Internet of Things: A Survey of Existing architectural models and their security Protocols

Nidal M. Turab

Al-Ahliyya Amman University,
Amman- Jordan

Abstract
The Internet of Things IoT is a new era in the cyber space, it is defined as a global network where every single entity or subject on the planet will be connected to the Internet. As any new technology or trend there will be a need for a reference architecture model to resolve compatibility issues between different parties. This paper aims to provide a literature review of the existing IoT architectural models and their security features. It will directly support researchers in their understanding of developments in the domain of IoT architectural models, thus enabling them to propose novel ideal models that can address the limitations of existing models.

Key-words:
Internet of Things, GS1 EPCglobal framework, IoT-A Reference architecture, Industrial Internet Reference Architecture IIRA, Arrowhead Framework, IEEE P2413 Standard Architectural Framework for the (IoT).

1. Introduction

The IoT implies that every object or entity in the universe will have digital identity (in the form of IP) with sufficient intelligent connection and communication to other objects or entities. Every day there is a new IoT enabled product in the market and new application of the IoT; some of IoT applications are: smart wearables, smart houses, smart power grid, smart connected car, smart digital health (Telehealth), smart supply chain, smart agriculture, smart cities and much more. Such wide intelligent space rises the need to give a standard definition and architectural model for the IoT that will adopt the huge number of hardware, software, structuring and modeling of IoT objects and domains [1]. Not all applications will need every single detail of the reference architecture. Nevertheless, architectural reference model will have its concerns of security and privacy.

Recently, several papers study some IoT reference models: [2] proposed the Business Operation Support Platform (BOSP) on the IoT, and indicated that the BOSP operations requires IoT services. [1] reviewed some architectures of IoT (IIRA and IoT-A); they compared the capabilities and layers of these architectures regarding of three perspectives views: semantic Orientation, Internet orientation and the things orientation. [3] provided recommendations of the best areas of research that will address weaknesses in IoT systems, polices , practices and tools. [4] reviewed and summarized some IoT technologies and architectures such as: European FP7 Research Project, ITU Architecture, IoT Forum Architecture, Qian Xiaocong, Zhang Jidong Architecture and Kun Han, et al architecture. The authors reassess two theoretical generic models: a primitive four layered structure, and a five layered structure. Consequently, they come up with a proposed architecture comprising of six layers. [5] demonstrated some of IoT security problems and solutions of IoT, and stated that "IoT security is an integration of several security layers". [6] reviewed some IoT technologies, protocols and applications, with description of application-use typical protocol integration scenarios to deliver desired IoT services. [7] reviewed and reported some of protocols, algorithms, and possible solutions of IoT issues and the relevance between theose issues.

The aim of this paper is to introduce a literature review of existing IoT reference architecture with a comparative study of their associated security concerns and solutions. This, in turn, should provide a good establishment for researchers who are interested in understanding of IoT architectures and their security protocols. The paper is organized as follows: Section 2 describe the literature search methodology used in this paper. Section 3 presents an overview of the existing IoT reference architectural models including: The GS1 EPCglobal, IoT-A, Industrial Internet Reference Architecture (IIRA), Arrowhead, and IEEE P2413 standard architectural frameworks. Section 4 studies the security features of the IoT reference models, and the final section is left for conclusions.

2. Method of Literature Search

The information reported in this review was obtained from different online databases and search engines

Manuscript received May 5, 2017
Manuscript revised May 20, 2017

including Scopus, Google, and Google Scholar. Keywords and expressions used for the search included EPCglobal, IoT-A, IIRA and IEEE P2413 and similar pre-identified terms were used in separate searches and in conjunction with each other to identify all related publications. Related publications published in English including Journal papers, books and reports were scrutinized to identify those that met a criteria of presenting information accredited to the purpose of this review. After elimination of studies that were not relevant to the subject matter, a total of forty-nine articles were reviewed and cited, seven of them had been studied and summarized in this study,

3. Overview of the Existing IoT architectural models

3.1 The GS1 EPCglobal Architecture Framework

GS1 is an international non-profit organization; that is responsible for standardizing barcodes that are widely used around the world [8]. The Electronic Product Code (EPC) assigns any physical object or entity with is a universal identifier with a unique name (identity), this non-repetitive name is independent of the geographical location of the object or time (it can last forever), this unique identifier can be used to track the entity. The EPCglobal Tag Data Standard [TDS1.9] describes in details the Electronic Product Code (EPC) [9]. GS1 general specifications defines keys to identify objects, unique objects and hybrid objects that may identify either categories or unique objects depending whether or not their object have serial number. In addition, there are two keys to identify logical grouping of objects [10].

