Insecure interfaces (web, mobile, cloud, etc.)
• Lack of transport encryption
• Confidentiality preserving
• Access control
Privacy
• Privacy, data protection and information security risk management
• Privacy by design and privacy by default
• Data protection legislation
• Traceability/profiling/unlawful processing
Trust
• Identity management system
• Insecure software/firmware
• Ensuring continuity and availability of services
• Realisation of malicious attacks against IoT devices and system
• Loss of user control /difficult in making decision

Fig.1 Security issues in IoT

To well illustrate the security requirements in IoT, we modelled the IoT as four-layer architecture: *sensing-layer, network-layer, service-layer, and application-interface layer*. Each layer is able to provide corresponding security controls, such as access control, device authentication, data integrity and confidentiality in transmission, availability, and the ability to anti-virus or attacks. In Table.1, the most security concerns in IoT are summarized:

Table 1 Top ten vulnerabilities in IoT

Security concerns	Interface Layer	Service layer	Network layer	Sensing layer
Insecure web interface	√	√	√	
Insufficient authentication/authorization	√	√	√	√
Insecure Network services		√	√	
Lack of transport encryption		√	√	
Privacy concerns		√	√	√
Insecure Cloud interface	√			

Insecure Mobile interface	√		√	√
Insecure Security configuration	√	√	√	
Insecure software/firmware	√		√	
Poor physical security			√	√

The security requirements depend on each particularly sensing technology, networks, layers, and have been identified in the corresponding sections.

2 Security Requirements in IoT Architecture

A critical requirement of IoT is that the devices must be inter-connected, which makes it be able to perform specific tasks, such as sensing, communicating, information processing, etc (Fielding and Taylor 2002; Frenken et al. 2008; Guinard et al. 2010). The IoT is able to acquire, transmit, and process the information from the IoT end-nodes (such as RFID devices, sensors, gateway, intelligent devices, etc.) via network to accomplish highly complex tasks. The IoT should be able to provide applications with strong security protection (for example, for online payment application, the IoT should be able to protect the integrity of payment information).

The system architecture must provide operational guarantees for the IoT, which bridges the gap between the physical devices and the virtual worlds. In designing the framework of IoT, following factors should be taken into consideration: (1) Technical factors, such as sensing techniques, communication methods, network technologies, etc.; (2) security protection, such as information confidentiality, transmission security, privacy protection, etc.; (3) business issues, such as business models, business processes, etc. In current, the service-oriented architecture has been successfully applied to IoT design, where the applications are moving towards service-oriented integration technologies. In business domain, the complex applications among diverse services have been appearing. Services reside in different layers of the IoT such as: sensing layer, network layer, services layer, and application-interface layer. The services based application will heavily depend on the architecture of IoT. Fig.2 depicts a generic service-oriented architecture for IoT, which consists of four layers:

- *Sensing layer* is integrated with end components of IoT to sense and acquire the information of devices;
- *Network layer* is the infrastructure to support wireless or wired connections among things;
- *Service layer* is to provide and management services required by users or applications;
- *Application-interfaces layer* consists of interaction methods with users or applications.

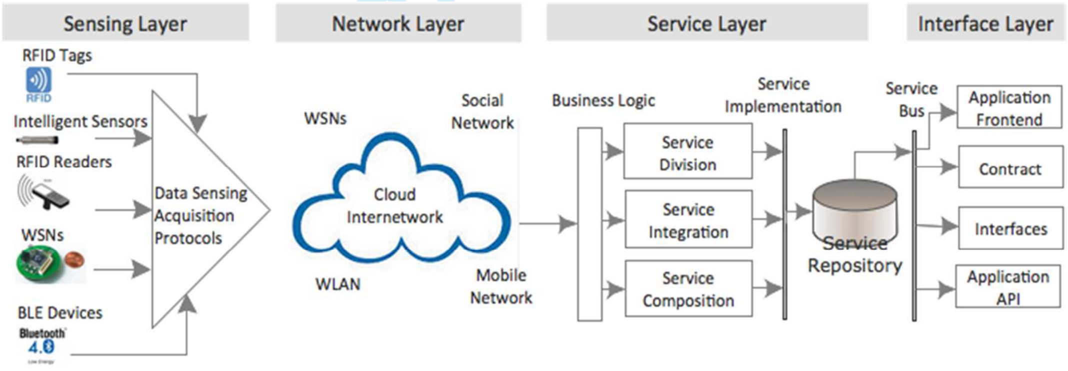

Figure 2. Service-oriented architecture for IoT (Bi et al. 2014; Li et al. 2014a; Li et al. 2014c)

The security requirements on each layer might be different due to its features. In general, the security solution for the IoT considers following requirements: (1) sensing-layer and IoT end-node security requirements, (2) network-layer security requirements, (3) service-layer security requirements, (4) application-interface-layer security requirements, (5) the security requirements between layers, and (6) security requirements for services running and maintenance.

2.1 Sensing Layer and IoT end-nodes

The IoT is a multilayer network that inter-connects devices for information acquisition, exchange, and processing. At the sensing layer, the intelligent tags and sensor networks are able to automatically sense the environment and exchange data among devices (Li et al. 2014c). In determining the sensing layer of an IoT, the main concerns are:

- *Cost, size, resource, and energy consumption*. The things might be equipped with sensing devices such as RFID tags, sensors, actuator, etc., which should be designed to minimize required resources as well as cost.
- *Deployment*. The IoT end-nodes (such as RFID reader, tags, sensors, etc.) can be deployed one-time, or in incremental or random ways depending on application requirements.
- *Heterogeneity*. A variety of things or hybrid networks make the IoT very heterogeneous.
- *Communication*. The IoT end-nodes should be designed able to communicate each other.
- *Networks*. The IoT involves hybrid networks, such as WSNs, WMNs, and SCADA systems.

The security is an important concern in sensing-layer. It is expected that IoT could be connected with industrial networks to provide users smart services. However, it may cause new concerns in devices controlling, such as who can input authentication credentials or decide whether an application should be trusted. The security model in IoT must be able to make its own judgements and decision about whether to accept a command or execute a task. At sensing-layer, the devices are designed for low power consumption with constraints resources, which often have limited connectivity. The endless variety of IoT applications poses an equally wide variety of security challenges (CCSA 2012).

