I J C T A, 9(26) 2016, pp. 115-120
© International Science Press

Internet of Things: Data Management and Security

A. Beatrice Dorothy[1] and S. Britto Ramesh Kumar[2]

ABSTRACT

The Internet of Things is one of the emerging technologies that support different domains to manage and optimize performance, allowing for new activities such as data analytics, management and security. First, this paper illustrate various application scenarios, the IoT supporting domains including resource management, Education, Agriculture, Health care, water quality, natural disasters, transportation, security, automobile, supply chain management, smart cities, Automated metering and monitoring of utilities, waste management, Oil & Gas, security and privacy, energy management. Future, IoT enabling ubiquitous connectivity will cause a faster enhance of data traffic load in both wired and wireless communication networks. The data will be both homogeneous and heterogeneous and the issue arises due to interoperability, Scalability and the middleware Architecture of the IoT systems. We have also discussed about the Issues and Challenges that were faced in the Internet of Things system. We have given an proposed Data Management and Security (DMS) Architecture for IoT system to face challenges like creating ontology's and defining data models are not enough, so data selection refining noisy data from the database through data clustering and selection method through the existing algorithms has to be done. Also, the Security of the Internet of Things systems has been discussed, to overcome some of the Issues and Challenges in Privacy and Security.

Keywords: Internet of Things, IoT, Artificial Intelligence, noisy data, interoperability, Security, Data Mining.

1. INTRODUCTION

The emerging technologies have witnessed major transformation of the life existence from the beginning of the evolution and one among them is Internet of Things (IoT). It can be commonly defined as an interface between the physical world and cyber world through ubiquitous sensing, between software and hardware, connection with the help of electronic devices. It is a hopeful intersection that IoT can emancipate our tedious life from arduous human-machine interface work and information exploration [1]. Many see IoT as the ultimate futuristic world, where ubiquitous smart devices and assets are connected to make human living easier and more convenient, and everything becomes smarter. Data management is a crucial aspect in the Internet of Things. When considering a world of objects interconnected and constantly exchanging all types of information, the volume of the generated data and the processes involved in the handling of those data become critical [2]. Some of the most relevant challenges and opportunities of data management are Data Collection and Analysis, Big Data, Semantic Sensor Networking, Virtual Sensors, Complex Event Processing [2]. Likewise, there are a number of speciûc security, privacy and trust challenges in the IoT, they all share a number of transverse non-functional requirements. In recent years, IoT has been redefined depending on different vista and applications. Already, the global digital space revolution has started which makes the Internet of Things more familiar to this world. The Asia-Pacific region is set to become a hotspot for IoT by the year 2020, it is estimated that there will be some 10 billion connected devices in this area. Digital India is being promoted by Indian government. In keenness of this growth and the regulatory challenges, countries are trying, different tactics to keep velocity. India's Department of Electronics & Information Technology, under the Ministry of Communication and Information Technology, has released

Research Scholar[1], Assistant Professor[2]
Dept. of Computer Science, St. Joseph's College, Trichy.

a Draft Policy on IoT. This project contributes the needs in the domains of Education, Agriculture, Health care, water quality, natural disasters, transportation, security, automobile, supply chain management, smart cities, Automated metering and monitoring of utilities, waste management, Oil & Gas, Power generating from different source and so on**.**

2. LITERATURE REVIEW

The IoT will be a promising facility of future network which has self-configuration ability in global dynamic network based on standard and interoperable communication protocols. In the network, all real and virtual items have specific identification and physical sensory data in order to achieve the goal of information sharing through seamless connection of intelligent interface [3]. These intelligent interfaces connect and communicate with users, society, and environment context on the basis of the agreed protocols. It is an extension and expansion of the network based on the Internet to achieve intelligent identifying, locating and tracking, monitoring and managing [4]. IoT is mainly supported by continuous progress in wireless sensor and actuator networks and by manufacturing low cost and energy efficient hardware for sensor and device communications. However, heterogeneity of underlying devices and communication technologies and interoperability in different layers, from communication and seamless integration of devices to interoperability of data generated by the IoT resources, is a challenge for expanding generic IoT solutions to a global scale [5].

According to Gartner, Inc. (a technology research and advisory corporation), there will be nearly 26 billion devices on the Internet of Things by 2020[6]. ABI Research estimates that more than 30 billion devices will be wirelessly connected to the Internet of Things by 2020. As per a recent survey and study done by Pew Research Internet Project, a large majority of the technology experts and engaged Internet users who responded—83 percent—agreed with the notion that the Internet/Cloud of Things, embedded and wearable computing (and the corresponding dynamic systems) will have widespread and beneficial effects by 2025[3]. It is, as such, clear that the IoT will consist of a very large number of devices being connected to the Internet [7].