Architecture framework is a vendor neutral manner and open, that is a collection of hardware, software, and data standards [11, 12]. The framework aims to recite and show the relations between the standards of the data, hardware and software that are part of the EPCglobal architecture framework to provide structured guidance to any person aiming to use EPCglobal architecture framework services such as technology vendors and end users and to explain the underlying principles of the standards and service components [13]. An important question here is who is responsible for issuing the EPC? The answer is that the EPC either issued by the Issuing Agency that produces the entity (object) or by an Issuing Organization that reserved one or more blocks of the EPC name space of the Issuing Agency. It may happen that the Issuing Organization delegates another organization to issue EPC provided that the uniqueness is guaranteed [8, 9, 14].

3.2 IoT- A Reference architecture

One of the most important IoT architecture model is the IoT-A architectural reference model. IoT-A is an European Lighthouse Integrated Project that addresses the architecture of IoT, and creates an architectural reference model that defines the key building blocks of IoT. IoT-A composed of four components: The first component is the reasons for providing an IoT architectural reference model, methodology and usage; the second component is the knowledge of businesses ambitions came from both business stakeholders (those stakeholders were representative of different business domains interested in IoT: Automotive, Service Integrators, Health Care Logistics, Telecom Operators etc.) and the ITU-A IoT Internal partners (those are a specialist in object of IoT, communication, lookup & discovery, and in IoT-objects) [15]. The third component is the understanding of the IoT domains; the IoT reference model is similar to the architecture in OASIS reference model (Organization for the Advancement of Structured Information Standards) [16] . Finally, the fourth component is providing perspectives and views on different architectural portions that concern the IoT stakeholders:

- The view is defined as “a model to what areas are of interest for the stakeholders.” [17]. The view contains: Functional, Deployment, Information and Operation.
- The prospective is defined as “a collection of activities, considered points, guidelines and strategies to ensure that some system properties are important for the architecture views” [18]. Prospective includes: availability and resiliency, growth and interoperability, privacy and security and finally scalability and performance.

It should be noted that only functional views and security and privacy perspectives are described in the reference architecture, other views and perspectives are left for future development [19]. The next subsequent section will discuss the functional views in more details, while security and privacy perspectives will be discussed in sub section 4.1.

3.2.1 Functional view

The functional components in the IoT-A reference architectural model are divided into seven functional groups [20, 21]:

Applications: This group describes the applications functionalities; these functionalities are at the top of any of IoT-A architecture based implementation.

Virtual Entity (VE) and information: This group is responsible of organizing the information related to physical entities and ways to enable search for services of these entities resources.

Process execution and service synchronization: This group is responsible for organizing the IoT resources and ensures that the resources are available to any services or entities.

IoT service & resource: this group retunes descriptions about queried services with links to exposed services.

Management: this functional group manages the computational resources.

Device communication and connectivity: This group provides the set of rules to enable IoT devices to communicate and connect to a network. Also, this group deals with content-based routing.

Security group: this group is applied by the different functional groups. Access control and privacy are the two important factors here; access-control policies shall be enforced to ensure that sensitive resources are accessed by only authorized entities. Also, privacy shall be enforced by using different identities to access the IoT services, in the specifications this is termed as pseudonymity [22].

3.3 Industrial Internet Reference Architecture IIRA

The Industrial Internet is an Internet connecting trillions of addressable devices found everywhere globally to represent every single physical entity. IIRA is an open architecture standard-based for Industrial Internet Systems (IISs). The ISO/IEC/IEEE 42010:2011 standard specification [23] systemizes the common conventions used in. The common conventions and constructs in the specification are: concern, architecture and architecture framework, viewpoint, and stakeholder. The term concern refers to any topic of interest relating to the system; which can be a stakeholder refers to any individual organization or team interested in a system [19], or it can be a viewpoint consists of the analysis and description a specific system concerns.