- Devices authentication
- Trusted devices
- Leveraging the security controls and availability of infrastructures in sensing-layer.
- In terms of software update, how the sensing devices receive software updates or security patches in a timely manner without impairing functional safety or incurring significant recertification costs every time a patch is rolled out.

In this layer, the security concerns can be classified into two main categories:

- The security requirements at IoT end-node: physically security protection, access control, authentication, non-repudiation, confidentiality, integrity, availability, and privacy.
- The security requirements in sensing-layer: confidentiality, data source authentication, device authentication, integrity, availability, and timeless etc.

Table.2 summarizes the potential security threats and security vulnerabilities at IoT end-node and Table.3 analyses the security threats and vulnerabilities in sensing layer.

Table 2 Security threats and vulnerabilities at IoT end-node

Security threats	Description
Unauthorized access	Due to physically capture or logic attacked, the sensitive information at the end-nodes is captured by the attacker;
Availability	The end-node stops to work since physically captured or attacked logically;
Spoofing attack	With malware node, the attacker successfully masquerades as IoT end-device, end-node, or end-gateway by falsifying data
Selfish threat	Some IoT end-nodes stop working to save resources or bandwidth to cause the failure of network
Malicious code	Virus, Trojan, and junk message that can cause software failure

Denial of Services (DoS)	An attempt to make a IoT end-node resource unavailable to its users
Transmission threats	Threats in transmission, such as interrupting, blocking, data manipulation, forgery, etc.
Routing attack	Attacks on a routing path

Table 3 Analysis of the security threats and vulnerabilities in sensing layer

IoT end-node threats and vulnerabilities	IoT end-devices	IoT end-node	IoT end-gateway
Unauthorized access	√	√	√
Selfish threat		√	√
Spoofing attack		√	√
Malicious code	√	√	√
Denial of Services (DoS)	√	√	√
Transmission threats			√
Routing attack	√	√	√

To secure devices in this layer before users are at risk, following actions should be taken: (1) Implement security standards for IoT and ensure all devices are produced by meeting specific security standards; (2) Build trustworthy data sensing system and review the security of all devices/components; (3) Forensically identify and trace the source of users; (4) Software or firmware at IoT end-node should be securely designed.

2.2 Network Layer

The network layer connects all things in IoT and allows them aware of their surroundings. It is capable of aggregating data from existing IT infrastructures and then transmits to other layers, such as sensing layer, service layers, etc. The IoT connects a verity of different networks, which may cause a lot of difficulties on network problems, security problems, and communication problems.

The deployment, management, and scheduling of networks are essential for the network layer in IoT. This enables devices to perform tasks collaboratively. In the networking layer, the following issues should be addressed:

- Network management technologies including the management for fixed, wireless, mobile networks

- Network energy efficiency

- Requirements of QoS
- Technologies for mining and searching
- Information confidentiality
- Security and privacy

Among these issues, information confidentiality and human privacy security are critical because of its deployment, mobility, and complexity. The existing network security technologies can provide a basis for privacy and security protection in IoT, but more works still need to do. The security requirements in network layer involve:

- *Overall security requirements*, including confidentiality, integrity, privacy protection, authentication, group authentication, keys protection, availability, etc.
- *Privacy leakage*. Since some IoT devices physically located in untrusted places, which cause potential risks for attackers to physically find the privacy information such as user identification, etc.
- *Communication security*. It involves the integrity and confidentiality of signalling in IoT communications.
- *Overconnected*. The overconnected IoT may run risk of losing control of the user. Two security concerns may be caused: (1) DoS attack, the bandwidth required by signalling authentication can cause network congestion and further cause DoS; (2) Keys security, for the overconnected network, the keys operations could cause heavy network resources consumption.

- *MITM attack*, the attacker makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a private connection, when in fact the attacker controls the entire conversation.

- *Fake network message*, attackers could create fake signalling to isolate/mis-operate the devices from the IoT.

In the network-layer, the possible security threats are summarized in Table. 4 and Table 5, the potential security threats and vulnerabilities are analysed.

Table 4 Security threats in network layer

Security threats	Description
Data breach	Information release of secure information to an untrusted environment
Transmission threats	The integrity and confidentiality of signaling,
Denial of Services (DoS)	An attempt to make a IoT end-node resource unavailable to its users
Public key and private key	The comprise of keys in networks
Malicious code	Virus, Trojan, and junk message that can cause software failure
Denial of Services (DoS)	An attempt to make a IoT end-node resource unavailable to its users
Transmission threats	Threats in transmission, such as interrupting, blocking, data manipulation, forgery, etc.
Routing attack	Attacks on a routing path

Table 5 The security threats and vulnerabilities in network layer

	Privacy leakage	Confidentiality	Integrity	DoS	PKI	MITM	Request Forgery
Physically protection	√	√					√
Transmission Security		√	√	√	√	√	√
Overconnected			√	√	√		
Cross-layer fusion	√	√				√	√

The network infrastructure and protocols developed for IoT are different with existing IP network, special efforts are needed on following security concerns: (1) Authentication/Authorization, which involves vulnerabilities such as password, access control, etc.; (2) Secure transport encryption, it is crucial to encrypt the transmission in this layer.

2.3 Service layer

In IoT, the service layer relies on middleware technology, which is an important enabler of services and applications. The service layer provides IoT a cost-effective platform where the hardware and software platforms could be reused. The IoT illustrates the activities required by the middle service specifications, which are undertaken by various standards developed by the service providers and organizations. The service layer is designed based on the common requirements of applications, application programming interfaces (APIs), and service protocols. The core set of services in this layer might include following components: event processing service, integration services, analytics services, UI services, and security and management services (Choi et al. 2012). The activities in service layer, such as information exchange, data processing, ontologies databases, communications between services, are conducted by following components:

- *Service discovery*. It finds infrastructure can provide the required service and information in an effective way.
- *Service composition*. It enables the combination and interaction among connected things. Discovery exploits the relationships of things to find the desired service, and service composition schedules or re-creates more suitable services to obtain the most reliable ones.
- *Trustworthiness management*. It aims at understanding how the trusted devices and information provided by other services.
- *Service APIs*. It provides the interactions between services required by users.