Gartner's Emerging Technology Hype Cycle represents the impact and expectations of specific technologies where X- axis denotes time and Y- axis denotes expectation [6].

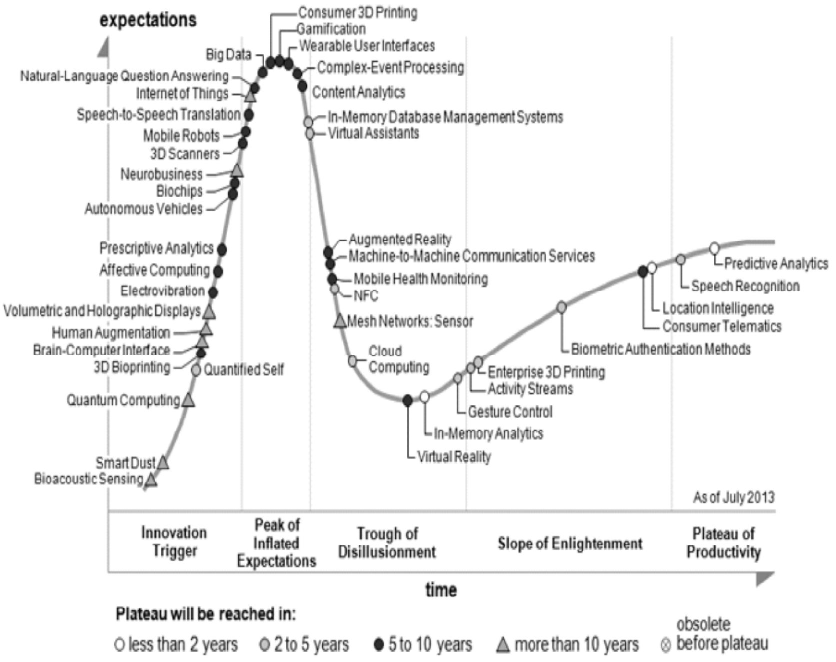

Figure 1: Gartner's Hype Cycle

The Internet of Things is an embedded one which consists of sensors, actuators, RFID, WSN, ZigBee, Internet, Protocols and Applications. The sensors and actuators are used to converts energy into motion. Sensors provide much of the data gathering, actuators, radio chips provide the underlying connectivity, micro-controllers provide the processing of that data, modules combine the radio, sensor and actuators, combine it with storage [8]. RFID is a system used to transmit the identity of a human or a thing wirelessly using radio waves in the form of a serial number. WSN is a wireless network consisting of spatially distributed autonomous devices using sensors to cooperatively monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants, at different locations [7]. ZigBee is one of the protocols developed for enhancing the features of wireless sensor networks (WSN). The WSN provides the means of transporting the data while a service infrastructure needs to be created for the tasks of designing, installing, monitoring and servicing the IoT deployment. In Protocols, Internet Protocol (IP) is the primary communications protocol in the Internet protocol suite for relaying or transporting data across network and one among them is IPv6. The application is a software program used by end users in their everyday life.

While we talk about Internet of Things we have to take into consideration of Middleware which acts as a bond joining the heterogeneous components together and also provides API (Application Programming Interfacing) for physical layer communications, and required services to the applications, hiding all the details of different layers and components. The functional components of middleware [9] are as follows:

- Interoperation
- Context detection
- Scalability
- Device discovery and management
- Security and privacy
- Managing data volume

3. CHALLENGES OF IOT SYSTEM

The challenges that are faced by the IoT systems [10] are as follows:

- The models provide the basic description frameworks, but alignment between different models and frameworks are required.
- Reasoning and interpretation of data is required for automated process.
- Data or services from different frameworks and providers cannot be interchanged and used with minimised intervention.
- Privacy and Security at Technical and Semantic level is needed.
- Quality of Service, Data Management has to be provided.

4. PROPOSED DMS ARCHITECTURE FOR IOT SYSTEM

In this proposed Data Management and Security (DMS) Architecture for Internet of Things system, the Data is received from the Sensors and actuators which is relayed by the micro-controller through WiFi, GPRS, RFID, ZigBee and open connectivity to the Router. These data has to be refined from the database or repository using the Data Mining algorithms like clustering and classification which analyses semantically and syntactically. Reasoning and Interpretation of data can be achieved by Artificial Intelligence (AI) and the Noisy data is segregate from Knowledge Discovery in Database (KDD) to provide Quality of Service (QoS). The Security system can be obtained by the Cryptography, Authentication, Trust & Reputation and Identity Management, such that, the End- User can use the various domains effectively from the applications.

