International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 16 (2018) pp. 12805-12812
 https://dx.doi.org/10.37622/IJAER/13.16.2018.12805-12812

# Intrusion Detection in Internet of Things: The Review of Taxonomy

**M. Jagadeesh Babu**
*[1]Research Scholar, Department of Electronics and Communication Engineering, JNTU-A, Ananatapuramu-515005, A.P, India.*

**Dr. A. R Reddy**
*Professor, Department of Electronics and Communication Engineering, MITS, Madanaplle-517325, A.P, India.*

**Abstract**

The concept of IoT is significant which robustly increase with the devices which are smartly connected. It includes the physical devices which are capable to exchange the data with the other devices. Multiple services are done by IoT, boosting the individual personal lives to achieve from its consistent operations. Consequently, task of promising security and safety of both connectivity and information in the environment of IoT achieves a voluminous significance. Hence an efficient and appropriate "intrusion-detection-system (IDS)" is necessary for guaranteeing the security in the IoT environment. This article tries to examine taxonomy connected to the IDS in the IoT.

**Keywords:** Internet of things, RFID, Wireless sensor networks, Power management, 6LoWPAN.

## INTRODUCTION

The IoT is connected to the 50 billion devices which are smart by the year 2020 and is 6 times greater than the population which is projected. Consequently, in computing [1] IoT is deliberated as the fast growth of the technical innovations. These devices which are smart will support our entire daily routines and completely change the case in which we intermingle with the physical devices. And the effect is predicted to be hugely felt on the industries comprising automation, telemetry, road, pharmaceuticals, rail, computing and the other device sensing, infrastructure and other segments.

The work [2] presents that IoT connects the entire physical devices with internet to allow exchange of data within the known protocols. Consequently, based on the virtual, entire physical devices are available at any location and any point of time [3]. And entire devices are connected wirelessly to the small sensors.

In the IoT, physical devices are provided to connect amid themselves without interference of human actions [4]. And the network uses different addressing systems to connect with the objects and novel applications are generated. The work [5] presents that it makes manifold applications such as medical smart water, medical sensing and smart homes etc. Nevertheless with the increase in various services, many challenges will also take place.

The security challenge is the most important problem among diverse challenges which occur in the network of IoT. Because of the objects are accessible at any location via internet, then these objects and network remains unprotected against various intrusions. Hence maintaining security in the network of IoT is the most significant task to the researchers. Here there are some of important security aspects are:

1. Privacy of data: The data which is transmitted among the receiving node and sending node is hacked by the intruders, as it is modifiable [6], confidentiality will be affected. Therefore it is important to secure the data in IoT.
2. Integrity: In the process of transmission, information or data while transmitting should not be altered. There accuracy should be maintained in the message in the entire transmission process. The work [6] presents that in the IoT environment, integrity need to be ensured.
3. Availability: The work [6] presents that resources availability remains crucial for sensitive-time and the prospect information transmission. The bandwidth is loaded intentionally by the intruders to confine the resources availability through diverse means comprising black-hole intrusion, flooding, DoS intrusion etc.
4. Authenticity: The work [7] presents that both devices and data need to be accessible to the legitimate users only. End users should be able to detect the identity of others during the process of interaction. The work [8] presents that the procedure of verification should be free from error to make sure that the users who are illegitimate cannot access the devices or information.
5. Non-repudiation: The work [9] presents that this safeguards that the receivers or transmitters will not negate the receiving or transmitting the data respectively.
6. Information Recentness: According to the requirement, the information or data should be novel. The work [10] presents that IoT should safeguard that the information which is lagged by times should not be re-delivered by an intruder.

This article examines the current IDS techniques in the domain of IoT, by putting forward the cons and pros in the aspect. To represent the differences among current trends of study and IDS platform, the study gives a serious assessment of the available strategies of attack detection.

## TAXONOMY

The technical concepts of IoT environment were not built with extensive support for safety and security and therefore, this is now developing a potential barrier to universal adoption of IoT applications [11]. For handling security challenges, accurate identification of intruders is an important aspect. This can be identified across all four network layers of IoT framework, [12] as depicted in Figure 1 [13]. These layers function both as support for interconnections among various IoT equipment along with offering opportunities for implementing defense strategies such as NIDS [14], [15], [16].