In recent, a number of service layer solutions have been reported. The SOCRADES integration architecture (SIA) is proposed that can be used to interact between applications and service layers effectively (Fielding and Taylor 2002); things are abstracted as devices to provide services at low-levels as network discovery services, metadata exchange services, and asynchronous publish and subscribe event in (Kranenburg et al. 2011; Sundmaeker et al. 2010); In (Peris-Lopez et al. 2006), a representational state transfer (REST) is defined to increase interoperability between loosely coupled services and distributed applications. In (Hernandez-Castro et al. 2013), the services layer introduced a service provisioning process (SPP) that can provide the interaction between applications and services. It is important to design an effective security strategy to protect services against attacks in the service layer. The security requirements in the service layer include:

- Authorization, service authentication, group authentication, privacy protection, integrity, integrity, security of keys, non-repudiation, anti-replay, availability, *etc*.
- Privacy leakage. The main concern in this layer involves privacy leakage and malicious location tracking.
- Service abuses, in IoT the service abuse attack involves: (i) illegal abuse of services; (ii) abuse of unsubscribed services;
- Node identify masquerade.
- DoS attack, Denial of service.
- Replay attack, the attacker resend the data.
- Service information sniffer and manipulation.
- Repudiation in service layer, it includes the communication repudiation and services repudiation.

The security solution should be able to protect the operations on this layer from potential threats. Table 6 summarizes the security threats on the service layer.

Table 6 The security threats in service layer

Security threats	Description

Privacy threats	Privacy leakage or malicious location tracking
Services abuse	Unauthorized uses access services or the authorized users access unsubscribed services
Identity masquerade	The IoT end-device, node, or gateway are masqueraded by attacker
Service information manipulation	The information in services is manipulated by the attacker
Repudiation	Denial the operations have been done
Denial of Services (DoS)	An attempt to make a IoT end-node resource unavailable to its users
Replay attack	The attack re-send the information to spoof the receiver
Routing attack	Attacks on a routing path

Ensure the data in service layer secure is crucial but difficult. It involves fragmented, full of competing standards and proprietary solutions. The service oriented architecture (SoA) is very helpful to improve the security of this layer (Atzori et al. 2010; Esad-Djou 2014), but following challenges still need to be faced when building an IoT services or application: (1) data transmission security between service and/or layers; (2) secure services management, such as service identification, access control, services composite, etc.

2.4 Application-interface Layer

The application-interface layer involves a variety of applications interfaces from RFID tag tracking to smart home, which are implemented by standard protocols as well as service-composition technologies (Gu et al. 2014; Ning et al. 2013). The requirements in application-interface layer strongly depend the applications. For the application maintenance, following security requirements will be involved:

- Remote safe configuration, software downloading and updating, security patches, administrator authentication, unified security platform, *etc*.

For the security requirements on communications between layers,

- Integrity and confidentiality for transmission between layers, cross-layer authentication and authorization, sensitive information isolation, etc.

In IoT designing the security solutions, following rules should be helpful:

a) Since most constrained IoT end-node works with an unattended manner, the designer should pay more attention to the safety of these nodes;

b) Due to IoT involves billions of clustering nodes, the security solutions should be designed based on energy efficiency schemes;

c) The light security scheme at IoT end-nodes might be different with existing network security solutions, however we should design security solutions in a big enough range for all parts in IoT.

Table 7 summarizes the security threats and vulnerabilities in IoT application-interface layer.

Table 7 The security threats in application-interface layer

Security threats	Description
Remote configuration	Fail to configure at interfaces
Misconfiguration	Mis-configuration at remote IoT end-node, end-device, or end-gateway
Security management	Log and Keys leakage
Management system	Failure of management system

In Table 8, we analyse the security threats and potential vulnerabilities in application-interface layer.

Table 8 shows the security threats and vulnerabilities in Application-interface layer

	Unauthorized access	Failure of node	Masquerade	Selfish node	Trojan, virus, spam	Privacy leakage
Physically security protection	√	√	√			
Anti-virus, firewalling				√		
Access Control	√	√	√			√
Confidential	√	√	√			√
Data Integrity		√	√	√	√	
Availability						
Authentication	√	√	√			√
Non-Repudiation	√	√	√			√

The application-interface layer bridges the IoT system with user applications, which should be able to ensure that the interaction of IoT systems with other applications or users are legal and can be trusted.

2.5 Cross-layer Threats

Information in the IoT architecture might be shared among all of the four layers to achieve full interoperability between services and devices. It brings a number of security challenges such as trust guarantee, privacy of the users and their date, secure data sharing among layers, etc. In the IoT architecture described in Fig.2, information is exchanged between different layers, which may cause potential threats as shown in Table. 9

Table 9 Security threats between layers in the IoT architecture

Security threats	Description
Sensitive information Leakage at border	The sensitive information might be not protected at the border of layers.
Identity spoofing	The identities in different layers have different priorities.
Sensitive information spreads between layers	Sensitive information spreads at different layers and cause information leakage

The security requirements in this layer include (1) security protection, securing to be ensured at design and execution time; (2) privacy protection, personal information access within IoT system, privacy standards and enhancement technologies; (3) trust has to be a part of IoT architecture and must be built in.

2.6 Threats caused in maintenance of IoT

The maintenance of IoT can cause security problems, such as in configuration of the network, security management, and application managements. Table.10 summarized the potential threats that can cause risky in IoT.

Table 10 Security threats between layers in the IoT architecture

Security threats	Description
Remote configuration	Fail to configure remote IoT end-node, end-device, or end-gateway
Misconfiguration	Mis-configuration at remote IoT end-node, end-device, or end-gateway
Security management	Log and Keys leakage at IoT end-node
Management system	Failure of management system

3 Security in Enabling Technologies

3.1 Security in Identification and Tracking Technologies

The concept of IoT was coined based on the RFID-enabled identification and tracking technologies. A basic RFID system consists of an RFID reader and RFID tags. Due to its capability for identifying, tracing, and tracking, the RFID system has been widely applied in logistics, such as package tracking, supply chain management, healthcare applications, etc. A RFID system could provide sufficient real-time information about things in IoT, which are very useful to manufacturers, distributors, and retailers. For example, RFID application in supply chain management can improve backroom inventory-management practices.