3.3.1 Industrial Internet Viewpoints

The Industrial Internet Systems (IIS) specifications classify the IoT concerns as four viewpoints: business, usage, functional and implementations [4, 18]:

The business viewpoint presents business vision and objectives to the concerns stakeholders. These concerns are business-oriented and important for industry decision-makers, engineer, etc.

- The usage viewpoint deals with the expected system usage concerns. These concerns typically represented typically logical or human users who deliver the system intended functionality.
- The functional viewpoint deals with the interrelation, interaction and structure of the IIS functional components.
- The implementation viewpoint deals with their communication schemes and their lifecycle procedures of the technologies needed to implement functional components.

3.4 Arrowhead Framework

The aim of the Arrowhead frame work is to enable interoperability between any IoT industrial devices which are normally diverse; this automation is based on the Service Oriented Approach SOA. The Arrowhead frame targets five domains: Production, Smart Buildings and infrastructures, Electro mobility, Energy production and End user services Energy. Arrowhead frame Enables the integrity and interoperability of services between and IoT device. Also, it aims to address the challenges associated with cooperative automation such as: integration with legacy systems, provide technical framework for IoT devices functions and performance [24, 25].

3.5 IEEE P2413 Standard Architectural Framework for the (IoT)

This IEEE standard defines an IoT reference framework, defining descriptions of various IoT domains (transportation, healthcare, etc.) and their abstraction and shared attributes. This standard emphasizes on the four elements of the trust: safety, security, privacy and protection [3]. The following paragraphs give a brief description of the IEEE standards related to of IoT security.

1- The first series is the IEEE 1363 family of standards used for public key cryptography. This family of standards composed of four members:
   a) IEEE 1363-2000 (IEEE Standard Specifications for Public-Key Cryptography): The standard covers cryptographic schemes based on public-key such as: public and private keys, the mathematical derivation of secret key, digital signature and public-key encryption [26].

b) IEEE 1363.1-2008 (Standard Specification for Public Key Cryptographic Techniques Based on Hard Problems over Lattices): it uses public and private keys, the mathematical derivation of secret key, digital signature and public-key encryption [27].

c) IEEE 1363.2-2008 (IEEE Standard Specification for Password-Based Public-Key Cryptographic Techniques): This includes specifications of for password-based authentication and key establishment. Also, it including schemes for key agreement and retrieval [28].

d) IEEE 1363.3-2013 (IEEE Standard for common Identity-Based Public-Key Cryptographic Techniques): it uses public and private keys, the mathematical derivation of secret key, digital signature, pairings and public-key encryption [29].

2- The second series is the IEEE 1619 family of standards used for encryption in storage media. This family of standards is composed of three members:

- IEEE 1619-2007 (IEEE Standard for Cryptographic Protection of Data on Block-Oriented Storage Devices): this standard specifies mechanisms for authenticating and encrypting data in storage devices with fixed data length [30].
- IEEE 1619.1-2007 (IEEE Standard for Authenticated Encryption with Length Expansion for Storage Devices): this standard contains procedures for authenticating and encrypting data for storage devices capable of expanding data length, some of these devices are tape drives. These procedures include the CCM, GCM, CBC-HMAC, and XTS-HMAC cryptographic modes of the AES block cipher [30].

3- IEEE 1619.2-2010 (IEEE Standard for Cryptographic Protection of Data stored on Shared Storage Media): this standard describes procedures for encrypting storage devices with random access random access storage. These procedures include the EME2-AES and XCB-AES with Encoded Archival Description (EAD) modes of the AES block cipher [31].

4. Security Features of the IoT Architectural Models

Security of the IoT architecture should be applies to different levels [32]. The security challenges resulted from the diverse nature of billions of IoT connected devices and their use of standard security protocols. The security threats in IoT can be summarized as follows [7, 33]:

- Threats that related to the physical nature of IoT devices such as: IoT devices malicious cloning, and malicious replacement of IoT devices.
- Threats resulted from the fact that IoT connected objects will exchange data among them: such as eavesdropping, routing and man-in-the-middle attacks.
- Threats related to the nature of the sensitivity and confidentiality of the exchanged data such as denial-of-service attacks, and privacy threats.