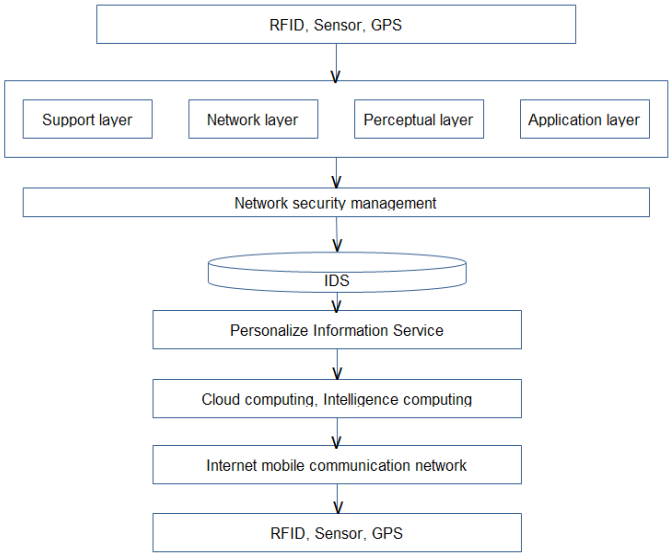


**Figure 1:** IoT Network Security Architecture

### *A. The concept of IoT*

The concept of IoT was introduced in 1999 and then it was regarded as uniquely detectable inter-operable interconnected devices through RFID platform. To date, the precise definition for IoT network is not yet finalized as is still in developing stage [17], [18], [19]. Typically, the IoT is described as dynamic and universal network framework containing auto-configuration abilities on the basis of certain protocols. Further, it comprised both physical and virtual devices, which possess separate identifications, features and are able to utilize intelligent interfaces. Further, these devices can be combined into an information network [20], [21].

Fundamentally, the concept can be considered as a superset of interconnecting equipment, which is distinctly detectable through available NFC methods [22]. The terms “Internet” and “Things” refer to interconnected global network on the basis of sensory, data transmission, data processing tools and these concepts can be the next future of ICT [23], [24]. Though several differences prevail over the definition of IoT, the concept is largely talked about and associated technologies continue to emerge quickly [17], [25], [26], [19]. In specific, recently the intelligent sensors and wireless data transfer methods formed an integral part of the IoT, thereby, leading to the development of new issues and wider research scope [27], [28].

The ITU presented the details of most prospect nations to incorporate IoT, supporting technologies and platforms, prominent issues and the future impact of IoT [29], [25]. From identification through RFID, the concept is incorporated in transportation, pharma, retail and various other business sectors [30], [31].

The evolving wireless- sensing technologies largely boosted the sensory abilities of objects and thereby, the initial principle of IoT is in extending it to self-control. Currently, several new technologies are built for functioning in IoTs like WSNs, bar-coding, RFIC, NFC, cloud-computation etc. [32], [33], [34], [35], [36], [37], [38]. Emergence of such technologies strengthens the growth and functioning of IoT [39], [40], [20], [21], [41], [42], [43], [44], [45]. The IoT denotes the future of the internet in which both physical and virtual objects are accessible and detected via the internet.

Based on different technologies available for incorporation and deployment, the IoT concept is defined in various terms. Despite several definitions being put forward, the underlying basis of IoT is that all the devices in the environment can be distinctly referred virtually. In the IoT, all devices can interchange information and based on the requirement, information processing can also be done based on certain pre-determined standards.

### *B. Standards*

Some of the studies in the contemporary literature analyzed that absence of globally accepted and followed standards result in lowered competitiveness of IoT devices [46], [47], [48], [49], [50], [51], [52], [53]. Over the last ten years, several technical standards are designed and implemented by different manufacturers. Such standards form the most vital role in the successful growth of IoT. In specific, the technical standards adopted for middleware and interfaces remain the most prominent. Some of the studies developed are- (1) planning policies and distributed framework; (2) protecting the individual data and maintaining secrecy; (3) understanding the trustworthiness, adaptability, and safety of transmission systems; (4) designing acceptable standards; (5) exploiting novel techniques like MEMS objects and omnipresent localization [51], [52], [53].