Although RFID technology is successfully used in many areas, it is still evolving in developing active system, Inkjet-printing based RFID, and management technologies in (Hepp et al. 2007). For adoption by the IoT, more identified problems need to be resolved, such as: *collision of RFID readings*, *signal interferences*, p*rivacy protection*, s*tandardization, integration, etc*.

In the new era of IoT, the scope of identifications has expended and included RFIDs, Barcodes, and other intelligent sensing technologies. In RFID-enable contactless technologies (ISO 14443 and 15693), security features have been implemented, such as cryptographic challenge-response authentication, 128-bit AES, triple-DES, and SHA-2 algorithms. The increasingly use of RFID devices requires the RFID security guarantee from multiple sides: manufacture, privacy protection, business processes. In general the security features of RFID includes (Bottani and Rizzi 2008; Broll et al. 2009; EPCglobal 2004):

- Tags/Readers collision problem
- Data confidentiality
- Tag-to-reader authentication
- High-assurance readers

Table 11 summarizes the security features of RFID standards.

Table 11 Security features in RFID standards

Security RFID\	Confidentiality	Integrity	Availability
EPC Class 0/0+		√	√
EPC Class 1 G1		√	√
EPC Class 1 G2	√	√	√
ISO/IEC 18000-2	√	√	
ISO/IEC 18000-3	√	√	√
ISO/IEC 11784/5	√	√	
ISO/IEC 15693	√	√	√
Non-Repudiation	√	√	√

In RFID technologies, the security and privacy protection are not just technical issues; important policy questions arise as RFID tags join to create large sensor networks.

3.2 Security in Integration of WSN and RFID

The integration of wireless sensors and RFID empowers IoT in the implementation of industrial services and the further deployment of services in extended applications. IoT with the integration of RIFD and WSNs make it possible to develop IoT applications for healthcare, decision-making of complex systems, and smart civic systems such as smart transport, cities or water supply systems(Alcaraz and Lopez 2010).

The security issue in integration of RFID and WSNs involves following challenges:

- *Privacy*, it involves the privacy of RFID devices and WSNs devices,
- Identification and authentication, the identification has to be protected from tracking by unauthorized user in the network.
- *Communication security*, the communication between RFID devices and IoT devices poses security threats, which need to be addressed proactively, and appropriate measures must be implemented well.
- *Trust and ownership*, trust implies the authenticity and integrity of the communication parts such as sensor nodes and RFID tags.
- *Integration*
- *User authentication*

3.3 Security in Communications

In IoT things are connected together in network access layer through different communication technologies. The IoT can be seen as an aggregation of heterogeneous networks, such as WSNs, wireless mesh networks, mobile networks, RFID systems, and WLAN. The communications between things/networks are essential to make reliable information exchange, which requires the IoT to provide secure, reliable, and scalable connections. IoT would also greatly benefit from the existing communication protocols in Internet such as IPv6, as this address any number of things needed through the Internet directly (Pretz 2013). The basic principles of secure communications in IoT include: *authentication, availability, confidentiality, and integrity*. The limit of resources of things makes it difficult to build a secure enough for IoT; however, the IoT communication systems have to be designed to provide 'secure enough' by finding the right balance between effort and benefit of protection measures. The security solution for communications should be designed high enough to force the hackers give up before they succeed. The commonly used communication protocols and the potential security features include:

- RFID (e.g. ISO 18000 6c EPC class 1 Gen2), the security features include confidentiality, integrity, and availability. The security features for different standards can be found in Table .10.
- NFC, IEEE 802.11 (WLAN), IEEE 802.15.4, IEEE 802.15.1(Bluetooth), in these wireless communication technologies, following security are needed: confidentiality, integrity, authentication, availability, and detection malicious intrusion.

- IETF Low power Wireless Personal Area Networks (6LoWPAN). Since 6LoWPAN is a combination of IEEE 802.15.4 and IPv6, which may cause potential vulnerabilities from the two sides that target all layers of the stack:

Table 12 Security features in 6LoWPAN

Layers	Main potential attacks
Application Layer	Overwhele attack, path-based DoS attack
Transport Layer	Flooding attack
Network Layer	Malicious node attack; Sybil attack; Wormhole attack, Spoofing attack, and routing attack, etc.
Adaption Layer	Packets fragmentation attack;
Link Layer	Exhaustion attack, collision attack; interrogation attack;
Physical Layer	Tampering attack, etc.

- Machine-to-Machine (M2M), tradition disruptive attacks in M2M such as DoS could have new consequences in M2M.
- Traditional IP technologies, such as IP, IPv6, etc. IPv4, secure every device, addresses nearing exhaustion, networks simple won’t have enough addresses to assign to the explosion of devices unless they transition to IPv6. However, for IPv6 it could have further vulnerabilities that haven’t been discovered. In IPv6, IPsec could provide authenticity and integrity with authentication header, and the *Encapsulated* security payload provides confidentiality. In recent, the transport layer security (TLS) is developed as an alternative to IPsec to provide mutual authentication of two parties using public key infrastructures and X.509 certificates (Tao et al. 2014).
- Key Management in IoT. Many key management systems (KMSs) have been proposed in recent. In IoT, the KMS should be designed based on standard protocols. The IPsec applies the Internet Key Exchange (IKE) for automatic key management. For IEEE 802.15.4, no key management system is defined but in (Cai et al. 2014), a lightweight key management IKEv2 is proposed for 6LoWPAN IPsec and IEEE 802.15.4.

3.4 Security in Networks

The IoT is a hybrid network that involves a lot of heterogeneous networks, which requires multi-faceted security solutions to against network intrusions and disruptions. The IoT contains networks that connected with daily used devices, such as smartphones, surveillance cameras, home appliances, etc. Support for heterogeneous networks can help IoT to connect the devices with different communication specification, QoS requirements, functionalities, and goals. On the other hand, support for heterogeneity can reduce the cost to implement IoT by well integrating diversified things. Meanwhile, some of the existing networking technologies such as architecture, protocols, network management, security schemes, can be directly applicable in an IoT context. The networks involved in IoT are core parts of security working, and each sub-network is required to provide confidentiality, secure communication, encryption certificates and that sort of things. In IoT no IDS and IPS are specifically designed yet, but many watchdog-based IDS and IPSs could be used in the context of IoT.