IoT reference architectures must contain a description of the common security functions, measures and protocols as described in the international standard Common Criteria for Information Technology Security Evaluation [34] to ensure the following security properties:

- Authentication: data came from trusted and known source.
- Authorization: data access and modification privileges are granted to authorized entity (e.g. authenticated users)
- Availability: the communicating entities are always available and reachable
- Integrity: transmitted data are not modified or deleted during transmission.
- Confidentiality: data can be accessed and read only by authorized communicating entities.

This section will discuss the security functions offered by of the IoT architectures, and how they implement each function.

4.1 IoT-A

IoT-A D4.2 security reference model defines the security components as : Authentication, authorization, trust and repudiation architecture, Identity management , key management and exchange [35]. The reference model composed of three layers: Application, communication and security. The security perspectives are dealing with security and privacy at communication level and at the application-layer. In IoT-A architecture, any entity requires accessing resources requires a valid identity, in case of human user this is called Active digital entity while in case of something stored in a file or a database entry it is called passive Id. Authentication

functionality can be either local or server based, the authentication functionality can be invoked by different entities like:

- A user needs to confirm his ID to gain access to IoT-A resources and services.
- An IoT Service that plays the role of service provider and received authentication request from a user. furthermore, the IoT services provider will change its state from idle to active and want to join an IoT-A system securely.

The authorization functionality grants access rights that control the access privileges to an IoT-A resource or service based on the security policy that govern that resource or service. two authorization approaches have been identified

- On-the-fly: where the authorization functionality evaluates the access rights of a privileged user according to the access. This approach is suitable for all kind of resource.
- Credential-based: the user submits his credentials to get authorized privileges. This method is suitable for cases where the communication entities are not available all time [36].

In the IoT-A reference architectural model, IoT devices are classified as either constrained or unconstrained form the resources viewpoint (power supply, bandwidth, processing capabilities).

The constrained devices contain great incompatible communication technologies (such as functional and communication patterns between connected devices and auto-ID devices mentioned earlier) with their associated security solutions, this can lead to a general architecture design problem to encompass all these technologies. Besides, securing the communication at protocol level is very difficult which leads to the conclusion that the security features have to be balanced with the abovementioned limited resources [20, 36]. One solution can be is providing a high abstraction security model to mitigate these incompatibilities.

Authentication and Authorization (AA) system, based on X509 certificates and PKI, is used to achieve authentication, confidentiality and authorization. In PKI, Certificate Authority (CA) assigned the role of issuing, signing, and validating the contents of digital certificates; this CA is trusted by both communication parties. In IoT-A architecture, the certificates issued by CA provides security services such as secure communication, authorization in addition to trust and reputation. Key Exchange and Management (KEM) is used to creating, managing and distributing keys. The key can be either symmetric (in case of Machine to Machine M2M communication) or asymmetric (in case of Pseudonymisation (PN)). Encryption keys are stored in what is called key-exchange-management component while authentication keys are stored in certificate authority CA. Pseudonymisation (PN) or aliasation is a feature of authentication and authorization components of IoT-A that allows the creation and management of pseudonyms for either user who uses pseudonym for authentication process or an IoT services. The keys used by CA to issue aliases are created by Key Exchange and Management (KEM). KEM is responsible for the creation and management of both symmetric and asymmetric keys[37] .

4.2 GS1 EPCGlobal architecture:

Many security standards were created to address the shared security issues of the GS1 data (the v 1.9 tag data standard of GS1 specifies the data format of the EPC information be either in Uniform Resource Identifier (URI) that uniquely identities a specific physical or stored in its binary form). In EPCGlobal architecture, the entities include physical devices, services and users. The EPCglobal architecture framework allows variety of authentication mechanisms. However, the X.509 certificate based authentication will be the most used. The EPCglobal X.509 certificate profile provides a minimum cryptographic security requirements and parameters and concurrently clarifying and narrowing the existing authentication functionality [38].