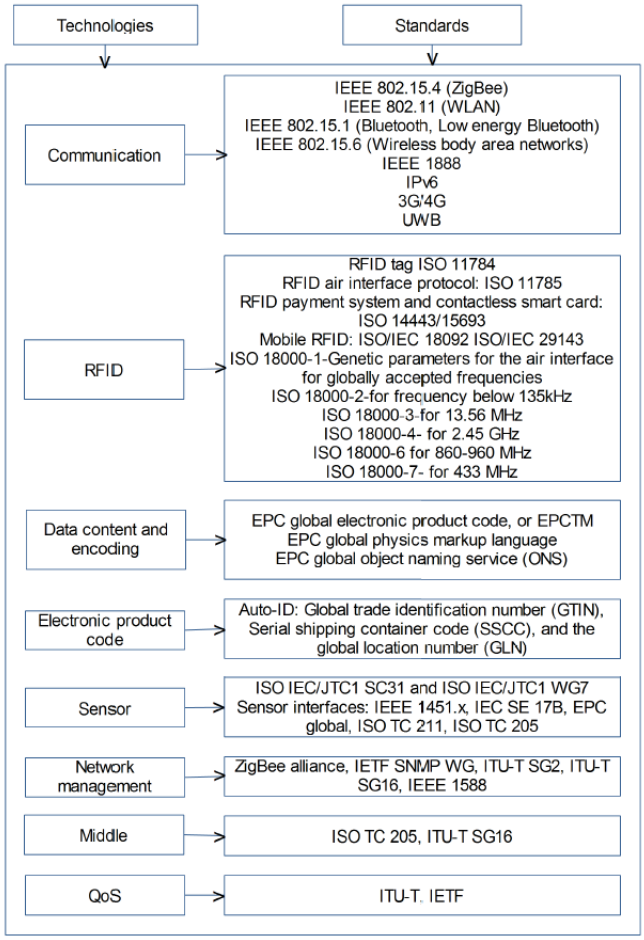


**Figure 2:** An Overview of Standards in IoT [46], [47], [48], [49], [50], [51], [52], [53]

Designing global standards for IoT devices has been one of the most interesting and attentive areas of research in several nations. Globally, [46], [47], [48], [49], [50], [51], [52], [53], ITU, EPC-global, IEC, ISO, and IEEE remain major organizations to present standards to detect, obtain and transfer information through RFID domain. On a regional scale, ETSI, CEN/CENELEC also presented certain standards like RFID, WSN and so on. In North America, ANSI is engaged in designing managerial standards for IoT devices and is a country level priority task. Japan designed 'uID' as a framework to interconnect different works with applied R&D [52], [53]. CCSA (China) and CESI are also involved in building standards of semi-passive RFID and UHF- RFID. Further, 973 works have been designed in the country towards designing standards and basic of IoT [30]. Figure 2 provides an overview of various standards being designed for IoT.

Achieving global standards in IoT requires both performance and availability of designed specifications to be considered [24], [54]. Though several entities are engaged in building basic standards for IoT, a worldwide cooperation among these entities is required to ensure uniformity and usability of the standards. Further, the WSC must be capable of handling the relation between different global and regional/national standardization entities.

In addition, the need for standardization in the technological build of IoT is also vital. The standards assist the manufacturers and consumers to decide on the most viable and optimal protocols for their respective products and services. Further, ensuring standards in technological platforms remains the most immediate task, which will ensure security and assist in the rapid growth of IoT technology. Figure 3 presents an overview of different enabling-technologies:

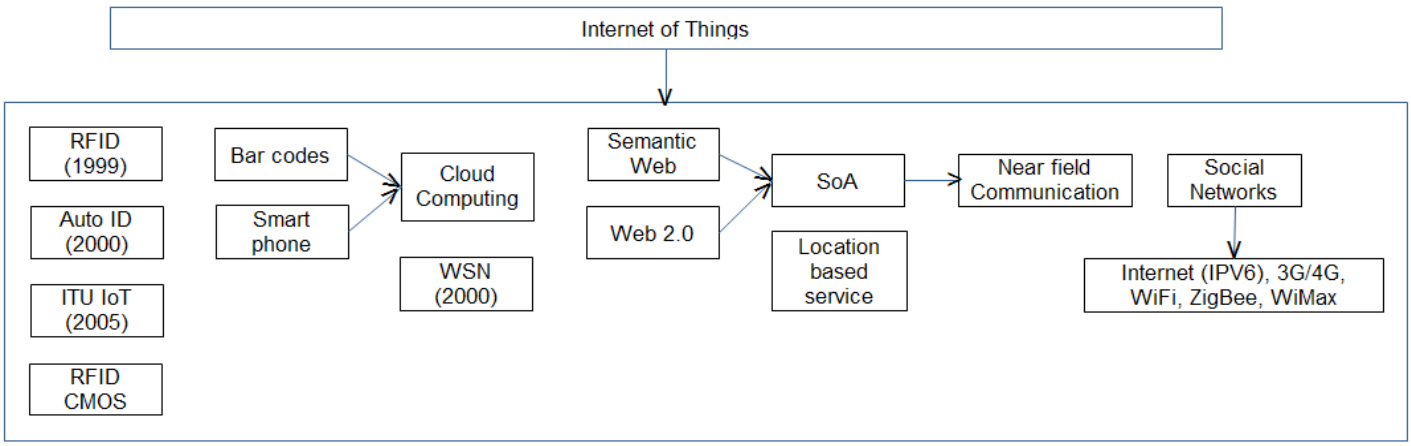


**Figure 3:** Enabling Technologies for IoT

### C. *Design Framework*

Typically, any IoT object comprises of four segments:

1. Sensor segment: It is mostly analog or MEMS-based. The sensor ranges from being a mere heat sensor to a sophisticated ECG measurement [55]. In all conditions, analog or MEMS segment remains the vital portion of the chip design.
2. Processing Segment: It is digital in nature. It comprises of a processor, storage, filter, and boosters for effectively managing the sensor output information [56]. Further, it also involves a secure IP for encrypting information in both storage and transmission.
3. Radio Segment: The radio segment that can be either Bluetooth or ZigBee or even Wi-Fi enabled.
4. Power handling segment: The segment comprises power managing devices, generation equipment along with clock frequencies for effective power saving.

In addition to the primary functioning of different nodes and varieties of sensors, these nodes can also vary in terms of processor efficiency, stream flow rate, chip buffer volume, the extent of activity and power management systems. All these factors can alter the way in which the device will be evaluated. For instance, the testing process of a temperature sensor varies largely from the ECG monitoring device.

The primary factor for determining the system design is often the costs involved. Due to billions of nodes are involved in the process, minute and highly efficient chips are required. Often analog, digital and RF designs are combined into a single chip to achieve these features. In particular, due to the prominence of the analog segment that consists of restricted scaling advantages, old manufacturing technologies like CMOS may be preferred to ensure low costs [57].

### D. *Service-Focused Framework*

One of the important needs of an IoT is the need for inter-connectivity among different objects within the network. The IoT network framework should assure IoT operations that ensure smooth flow of operations between physical devices and virtual information. Development of IoT framework includes several features like networking, transmission, managerial processes along with safety features [58], [59]. For the efficient design of this framework, device-to-device operations, achieving scalability among different types of objects and their individual business concerns must be taken into account. Further, as these physical objects can be transported between countries or regions and require interactions with other devices on a real-time basis, the designed framework must support such interaction and also assist in the error-free transmission of information. Further, the infrastructure must be of both decentralized and varied nature.

Service-based framework remains an imperative for both vendors and consumers in the IoT environment [60], [61]. The framework guarantees that the interconnections between different type of objects function smoothly in different ways [62], [63], [45]. Figure 4 depicts the typical service based framework structure that comprises 4 layers, each with different functionalities:

- Sensory Layer: It is incorporated into different hardware devices to enable the monitoring of current conditions of different objects
- Network Layer: It is the networking structure to assist connectivity between devices in both wired and wireless environments
- Service Layer: The primary function of this layer is for generating and handling services needed by the consumers
- Interface Layer: The layer comprises of the different interactive options with consumers

The service-based architecture considers the complex system as a group of pre-defined sub-systems [64]. Such sub-systems are enabled to be re-utilized and sustained independently, thereby ensuring that both the software and firmware elements in the IoT to be re-utilized in an effective manner. Driven by these benefits, the Service-Oriented-Architecture (SoA) is being adapted as the fundamental framework for wireless environments [65], [66], [67]. For extending the SoA framework in IoT environment, it is developed to present extensive usage, scalability, inter-operations between different objects and modularity. Further, the SoA functions are clustered into a regular group of services [68]. Figure 4 depicts an illustration of SoA incorporation in IoT along with analysis of each element.