3.5 Security in Service Management

Service management refers to the implementation and management of the services that meet the needs of users or applications. Security solution at service layer is designed specifically in the context of the services. For services such as consumer applications, logistical, surveillance, intelligent healthcare, the security concerns have some similarities: authentication, access control, privacy, integrity of information, certificates and PKI certificates, digital signature and non-repudiation, etc. For different services, the security concerns might be specifically designed depends the service feature, scenarios, and special requirements, etc.

4 Security Concerns in IoT Applications

The IoT enables information gathering, transmitting, and storing be available for devices in many scenarios, which creates or accelerates many applications such as industrial control systems, retailing industry, smart shelf operations, healthcare, food and restaurant industry, logistic industry, travel and tourism industry, library applications, etc. It can also be foreseen that the IoT will greatly contribute to address the important issues such as business model, healthcare monitoring systems, daily living monitoring, and traffic congestion control.

For applications in IoT, security and privacy are two important challenges. To integrate the devices of sensing layer as intrinsic parts of the IoT, effective security technology is essential to ensure security and privacy protection in various activities such as personal activities, business processes, transportations, and information protection. In this section, we will focus on following five typical applications to address the potential security challenges.

4.1 Security Concerns in Supervisory Control and Data Acquisition (SCADA) systems

SCADA systems are generally designed as more technical-oriented solutions often in the industrial environment with the sole intent to monitor processes without considering the security requirements and the needs to protect them from external threats (Perna 2013). The SCADA systems are believed to play a huge role in industrial applications of IoT (Di Pietro et al. 2014). A SCADA could contain multiple elements: supervisory systems, programmable logic controllers (PLCs), human-machine interface (HMI), remote machine telemetry units (RTUs), communication infrastructure, and various process and analytical instrumentation. From a security viewpoint, an attacker could target each of the above elements to compromise a SCADA system. In order to ensure the integration of SCADA systems into IoT, secure SCADA protocols should be designed to be able to connect with IoT environments. However this could raise the following security concerns (Bamforth 2014; Kim 2012; Perna 2013):

- Authentication and access control. To ensure secure communication, strong authentication must be implemented to allow access to main functionalities; On the other hand, authenticating and access control can well identify and assess the information sources.
- Identification of SCADS vulnerabilities. It is important to implement proper countermeasures and take corrective actions as appropriate. The software in SCADA should be regularly updated to tackle the security vulnerabilities.
- Physical security. In SCADAs, physical security protection must be carefully evaluated for each component and each component is recommended to meet NIST FIPS standards.
- System recovery and backups. The SCADAs should be designed to be able to rapidly recover from disaster or compromised status.

4.2 Security concerns in Enterprise information systems

Most companies have fulfilled their missions of installing enterprise information systems within the companies in the last two decades. These enterprise information systems have played the pivotal role in modern organizations existing as Enterprise Resource Planning (ERP) systems which integrated intra-organizational business processes, supply chain management systems that link inter-organizational business processes, and Customer Relationship Management (CRM) systems that maintain relationships with customers (Li 2011). Although the direct financial benefits and business performance of enterprise systems usage are still in controversy according to a series of studies conducted to investigate the enterprise system usage and organizational performance (Hendricks et al. 2007; Hitt et al. 2002; Wieder et al. 2006), most of them reported that enterprise systems usage cause positive impact on organizational operations by improving decision making processes, and most importantly, integrating information and resources of an organization into one system. Centralizing information and resources is thus identified as the most important factor for adopting enterprise systems. Looking back historically, it's the technology innovation that moves the enterprise systems wave forward. The increasing processing power of servers and PCs in the last two decades has enabled the client/server architecture for enterprise systems. It could be foreseen that the increased processing power will shift to small embedded-devices such as RFID tags, which could be widely implemented in many physical objects, leading to the new type of IOT enabled enterprise systems. The new IoT enabled enterprise systems extend the current systems and could gather more integrated data and information, bringing the security challenges to a new level. As most enterprise systems are installed inside organizations' intranets, the traditional security issues for enterprise systems mainly involve the identification process for users to access the system (Wieder et al. 2006). However, the IoT enabled enterprise systems incorporate sensors into the enterprise systems and will involve more security challenges than the traditional enterprise systems because the data and information carried by the sensors might go beyond the enterprise system physically. For example, the collaborative warehouse implemented with the IoT technology gather data from the warehouse outside the ERP system and communicates with the ERP systems through different protocols (Wang et al. 2013). This new architecture of enterprise systems require the security concerns to focus more on the sensor layer as well as the middleware layer because both there might be issues of data breach at these layers. For the application layer where the IoT applications might interact with the enterprise systems, special attention shall be given to identity authentication and application architecture because this layer is more vulnerable than other layers.

4.3 Security concerns in Social IoT

Social IoT is the spread and diffusion of IoT applications into societal level. Similarly to the socialization of many other technologies, IoT played an important role at the societal level. It will influence every part of our life from entertainment to energy usage. For example, wearable devices such as google glasses will be very popular in the foreseeable future and the popular UP wristband by Jawbone has proven how popular the wearable devices could be. Other applications such as smart TV, smart meter, and smart home devices all implying a new digital world enabled by IoT is coming. IoT will make our worlds more connected as the connected car and many other connected devices are on the road (Atzori et al. 2012). However, IoT technology alone won't be able to fulfil the task rather, other technologies have to be considered together to function as an integrated process. Social media and mobile APPs all played key role in this socialization of IoT part. In the future, we could see us all connected through social networks and social IoT devices. Security would be an essential part for the social IoT. As we are entering a new digital world enabled by the IoT, security issues in this digital world are a new challenge compared to the previous internet security. Previous internet security mainly focuses on the security protocols, antivirus software implementation, and firewalls etc. The Social IoT security shall has some similarity to the internet security in that they both shall have the security protocols but the social IoT security might involve more complex issues because the social IoT needs to integrate the heterogynous devices together. How to manage the interactions among all these heterogynous devices become the top issue for the social IoT security. Data and information communicated over the IoT network need to be managed through a reliable framework. Ethical issues such as privacy, data access right, the degree of openness of data will all influence how the security architecture for social IoT to be constructed. When more and more devices are connected together, the traffic of data over the social IoT will also become a big issue. How to effectively design the traffic so that data over social IoT could be transferred securely in a reliable way will also become challenging.