The X.509 certification profile of EPCglobal network describes the authentication and certification processes of entities (users, servers/services, physical devices). For certificates the SHA2 with RSA public key encryption is used; as SHA2 family has different digest keys (224, 256, 348 and 512) any EPCglobal network compliant certificate can use any of SHA2 family. Also, the specifications profile requires the use of 2048-bit RSA encryption key size (till 31-12-2030); thereafter 3072-bit key size will be used. To ensure backward compatibility, the framework ratifies MD5 with RSA public key encryption [39, 40].

The EPCglobal standards use Transport Layer security TLS or HTTPS to provide authentication and authorization and exchanging certificates and keys for data encryption. One of the fundamental principles of the EPCglobal Architecture Framework is the Unique Identity in which every entity in EPCglobal has a unique and serialized ID, this unique identity is the Electronic Product Code EPC, defined by the EPCglobal Tag Data Standard [41].

The communication between the tag reader and reader device is specified by the Tag Air Interface. This interface is used to write and read data to and from an RFID tag. Legacy tags with limited resources can transmit EPC information over the air. To prevent such transmission, the Gen2 standard employs temporary identities or pseudonyms for communication with tags [8, 42].

4.3 IIRA

In IIRA, the enterprise systems are connected with the Industrial Internet and exchange data continuously with them. As the industrial security relies on physical security and the isolation of the ambiguity of heterogeneous industry communication protocols, they consequently suffer from significantly smaller attacks then Industrial Internet Systems. IISs integrates security approaches that span different layers of networks and physical domains (physical world includes physical security or direct observability, the network world includes the assigning access rights to data to legitimate users, the business world includes property rights) [23, 43].

To address security concerns of IIS, trust and privacy, end-to-end security capability, secure device-to-device communications, secure remote monitoring, management, and to assure that data is distributed securely; IIS viewpoints have the following security concerns[44]:

Concerns of the business viewpoint which are the cost factors, business risks, requirements of audit and regulatory.

Concerns of the usage viewpoint, security of IIS end-to-end activities, such as privileges.

Concerns of the functional viewpoint which are the assessment of security functions required to for secure operations and activities.

Concerns of the implementation viewpoint: assuring that security technologies are consistent with secure architectures.

Concerns of endpoints secure communication, secure data storage and exchange, and monitoring and managing the security mechanisms between endpoints.

In IIRA, the security requirements of information related to the industrial systems include: the verification of the identity of the communicating entities to ensure the integrity of the industrial data and using encryption to assure the confidentiality of the date at rest or while in transit. In addition, authentication ensures that the components are accessed by only intended entities. IIRA specifications mandate communication endpoints and users to perform mutual authentication and authorization before they can exchange data [45].

As there are numerous legacy systems that do not have security capabilities and can pose the security of the overall system, a proxy security gateway is used to provide minimum security requirements. This proxy security gateway bridges the legacy protocols and the new end protocols. The management of many endpoint credentials can be accomplished, updated and revoked automatically, remotely and securely by many security agents at the same time; this requires the use of X509 based certificate authorities and PKI. Existing PKI concerns of scalability and reliability and complexity of managing large number of IIS endpoints; emerging authentication schemes such as the DNS-based Authentication of Named Entities (DANE) (that allows Transport Layer Security (TLS) using to be confined to DNS names using Domain Name System Security Extensions (DNSSEC)) can deal with these concerns. [46]. As cryptography can prevent unauthorized access or modification of data, IIRA mandates the use of any encryption algorithms with symmetric or asymmetric keys. To assure data integrity the digital signature technique is used.

4.4 Arrowhead framework

As any communication environment, an Arrowhead can be subject to numerous threats. These threats may include (but not limited to): Denial of Services Attack DoS, any kind of spoofing (IP address Spoofing, MAC address Spoofing, ARP spoofing and DNS Server spoofing) and any form of tampering attacks (software, Web page); these threats can compromise the integrity of the IoT industrial connected devices [42]. As any distributed architecture, the authentication and authorization are not limited to one single entity but to be taken as including every single entity in the distributed system. the following concerns (issues) have to be solved [47]:

Confidentiality: means that access to data is granted only to authorized entities; information disclosure and spoofing are major concerns of confidentiality this can be mitigated by using proper encryption scheme along with proper authorization (checking the identity of the both communication entities).

a) Integrity: means that data is transmitted and arrived in the same manner as it was transmitted with no modification, tampering or modification. Integrity can be assured by using message integrity techniques such as MD

(Message Digest) or SHA (Secure Hash Algorithm).

b) Availability: is the probability that a system will work as expected and when required on the 24/7 basis; with no risk of Denial of Services theat.

c) Accountability: means that any entity in the system could not deny performing any action that could be harmful to the system.