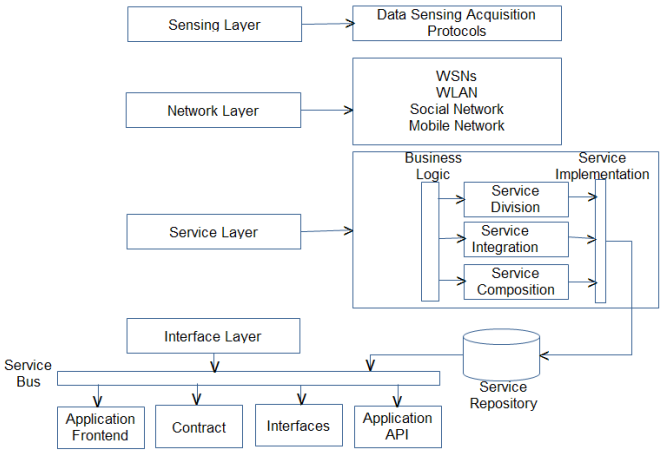


**Figure 4:** SoA framework for incorporation in IoT

### E. *Malware intrusion on IoT Devices and Applications*

Both intrinsic and extrinsic intrusions are observed in sensory networks. Intrusions are primarily categorized into two groups as intrinsic generated and external intrusions. In specific, the external intrusions involve attacks from intruders not involved in the environment and on the other hand, internal intrusions occur due to a corrupted or compromised node within the

environment. The below points detail a few prospectus malware intrusions in IoT domain-

- **Sink-hole Intrusion:** This type of intrusion involves the corrupted node attracting unintended data flows towards it. In order to create this intrusion, the corrupted node attracts all nearby nodes to deliver their respective data through the corrupted node by posing pseudo low costs. The intruder causes the attack by incorporating a pseudo node within the transmission system [69].
- **Worm-hole Intrusion:** In a worm hole intrusion, the corrupted node generates a virtual path between two nodes. The malicious node behaves as a forwarder between two original nodes. The two corrupt nodes falsely pose that they are only one-hop far from the base station. Further, this type of intrusion is also utilized to convince two different nodes that they are in proximity by relaying data messages among them [69], [70].
- **Selected Forwarding Intrusion:** The corrupt node behaves like a genuine node but on a selected basis, it sinks certain data messages [69].
- **Sybil Intrusion:** The corrupt node consists of more than one identity. The route determining protocol along with detection program are targeted by the corrupt node. [69].
- **Hello Flood Intrusion:** The routing protocol transmits the hello message to share its existence to nearby nodes. The nearby node, which receives this hello message considers that the source node is in proximity and therefore, includes the corrupt node to its nearby nodes list [70].
- **DoS Intrusion:** By denying availability of resources to nearby nodes, the malicious node causes resource loss in the network. When multiple nodes cause such intrusion, it is termed as DDoS. It often impacts the available resources, bandwidth and processing duration etc.

Typically, the cyber intrusion characteristics in networks are categorized into four basic classifications according to KDD99 [12], NSL-KDD [71], [16]:

- Probe: Intruder attempts to obtain unauthorized data on the target network via probing into the network and scanning ports.
- DoS: Intruder attempts to deny resources to the genuine consumer and restricts the application from gaining access
- U2R: Intruder aims to increase the limited rights of consumer to higher level rights through illegitimate credentials
- R2L: Intruder attempts to obtain remote access to a target device by falsely replicating as a genuine local user

The last two intrusion types are the most complex types and involve tough challenges for detection algorithms as they mimic genuine user characteristics [72], [73].

## CONCLUSION

The principles of complete infrastructure of IoT for detection are continuously being a researched topic for the former five years. However in the starting stages, trend is predicted to increase rapidly in the detection system by combining each layer as well as with the benchmarks amid systems should be crucial for promising the security to the users and the devices.

With the broad range of the frameworks which are ranging from the ad-hoc and non-documented objects to the objects which are highly structured confined to the protocols, and the environment is encumbered with the challenges of security. Consequently, the detection system which is omnipresent is able to connecting with the entire layers has a great significance. This is strongly felt with the applications which are growing rapidly and the services which are interrelated with the network. This article endeavored to depict the IoT structure nomenclature and the intrusion detection objective in the IoT.

## REFERENCES

[1] Evans, Dave. "The internet of things: How the next evolution of the internet is changing everything." CISCO white paper 1.2011 (2011): 1-11.

[2] Chen, Shanzhi, et al. "A vision of IoT: Applications, challenges, and opportunities with china perspective." IEEE Internet of Things journal 1.4 (2014): 349-359.

[3] Benabdessalem, Raja, Mohamed Hamdi, and Tai-Hoon Kim. "A survey on security models, techniques, and tools for the internet of things." Advanced Software Engineering and Its Applications (ASEA), 2014 7th International Conference on. IEEE, 2014.

[4] Li, Shancang, Li Da Xu, and Shanshan Zhao. "The internet of things: a survey." Information Systems Frontiers 17.2 (2015): 243.