4.4 Confidentiality and security for IoT based Healthcare

The IoT motives *eHealthcare* and mobile healthcare integrated into IoT based Healthcare, which covers traditional internet-enabled healthcare applications (such as e-Pharmacy, e-Care, mobile healthcare, etc.). Similar to the social IoT Security, the healthcare IoT security will involve integration of multi-source data and information distributed over both the internet and evolving IoT. As the healthcare is a highly sensitive yet personal area dealing with much private information from patients, especially the vulnerable group of people, the security design shall be paid more attention than many other IoT networks. For this reason, data confidentiality and data security might emerge as the most important two factors to be considered when design the healthcare security architecture. Other factors such as reliability (anti-hacker, anti-virus, etc), design issues (such as signature, authentication, etc.), and compliance issues shall also be carefully considered. In addition to the previous factors, healthcare security is different from other industries, which features:

- Not bilateral condition;
- Regulated;
- Community interested;
- Legal issues

For these reasons, the design of the healthcare security system shall adopt a more reliable approach. The current healthcare-specific security standards include following four parts:

- Authentication, identification, signature, non-reputation
- Data integrity, encryption, data integrity process, permanence
- System security, communication, processing, storage, permanence
- Internet security, personal health records, secures Internet services.

In IoT-based healthcare system, the security issues include:

- Security for patient confidentiality
- Security that enables electronic health records (authentication, data integrity)
- Transmission security,
- Security in healthcare data access, processing, storage, etc.

5 Summary

Security at both the physical devices and service-applications is critical to the operation of IoT, which is indispensable for the success of IoT. Open problems remain in a number of areas, such as security and privacy protection, network protocols, standardisation, identity management, trusted architecture, etc. In this paper, we analyse the security requirements and potential threats in a four-layer architecture, in terms of general devices security, communication security, network security, and application security. The security challenges in enabling technologies of IoT also are reviewed. In future research, the security strategies for IoT should be carefully designed by managing the tradeoffs among security, privacy, and utility to provide security in multi-layer architecture of IoT.

References

Alcaraz, C., and Lopez, J. (2010), "A Security Analysis for Wireless Sensor Mesh Networks in Highly Critical Systems," *IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews,* , Vol. 40, No. 4, pp. 419-428.

Atzori, L., Iera, A., and Morabito, G. (2010), "The Internet of Things: A Survey," *Computer networks*, Vol. 54, No. 15, pp. 2787-2805.

Atzori, L., Iera, A., Morabito, G., and Nitti, M. (2012), "The Social Internet of Things (Siot)–When Social Networks Meet the Internet of Things: Concept, Architecture and Network Characterization," *Computer Networks*, Vol. 56, No. 16, pp. 3594-3608.

Bamforth, R. (2014), "Internet of Things, Scada, Ipv6 and Social Networking," http://www.it-director.com/business/innovation/content.php?cid=14590, Retrieved 14th December 2013.

Bi, Z., Xu, L., and Wang, C. (2014), "Internet of Things for Enterprise Systems of Modern Manufacturing," *IEEE Transactions on Industrial Informatics*, Vol. 10, No. 2, pp. 1537 - 1546.

Bottani, E., and Rizzi, A. (2008), "Economical Assessment of the Impact of Rfid Technology and Epc System on the Fast-Moving Consumer Goods Supply Chain," *International Journal of Production Economics*, Vol. 112, No. 2, pp. 548-569.

Broll, G., Rukzio, E., Paolucci, M., Wagner, M., Schmidt, A., and Hussmann, H. (2009), "Perci: Pervasive Service Interaction with the Internet of Things," *IEEE Internet Computing*, Vol. 13, No. 6, pp. 74-81.

Cai, H., Xu, L., Xu, B., Xie, C., Qin, S., and Jiang, L. (2014), "Iot-Based Configurable Information Service Platform for Product Lifecycle Management," *IEEE Transactions on Industrial Informatics*, Vol. 10, No. 2, pp. 1558-1567.

CCSA. (2012), "Security Requirements of Internet of Things." from ftp://ftp.onem2m.org/Pool/CCSA/YDB 101-2012 Security Requirements of Internet of Things .pdf

Chen, Y., Han, F., Yang, Y.-H., Ma, H., Han, Y., Jiang, C., Lai, H.-Q., Claffey, D., Safar, Z., and Liu, K.R. (2014), "Time-Reversal Wireless Paradigm for Green Internet of Things: An Overview," *IEEE Internet of Things Journal*, Vol. 1, No. 1, pp. 81-98.

Choi, J., Li, S., Wang, X., and Ha, J. (2012), "A General Distributed Consensus Algorithm for Wireless Sensor Networks," *Wireless Advanced (WiAd), 2012*, London, United Kingdom: IEEE, pp. 16-21.

Council, N. (2008), "Disruptive Civil Technologies: Six Technologies with Potential Impacts on Us Interests out to 2025," *Conference Report CR*.

Di Pietro, R., Guarino, S., Verde, N., and Domingo-Ferrer, J. (2014), "Security in Wireless Ad-Hoc Networks–a Survey," *Computer Communications*, Vol. 51, No., pp. 1-20.

EPCglobal, E. (2004), "Radio-Frequency Identity Protocols Class-1 Generation-2 Uhf Rfid Protocol for Communications at 860 Mhz–960 Mhz Version 1.0. 9." 65, from http://www.gs1.org/gsmp/kc/epcglobal/uhfc1g2/uhfc1g2_1_0_9-standard-20050126.pdf

Esad-Djou, M. (2014), "It-Security: Weblogic Server and Oracle Platform Security Services (Opss)," http://thecattlecrew.wordpress.com/2014/02/17/it-security-weblogic-server_1/, Retrieved 5 July 2014.

Fielding, R.T., and Taylor, R.N. (2002), "Principled Design of the Modern Web Architecture," *ACM Transactions on Internet Technology (TOIT)*, Vol. 2, No. 2, pp. 115-150.