As Arrowhead Framework deals with and supports variety of devices from very powerful servers to devices with constrained resources. Consequently, Arrowhead Framework offers two authentication and authorization systems:

- For devices with enough resources, Authentication and Authorization (AA) system, based on X509 certificates and Public Key Infrastructure (PKI), is used to achieve authentication, message integrity, confidentiality and authorization.
- For devices with constrained resources (such as wireless sensor networks), Authentication, Authorization and Accounting system (AAA) system, based on Radius tickets, is used. An AAA generates issues and validates unique tickets (a token with small number of bytes) for every communicating device. All Tickets have a timeout that determines when the ticket is expired and need to be reissued; depending on the network timeouts varies between one minute and two hours [48, 49].

Based on the above, Table 1 is derived to summarize the security features offered by each of the discussed IoT reference architectures.

Table 1: Security features offered by each of the IoT reference architectures.

Architecture	***Security Feature***				
	Authentication/ Authorization	***Availability***	***Integrity***	***confidentiality***	***pseudonym***
IoT-A	Authentication and Authorization (AA) system, based on X509 certificates	Availability and Resilience prospective	Digital Entity Either passive or active	Any encryption standard Using symmetric or asymmetric keys	pseudonyms Using KEM
GS1 EPCGlobal architecture	TLS or HTTPS To exchange CA keys		Unique Identity EPC	2048-bit and 3072-bit RSA encryption key	Gen2 standard employs temporary identities or pseudonyms
IIRA	Authentication and Authorization (AA) system, based on X509 certificates	Endpoint physical security, identity, access control and data protection	digital signature	Any encryption standard Using symmetric or asymmetric keys	
Arrowhead	Authentication and Authorization (AA) system, based on X509 certificates		Authentication and Authorization (AA) system, based on X509 certificates	Authentication and Authorization (AA) system, based on X509 certificates	
IEEE P2413	IEEE 1363 family: (1363, 1363.1, 1363.2)	IEEE 1363 family: (1363, 1363.1, 1363.2)	IEEE 1363.3 standard	IEEE 1619, IEEE 1619.1, IEEE 1619.2	

5. Conclusions

This paper presents an informative review of the existing IoT architectural models with their associated security perspectives. It provides a review of a number of the existing IoT architectural models, namely: IoT-A, GS1 EPCGlobal , IIRA, Arrowhead and IEEE P2413 architectures. Each model has been studied with emphasis on its security features. Based on this literature, it is obvious that there is a need for a standard architecture to compensate the vendor to vendor incompatibilities form the architectural and security perspectives, this standardization will ease the spread of IoT. Thus, this study will support researchers and enable them to propose novel ideal models in the domain of IoT

that can obtain the desired features and address the limitations of existing models.

References

[1] M. Weyrich and C. Ebert, "Reference architectures for the internet of things," IEEE Software, vol. 33, pp. 112-116, 2016.

[2] Q. Xiaocong and Z. Jidong, "Study on the structure of “Internet of Things (IOT)” business operation support platform," in Communication Technology (ICCT), 2010 12th IEEE International Conference on, 2010, pp. 1068-1071.

[3] R. Alur, E. Berger, A. W. Drobnis, L. Fix, K. Fu, G. D. Hager, et al., "Systems Computing Challenges in the Internet of Things," arXiv preprint arXiv:1604.02980, 2016.

[4] S. Madakam, R. Ramaswamy, and S. Tripathi, "Internet of Things (IoT): A literature review," Journal of Computer and Communications, vol. 3, p. 164, 2015.

[5] K. Zhao and L. Ge, "A survey on the internet of things security," in Computational Intelligence and Security (CIS), 2013 9th International Conference on, 2013, pp. 663-667.