[5] Sreeram, P. Gokul Sai, and Chandra Mohan Reddy Sivappagari. "Development of Industrial Intrusion Detection and Monitoring Using Internet of Things." International Journal of Technical Research and Applications (2015).

[6] Patel, Manish M., and Akshai Aggarwal. "Security attacks in wireless sensor networks: A survey." Intelligent Systems and Signal Processing (ISSP), 2013 International Conference on. IEEE, 2013.

[7] L. Clemmer, Information Security Concepts: Authenticity. [Online] Available: http://www.brighthub.com/computing/smb-security/articles/31234.aspx.

[8] Kumar, ShyamNandan. "Review on Network Security and Cryptography." International Transaction of

Electrical and Computer Engineers System 3.1 (2015): 1-11.

[9] Chezhian, Umadevi, and Zaheer Uddin Khan. "Security Requirements In Mobile Ad Hoc Networks." International Journal of Advanced Research in Computer and Communication Engineering 1.2 (2012).

[10] Hossain, Md Mahmud, MaziarFotouhi, and RagibHasan. "Towards an analysis of security issues, challenges, and open problems in the internet of things." Services (SERVICES), 2015 IEEE World Congress on. IEEE, 2015.

[11] Sicari, Sabrina, et al. "Security, privacy and trust in Internet of Things: The road ahead." Computer Networks 76 (2015): 146-164.

[12] Shakshuki, Elhadi M., Nan Kang, and Tarek R. Sheltami. "EAACK—a secure intrusion-detection system for MANETs." IEEE transactions on industrial electronics 60.3 (2013): 1089-1098.

[13] Suo, Hui, et al. "Security in the internet of things: a review." Computer Science and Electronics Engineering (ICCSEE), 2012 international conference on. Vol. 3. IEEE, 2012.

[14] Liao, Hung-Jen, et al. "Intrusion detection system: A comprehensive review." Journal of Network and Computer Applications 36.1 (2013): 16-24.

[15] Bhuyan, Monowar H., Dhruba Kumar Bhattacharyya, and Jugal K. Kalita. "Network anomaly detection: methods, systems and tools." Ieee communications surveys & tutorials 16.1 (2014): 303-336.

[16] Butun, Ismail, Salvatore D. Morgera, and Ravi Sankar. "A survey of intrusion detection systems in wireless sensor networks." IEEE communications surveys & tutorials 16.1 (2014): 266-282.

[17] Hepp, Martin, Katharina Siorpaes, and Daniel Bachlechner. "Harvesting wiki consensus: Using wikipedia entries as vocabulary for knowledge management." IEEE Internet Computing 11.5 (2007).

[18] Joshi, Gyanendra Prasad, and Sung Won Kim. "Survey, nomenclature and comparison of reader anti-collision protocols in RFID." IETE Technical Review 25.5 (2008): 234-243.

[19] Pretz, K. The Next Evolution of the Internet. [cited 2013 May 20]; available from http://theinstitute.ieee.org/ technology-focus/ technology-topic/the-next-evolution-of-the-internet, (2013).

[20] Li, Shancang, et al. "Integration of hybrid wireless networks in cloud services oriented enterprise information systems." Enterprise Information Systems 6.2 (2012): 165-187.

[21] Li, Yuan, et al. "Towards a theoretical framework of strategic decision, supporting capability and information sharing under the context of Internet of Things." Information Technology and Management 13.4 (2012): 205-216.

[22] ETSI. The European Telecommunications Standards Institute, [cited 2013 May 20]; available from http://www.etsi.org/. (2013).

[23] Kranenburg, V. Moscow futurodesign lab co-create urban intelligence: designing smart interfaces between people and city, [cited 2013 May 20]; available from http://www.theinternetofthings.eu/ content/moscow-futurodesign-laboratory-workshop-co-createurban-intelligence-designing-smart-interfa. (2013).

[24] Marry, W. Disruptive civil technologies six technologies with potential impacts on us interests out to 2025, [cited 2013 May 20]; available from http://swemgovdocs.blogs.wm.edu/. (2013).

[25] ITU. The internet of Things, International Telecommunication Union (ITU), Internet Report [cited 2013 May 20]; available from http://www.itu.int/dms_pub/itu-s/opb/pol/S-POL-IR.IT-2005- SUM-PDF-E.pdf. (2013).

[26] Li, Shancang, Li Da Xu, and Xinheng Wang. "Compressed sensing signal and data acquisition in wireless sensor networks and internet of things." IEEE Transactions on Industrial Informatics 9.4 (2013): 2177-2186.