Floerkemeier, C., Roduner, C., and Lampe, M. (2007), "Rfid Application Development with the Accada Middleware Platform," *IEEE Systems Journal*, Vol. 1, No. 2, pp. 82-94.

Frenken, T., Spiess, P., and Anke, J. (2008), *A Flexible and Extensible Architecture for Device-Level Service Deployment*. Springer.

Furnell, S. (2007), "Making Security Usable: Are Things Improving?," *Computers & Security*, Vol. 26, No. 6, pp. 434-443.

Gama, K., Touseau, L., and Donsez, D. (2012), "Combining Heterogeneous Service Technologies for Building an Internet of Things Middleware," *Computer Communications*, Vol. 35, No. 4, pp. 405-417.

Gaur, H. (2013), "Internet of Things: Thinking Services," https://blogs.oracle.com/IOT/entry/internet_of_things_thinking_services, Retrieved 5 July 2014.

Gu, L., Wang, J., and Sun, B. (2014), "Trust Management Mechanism for Internet of Things," *China Communications*, Vol. 11, No. 2, pp. 148-156.

Guinard, D., Trifa, V., Karnouskos, S., Spiess, P., and Savio, D. (2010), "Interacting with the Soa-Based Internet of Things: Discovery, Query, Selection, and on-Demand Provisioning of Web Services," *IEEE Transactions on Services Computing* Vol. 3, No. 3, pp. 223-235.

He, W., Xu, L., and Li, S. (2012), "Integration of Distributed Enterprise Applications: A Survey," *IEEE Transactions on Industrial Informatics*, Vol. 10, No. 1, pp. 35-42.

Hendricks, K.B., Singhal, V.R., and Stratman, J.K. (2007), "The Impact of Enterprise Systems on Corporate Performance: A Study of Erp, Scm, and Crm System Implementations," *Journal of Operations Management*, Vol. 25, No. 1, pp. 65-82.

Hepp, M., Siorpaes, K., and Bachlechner, D. (2007), "Harvesting Wiki Consensus: Using Wikipedia Entries as Vocabulary for Knowledge Management," *IEEE Internet Computing*, Vol. 11, No. 5, pp. 54-65.

Hernandez-Castro, J.C., Tapiador, J.M.E., Peris-Lopez, P., Li, T., and Quisquater, J.-J. (2013), "Cryptanalysis of the Sasi Ultra-Light Weight Rfid Authentication Protocol," *arxiv*, Retrieved 20 May 2013.

Hitt, L.M., Wu, D., and Zhou, X. (2002), "Investment in Enterprise Resource Planning: Business Impact and Productivity Measures," *J. of Management Information Systems*, Vol. 19, No. 1, pp. 71-98.

Hoyland, C.A., M. Adams, K., Tolk, A., and D. Xu, L. (2014), "The Rq-Tech Methodology: A New Paradigm for Conceptualizing Strategic Enterprise Architectures," *Journal of Management Analytics*, Vol. 1, No. 1, pp. 55-77.

HP Company. (2014), "Internet of Things Research Study," http://h30499.www3.hp.com/hpeb/attachments/hpeb/application-security-fortify-on-demand/189/1/HP_IoT_Research_Study.pdf, Retrieved 5 September 2014.

ITU. (2013), "The Internet of Things, International Telecommunication Union (Itu) Internet Report."

Kang, K., Pang, Z., Da Xu, L., Ma, L., and Wang, C. (2014), "An Interactive Trust Model for Application Market of the Internet of Things," *IEEE Transactions on Industrial Informatics*, Vol. 10, No. 2, pp. 1516-1526.

Keoh, S., Kumar, S., and Tschofenig, H. (2014), "Securing the Internet of Things: A Standardization Perspective," *IEEE Internet of Things Journal*, Vol. 1, No. 3, pp. 265-275.

Kim, H. (2012), "Security and Vulnerability of Scada Systems over Ip-Based Wireless Sensor Networks," *International Journal of Distributed Sensor Networks*, Vol. 2012, No. Article ID 268478.

Kranenburg, R.v., Anzelmo, E., Bassi, A., Caprio, D., Dodson, S., and Ratto, M. (2011), "The Internet of Things," *1st Berlin Symposium on Internet and Society.(Versión electrónica). Consultado el.*

Li, D.X. (2011), "Enterprise Systems: State-of-the-Art and Future Trends," *IEEE Transactions on Industrial Informatics*, Vol. 7, No. 4, pp. 630-640.

Li, F., and Xiong, P. (2013), "Practical Secure Communication for Integrating Wireless Sensor Networks into the Internet of Things," *IEEE Sensors Journal*, Vol. 13, No. 10, pp. 3677 - 3684.

Li, L., Li, S., and Zhao, S. (2014a), "Qos-Aware Scheduling of Services-Oriented Internet of Things," *IEEE Transactions on Industrial Informatics*, Vol. 10, No. 2, pp. 1497 - 1505.

Li, L., Wang, B., and Wang, A. (2014b), "An Emergency Resource Allocation Model for Maritime Chemical Spill Accidents," *Journal of Management Analytics*, Vol., No. ahead-of-print, pp. 1-10.

Li, S., Da Xu, L., and Zhao, S. (2014c), "The Internet of Things: A Survey," *Information Systems Frontiers*, Vol., No., pp. 1-17.

Li, S., Sun, H., Nallanathan, A., Xu, L., Zhao, S., and Sun, Q. (2014d), "Industrial Wireless Sensor Networks," *International Journal of Distributed Sensor Networks*, Vol. 2014, No. 2014, pp. 2-3.

Lim, M.K., Bahr, W., and Leung, S.C. (2013), "Rfid in the Warehouse: A Literature Analysis (1995–2010) of Its Applications, Benefits, Challenges and Future Trends," *International Journal of Production Economics*, Vol. 145, No. 1, pp. 409-430.

Miorandi, D., Sicari, S., De Pellegrini, F., and Chlamtac, I. (2012), "Internet of Things: Vision, Applications and Research Challenges," *Ad Hoc Networks*, Vol. 10, No. 7, pp. 1497-1516.

Ning, H. (2013), *Unit and Ubiquitous Internet of Things*. CRC Press.