[6] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: A survey on enabling technologies, protocols, and applications," IEEE Communications Surveys & Tutorials, vol. 17, pp. 2347-2376, 2015.

[7] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," Computer networks, vol. 54, pp. 2787-2805, 2010.

[8] F. A. J. Johnson, M. Harrison, B. H. G. US, J. Mitsugi, O. R. CVS, and K. Suen, "The GS1 EPCglobal Architecture Framework 2," 2005.

[9] T. D. Standard, "version 1.9," GS1 EPCglobal Standard, 2014.

[10] W. Wang, K. Lee, and D. Murray, "Building a generic architecture for the Internet of Things," in Intelligent Sensors, Sensor Networks and Information Processing, 2013 IEEE Eighth International Conference on, 2013, pp. 333-338.

[11] C.-W. Tseng, Y.-C. Chen, and C.-H. Huang, "Integrating Transducer Capability to GS1 EPCglobal Identify Layer for IoT Applications," IEEE Sensors Journal, vol. 15, pp. 5404-5415, 2015.

[12] P. Peris-Lopez, J. C. Hernandez-Castro, J. M. Estevez-Tapiador, and A. Ribagorda, "LAMED—A PRNG for EPC Class-1 Generation-2 RFID specification," Computer Standards & Interfaces, vol. 31, pp. 88-97, 2009.

[13] V. R. Vatsa and G. Singh, "A Literature Review on Internet of Things (IoT)," International Journal of Computer Systems (ISSN: 2394-1065), vol. 2, 2015.

[14] T. Li and W. He, RFID product authentication in EPCglobal network: INTECH Open Access Publisher, 2009.

[15] J. Walewski, M. Bauer, N. Bui, P. Giacomin, N. Gruschka, S. Haller, et al., "Project Deliverable D1. 2–Initial Architectural Reference Model for IoT," ed: IoT-A, 2011.

[16] C. M. MacKenzie and K. Laskey, "Reference model for service oriented architecture 1.0," 2006.

[17] L. J. Langman and M. C. A. Hammett-Stabler, "Lab Guidelines & Standards," 2014.

[18] N. Rozanski and E. Woods, "Applying viewpoints and views to software architecture," Whitepaper, http://www. viewpoints-andperspectives. info/vpandp/wpcontent/themes/secondedition/doc/VPandV_WhitePaper. pdf (accessed 2012-05-23), 2005.

[19] D.-L. Yang, F. Liu, and Y.-D. Liang, "A Survey of the Internet of Things," in Proceedings of the 1st International Conference on E-Business Intelligence (ICEBI2010), 2010.

[20] H. Sundmaeker, P. Guillemin, P. Friess, and S. Woelfflé, "Vision and challenges for realising the Internet of Things," Cluster of European Research Projects on the Internet of Things, European Commision, 2010.

[21] P. Shames and T. Yamada, "Reference architecture for space data systems," in International Telemetering Conference Proceedings, 2003.

[22] S. Haller, "The things in the internet of things," Poster at the (IoT 2010). Tokyo, Japan, November, vol. 5, 2010.

[23] M. ISO, "Systems and Software Engineering–Architecture Description," ISO/IEC/IEEE 420102011.

[24] D. Ref, A. S. Segura, and N. V. SAG, "Internet of Things Architecture IoT-A Project Deliverable D6. 2–Updated Requirements List," 2011.

[25] n. o. Excellence, "Deliverable D6. 2: Intermediate Report on the Security of the Connected Car," 2014 2014.

[26] D. Jablon, "IEEE 1363-2000: Standard Specifications for Public Key Cryptography," in retrieved at<>, NIST Key Management Workshop, 2001.

[27] E. El Moustaine and M. Laurent, "A lattice based authentication for low-cost RFID," in RFID-Technologies and Applications (RFID-TA), 2012 IEEE International Conference on, 2012, pp. 68-73.

[28] Y. Trivedi, "Innovation & competition: succeeding through global standards: a new massive open online course delivered on IEEE X. org," IEEE Communications Magazine, vol. 54, pp. 7-9, 2016.

[29] T. Hyla and J. Pejaś, "A Fault-Tolerant Authenticated Key-Conference Agreement Protocol with Forward Secrecy," in IFIP International Conference on Computer Information Systems and Industrial Management, 2016, pp. 647-660.