[27] Hunter, David, et al. "Selection of proper neural network sizes and architectures—A comparative study." IEEE Transactions on Industrial Informatics 8.2 (2012): 228-240.

[28] Wilamowski, Bogdan M. "Challenges in applications of computational intelligence in industrial electronics." Industrial Electronics (ISIE), 2010 IEEE International Symposium on. IEEE, 2010.

[29] Frenken, Thomas, PatrikSpiess, and Jürgen Anke. "A Flexible and Extensible Architecture for Device-Level Service Deployment." ServiceWave 8 (2008): 230-241.

[30] Guinard, Dominique, et al. "Interacting with the soa-based internet of things: Discovery, query, selection, and on-demand provisioning of web services." IEEE transactions on Services Computing 3.3 (2010): 223-235.

[31] Xu, Li Da. "Information architecture for supply chain quality management." International Journal of Production Research 49.1 (2011): 183-198.

[32] Jiang, Lihong, et al. "An IoT-oriented data storage framework in cloud computing platform." IEEE Transactions on Industrial Informatics 10.2 (2014): 1443-1451.

[33] Kataev, Michael Yu, et al. "Enterprise systems in Russia: 1992–2012." Enterprise Information Systems 7.2 (2013): 169-186.

[34] Li, Qing, et al. "Applications integration in a hybrid cloud computing environment: Modelling and

platform." Enterprise Information Systems 7.3 (2013): 237-271.

[35] Ren, Lei, et al. "A methodology towards virtualization-based high performance simulation platform supporting multidisciplinary design of complex products." Enterprise Information Systems 6.3 (2012): 267-290.

[36] Tao, Fei, et al. "CCIoT-CMfg: cloud computing and internet of things-based cloud manufacturing service system." IEEE Transactions on Industrial Informatics 10.2 (2014): 1435-1442.

[37] Tao, Fei, et al. "IoT-based intelligent perception and access of manufacturing resource toward cloud manufacturing." IEEE Transactions on Industrial Informatics 10.2 (2014): 1547-1557.

[38] Wang, Chengen, Zhuming Bi, and Li Da Xu. "IoT and cloud computing in automation of assembly modeling systems." IEEE Transactions on Industrial Informatics 10.2 (2014): 1426-1434.

[39] Deng, Robert H., et al. "A New Framework for RFID Privacy." ESORICS. Vol. 6345. 2010.

[40] Van Kranenburg, Rob, et al. "The Internet of Things." (2011).

[41] Malatras, Apostolos, AbolghasemAsgari, and Timothy Baugé. "Web enabled wireless sensor networks for facilities management." IEEE systems journal 2.4 (2008): 500-512.

[42] Miorandi, Daniele, et al. "Internet of things: Vision, applications and research challenges." Ad Hoc Networks 10.7 (2012): 1497-1516.

[43] Pautasso, Cesare, and Erik Wilde. "Why is the web loosely coupled?: a multi-faceted metric for service design." Proceedings of the 18th international conference on World wide web. ACM, 2009.

[44] Vermesan, O. CERP-IoT strategic research agenda. [cited 2013 May 20]; available from http://www.rfid-in-action.eu/cerp/. (2013).

[45] Wang, Xi Vincent, and Xun William Xu. "DIMP: an interoperable solution for software integration and product data exchange." Enterprise Information Systems 6.3 (2012): 291-314.

[46] Broll, Gregor, et al. "Perci: Pervasive service interaction with the internet of things." IEEE Internet Computing 13.6 (2009): 74-81.

[47] Dada, Ali, and FrédéricThiesse. "Sensor applications in the supply chain: the example of quality-based issuing of perishables." The Internet of Things (2008): 140-154.

[48] Floerkemeier, Christian, Christof Roduner, and Matthias Lampe. "RFID application development with the Accada middleware platform." IEEE Systems Journal 1.2 (2007): 82-94.

[49] Gama, Kiev, Lionel Touseau, and Didier Donsez. "Combining heterogeneous service technologies for building an Internet of Things middleware." Computer Communications 35.4 (2012): 405-417.

[50] Ilic, Alexander, Thorsten Staake, and Elgar Fleisch. "Using sensor information to reduce the carbon footprint of perishable goods." IEEE Pervasive Computing 8.1 (2009).

[51] Karpischek, Stephan, et al. "Mobile sales assistant-an nfc-based product information system for retailers." Near Field Communication, 2009. NFC'09. First International Workshop on. IEEE, 2009.