Ning, H., Liu, H., and Yang, L.T. (2013), "Cyberentity Security in the Internet of Things," *Computer*, Vol. 46, No. 4, pp. 0046-0053.

Oppliger, R. (2011), "Security and Privacy in an Online World," *Computer*, Vol. 44, No. 9, pp. 21-22.

Peris-Lopez, P., Hernandez-Castro, J.C., Estevez-Tapiador, J.M., and Ribagorda, A. (2006), "M2ap: A Minimalist Mutual-Authentication Protocol for Low-Cost Rfid Tags," in *Ubiquitous Intelligence and Computing*. Springer, pp. 912-923.

Perna, M. (2013), "Security 101: Securing Scada Environments," http://blog.fortinet.com/post/security-101-securing-scada-environments, Retrieved 5 July 2014.

Pretz, K. (2013), "The Next Evolution of the Internet," http://theinstitute.ieee.org/technology-focus/technology-topic/the-next-evolution-of-the-internet, Retrieved 20 May 2013.

Raza, S., Shafagh, H., Hewage, K., Hummen, R., and Voigt, T. (2013), "Lithe: Lightweight Secure Coap for the Internet of Things," *IEEE Sensors Journal*, Vol. 13, No. 10, pp. 3711 - 3720.

Raza, S., Voigt, T., and Jutvik, V. (2012), "Lightweight Ikev2: A Key Management Solution for Both the Compressed Ipsec and the Ieee 802.15. 4 Security," *Proceedings of the IETF Workshop on Smart Object Security*, Paris, France.

Roe, D. (2014), "Top 5 Internet of Things Security Concerns," http://www.cmswire.com/cms/internet-of-things/top-5-internet-of-things-security-concerns-026043.php, Retrieved 5 September 2014.

Roman, R., Najera, P., and Lopez, J. (2011), "Securing the Internet of Things," *Computer*, Vol. 44, No. 9, pp. 51-58.

Roman, R., Zhou, J., and Lopez, J. (2013), "On the Features and Challenges of Security and Privacy in Distributed Internet of Things," *Computer Networks*, Vol. 57, No. 10, pp. 2266-2279.

Sundmaeker, H., Guillemin, P., Friess, P., and Woelfflé, S. (2010), *Vision and Challenges for Realising the Internet of Things*. EUR-OP.

Tan, W., Chen, S., Li, J., Li, L., Wang, T., and Hu, X. (2014), "A Trust Evaluation Model for E - Learning Systems," *Systems Research and Behavioral Science*, Vol. 31, No. 3, pp. 353-365.

Tao, F., Cheng, Y., Xu, L.D., Zhang, L., and Li, B.H. (2014), "Cciot-Cmfg: Cloud Computing and Internet of Things Based Cloud Manufacturing Service System," *IEEE Transactions on Industrial Informatics*, Vol. 10, No. 2, pp. 1435 - 1442.

Wang, F., Ge, B., Zhang, L., Chen, Y., Xin, Y., and Li, X. (2013), "A System Framework of Security Management in Enterprise Systems," *Systems Research and Behavioral Science*, Vol. 30, No. 3, pp. 287-299.

Wang, K., and Wu, M. (2010), "Cooperative Communications Based on Trust Model for Mobile Ad Hoc Networks," *IET Information Security*, Vol. 4, No. 2, pp. 68-79.

Weber, R.H. (2013), "Internet of Things–Governance Quo Vadis?," *Computer Law & Security Review*, Vol. 29, No. 4, pp. 341-347.

Welbourne, E., Battle, L., Cole, G., Gould, K., Rector, K., Raymer, S., Balazinska, M., and Borriello, G. (2009), "Building the Internet of Things Using Rfid: The Rfid Ecosystem Experience," *IEEE Internet Computing*, Vol. 13, No. 3, pp. 48-55.

Wieder, B., Booth, P., Matolcsy, Z.P., and Ossimitz, M.-L. (2006), "The Impact of Erp Systems on Firm and Business Process Performance," *Journal of Enterprise Information Management*, Vol. 19, No. 1, pp. 13-29.

Xiao, G., Guo, J., Xu, L., and Gong, Z. (2014), "User Interoperability with Heterogeneous Iot Devices through Transformation," *IEEE Transactions on Industrial Informatics*, Vol. 10, No. 2, pp. 1486-1496.

Xu, B., Xu, L.D., Cai, H., Xie, C., Hu, J., and Bu, F. (2014a), "Ubiquitous Data Accessing Method in Iot-Based Information System for Emergency Medical Services," *IEEE Transactions on Industrial Informatics*, Vol. 10, No. 2, pp. 1578-1586.

Xu, L., He, W., and Li, S. (2014b), "Internet of Things in Industries: A Survey," *IEEE Transactions on Industrial Informatics*, Vol. PP, No. 99, p. 1.

Xu, L.D. (2011), "Information Architecture for Supply Chain Quality Management," *International Journal of Production Research*, Vol. 49, No. 1, pp. 183-198.

Yao, X., Han, X., Du, X., and Zhou, X. (2013), "A Lightweight Multicast Authentication Mechanism for Small Scale Iot Applications," *IEEE Sensors Journal*, Vol. 13, No. 10, pp. 3693-3701.

Yuan Jie, F., Yue Hong, Y., Li Da, X., Yan, Z., and Fan, W. (2014), "Iot-Based Smart Rehabilitation System," *IEEE Transactions on Industrial Informatics*, Vol. 10, No. 2, pp. 1568-1577.

Biographical Details

Shancang Li, is a Research Assistant with the Faculty of Engineering, University of Bristol, Bristol, 683 U.K., and a Member of the Cryptography Research Group. His current research interests include mobile 685 security, wireless sensor networks, Internet of Things, and applications of wireless technologies.

Theo Tryfonas, is a senior lecturer in Faculty of Engineering, University of Bristol. His current research interests include modelling cyber-capability with system dynamics and applications of game theory to the analysis of cyber attacks. Dr. Tryfonas is a Chartered IT Professional Member of the British Computer Society (BCS) and is a Certified Information Systems Auditor.

Honglei Li, is a senior lecturer in Northumbria University. Her research interests broadly fall into two topics - virtual communities and business process management.