[30] J. P. Guigay, M. Langer, R. Boistel, and P. Cloetens, "Mixed transfer function and transport of intensity approach for phase retrieval in the Fresnel region," Optics letters, vol. 32, pp. 1617-1619, 2007.

[31] D. Chakraborty, V. Hernandez-Jimenez, and P. Sarkar, "Another look at XCB," Cryptography and Communications, vol. 7, pp. 439-468, 2015.

[32] T. Heer, O. Garcia-Morchon, R. Hummen, S. L. Keoh, S. S. Kumar, and K. Wehrle, "Security Challenges in the IP-based Internet of Things," Wireless Personal Communications, vol. 61, pp. 527-542, 2011.

[33] O. Garcia-Morchon, S. Kumar, R. Struik, S. Keoh, and R. Hummen, "Security Considerations in the IP-based Internet of Things," 2013.

[34] T. Agreement, "Common criteria for information technology security evaluation part 1: Introduction and general model july 2009 revision 3 final foreword," NIST, vol. 49, p. 93, 2009.

[35] T. Eder, D. Nachtmann, and D. Schreckling, "Trust and Reputation in the Internet of Things," in Conference Seminar (SS2013)-Real Life Security (5827HS), 2013.
[36] N. Bui, "Project deliverable D1. 1–SOTA report on existing integration frameworks/architectures for WSN, RFID and other emerging IoT related Technologies," IoT-A, pp32-34, 2011.
[37] K. A. Delic, "On Resilience of IoT Systems: The Internet of Things (Ubiquity symposium)," Ubiquity, vol. 2016, p. 1, 2016.
[38] E. Ratified, "EPCglobal Certificate Profile Specification," 2006.
[39] D. M. Konidala, W.-S. Kim, and K. Kim, "Security assessment of EPCglobal architecture framework," Auto-ID Labs, pp. 13-16, 2006.
[40] H. Krawczyk and P. Eronen, "Hmac-based extract-and-expand key derivation function (hkdf)," 2070-1721, 2010.
[41] D. Brock and C. Cummins, "EPC tag data specification," White Paper, Massachusetts Institute of Technology, Auto-ID Center, 2003.
[42] S. Plósz, M. Tauber, and P. Varga, "Information Assurance System in the Arrowhead Project," ERCIM News, vol. 2014, 2014.
[43] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," Future Generation Computer Systems, vol. 29, pp. 1645-1660, 2013.
[44] A.-R. Sadeghi, C. Wachsmann, and M. Waidner, "Security and privacy challenges in industrial internet of things," in Design Automation Conference (DAC), 2015 52nd ACM/EDAC/IEEE, 2015, pp. 1-6.
[45] Z. Shelby, K. Hartke, and C. Bormann, "The constrained application protocol (CoAP)," 2014.
[46] J. Schlyter and P. Hoffman, "The DNS-based authentication of named entities (DANE) transport layer security (TLS) protocol: TLSA," 2012.
[47] S. Plósz, C. Hegedűs, and P. Varga, "Advanced Security Considerations in the Arrowhead Framework," in International Conference on Computer Safety, Reliability, and Security, 2016, pp. 234-245.
[48] P. P. Pereira, J. Eliasson, and J. Delsing, "An authentication and access control framework for CoAP-based Internet of Things," in Industrial Electronics Society, IECON 2014-40th Annual Conference of the IEEE, 2014, pp. 5293-5299.
[49] S. Cirani, G. Ferrari, and L. Veltri, "Enforcing security mechanisms in the IP-based internet of things: An algorithmic overview," Algorithms, vol. 6, pp. 197-226, 2013.

Author's brief autobiography: Dr. Nidal Turab received a BSc degree in communication engineering from the University of Garounis, Benghazi, libya 1992 and an MSc in telecommunication engineering from the University of Jordan, Amman in 1996. His PhD in computer science from the Polytechnic University of Bucharest, 2008. His research interests include WLAN security, computer networks security and cloud computing security, eLearning and Internet of Things. He working as associate professor at Al-Ahliyya Amman University, Amman, Jordan.