[52] Li, Ling, Shancang Li, and Shanshan Zhao. "QoS-aware scheduling of services-oriented internet of things." IEEE Transactions on Industrial Informatics 10.2 (2014): 1497-1505.

[53] Li, Shancang, et al. "A distributed consensus algorithm for decision making in service-oriented internet of things." IEEE Transactions on Industrial Informatics 10.2 (2014): 1461-1468.

[54] Vilamovska, Anna-Marie, et al. "Study on the requirements and options for RFID application in healthcare." (2009).

[55] Van Helleputte, Nick, et al. "A multi-parameter signal-acquisition SoC for connected personal health applications." Solid-State Circuits Conference Digest of Technical Papers (ISSCC), 2014 IEEE International. IEEE, 2014.

[56] Konijnenburg, Mario, et al. "A battery-powered efficient multi-sensor acquisition system with simultaneous ECG, BIO-Z, GSR, and PPG." Solid-State Circuits Conference (ISSCC), 2016 IEEE International. IEEE, 2016.

[57] Michael White. IoT, Cost-per-Transistor Extend Lifetimes of Established Technology Nodes. Electronic Design. http://electronicdesign.com/eda/iot-cost-transistor-extend-lifetimesestablished- technology-nodes. (2015).

[58] Ulmer, Jean-Stéphane, Jean-Pierre Belaud, and Jean-Marc Le Lann. "A pivotal-based approach for enterprise business process and IS integration." Enterprise Information Systems 7.1 (2013): 61-78.

[59] Looy, Amy Van, Manu De Backer, and Geert Poels. "A conceptual framework and classification of capability areas for business process maturity." Enterprise Information Systems 8.2 (2014): 188-224.

[60] Ciganek, Andrew Paul, William Haseman, and K. Ramamurthy. "Time to decision: the drivers of innovation adoption decisions." Enterprise Information Systems 8.2 (2014): 279-308.

[61] Hachani, Safa, Lilia Gzara, and HervéVerjus. "A service-oriented approach for flexible process support within enterprises: application on PLM systems." Enterprise Information Systems 7.1 (2013): 79-99.

[62] Panetto, Hervé, and Joe Cecil. "Information systems for enterprise integration, interoperability and networking: theory and applications." (2013): 1-6.

[63] Jardim-Goncalves, Ricardo, et al. "Systematisation of Interoperability Body of Knowledge: the foundation for Enterprise Interoperability as a science." Enterprise Information Systems 7.1 (2013): 7-32.

[64] Da Xu, Li. "Enterprise systems: state-of-the-art and future trends." IEEE Transactions on Industrial Informatics 7.4 (2011): 630-640.

[65] Alcaraz, Cristina, and Javier Lopez. "A security analysis for wireless sensor mesh networks in highly critical systems." IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews) 40.4 (2010): 419-428.

[66] Roman, Rodrigo, et al. "Key management systems for sensor networks in the context of the Internet of Things." Computers & Electrical Engineering 37.2 (2011): 147-159.

[67] Roman, Rodrigo, and Javier Lopez. "Integrating wireless sensor networks and the internet: a security analysis." Internet Research 19.2 (2009): 246-259.

[68] Xiao, Guangyi, et al. "User interoperability with heterogeneous IoT devices through transformation." IEEE Transactions on Industrial Informatics 10.2 (2014): 1486-1496.

[69] Can, Okan, and OzgurKoraySahingoz. "A survey of intrusion detection systems in wireless sensor networks." Modeling, Simulation, and Applied Optimization (ICMSAO), 2015 6th International Conference on. IEEE, 2015.

[70] Sardar, AbdurRahaman, et al. "Intelligent intrusion detection system in wireless sensor network." Proceedings of the 3rd International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA) 2014. Springer, Cham, 2015.

[71] Tavallaee, Mahbod, et al. "A detailed analysis of the KDD CUP 99 data set." Computational Intelligence for Security and Defense Applications, 2009. CISDA 2009. IEEE Symposium on. IEEE, 2009.

[72] Bouzida, Yacine, and Frederic Cuppens. "Neural networks vs. decision trees for intrusion detection." IEEE/IST Workshop on Monitoring, Attack Detection and Mitigation (MonAM).Vol. 28. 2006.

[73] Beghdad, Rachid. "Efficient deterministic method for detecting new U2R attacks." Computer Communications 32.6 (2009): 1104-1110.