The amount of data is exploding due to the development of information technology. Data management is a crucial aspect, so that the velocity of the data is managed through IPv6 in the Internet of Things. The current IoT data communications often rely on binary or syntactic data models which lacks in providing machine interpretable meanings to the data, for that, reasoning and analysis of data which is achieved by Artificial Intelligence (AI).

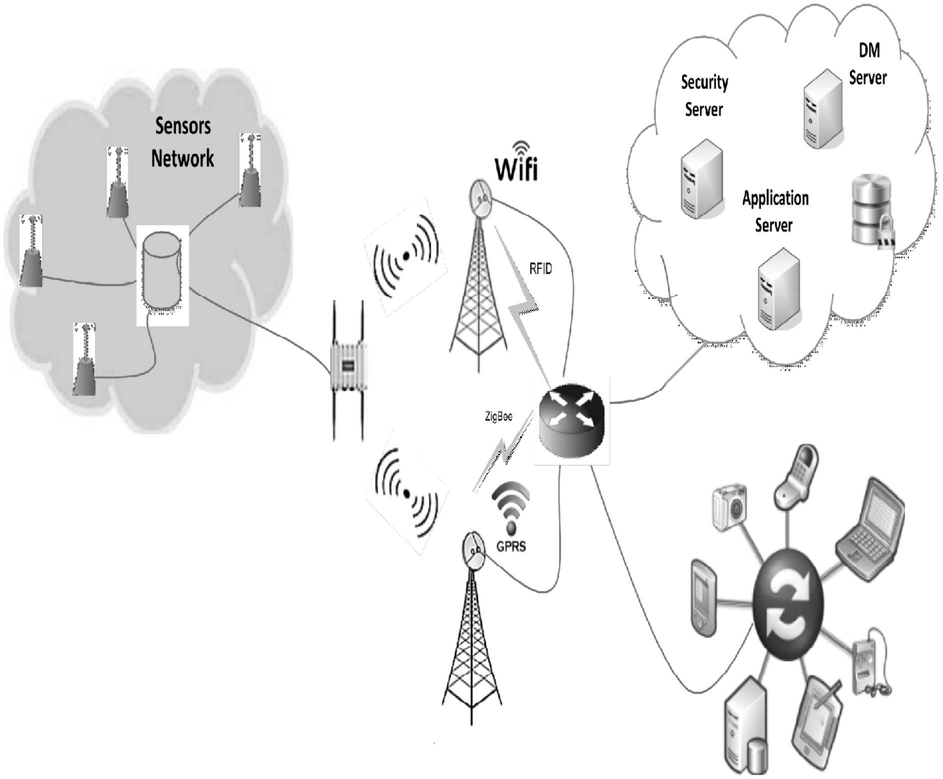

Figure 2: Proposed DMS Architecture for IoT System

Data encryption only protects encrypted pathways. Data that is transmitted over an encrypted link is still exposed at any point it is decrypted, such as prior to encryption, after decryption, and along any communications pathways that do not enforce encryption. As the IoT becomes established in Smart environment, the volume of the data generated will increase. Data will be generated and transmitted autonomously and these data will inevitably accessed by Smart environment. To accommodate the diversity of the IoT, there is a heterogeneous mix of communication technologies, which needs to be adapted in order to address the needs of IoT applications such as Security and reliability. The IoT provides solutions based on the integration of information technology, which refers to hardware and software used to store, retrieve and process data and communication technologies. Centralized data collection and smart object management do not provide the scalability required by the Internet. Sensors and actuators in a Smart Grid network cannot efficiently be done using a centralized approach. Because network bandwidth may be scarce and collecting environmental data from a central point in the network unavoidably leads to using a large amount of the network capacity. So to handle these large scale data we need IPv6 through which all the centralized data can be stored and retrieved from the database, Security server, Data Management Server and the Application server. In Security server, Authentication, provides and verify the identify information of an IoT entity. In Trust & Reputation, it gives access over the entire system. In Identity Management, it checks with Biometrics, so that we get highest control over the system security. Then, the End users can access the device provided the Privacy of the user is maintained.

5. CONCLUSIONS

In this paper, we have proposed a Data Management and Security (DMS) Architecture of IoT system in which data are collected from Sensors, actuators and relay with the help of RFID, ZigBee, WiFi and Wireless Sensor Network and stored and retrieved from Cloud or database that passes two ways process semantic and syntactical and refined to data selection. Noisy data is segregated from Knowledge Discovery of Database (KDD) through Artificial Intelligence and we get Quality of Service (QoS). The data also go through Privacy and Security like Authentication, Trust & Reputation and Identity Management in Server cloud which consists of Database, security server, data management (DM) server and Application server. Finally, the End user can use needed Domains like Education, Agriculture, Health, water quality, natural disasters, transportation, security, automobile, supply chain management, smart cities, Automated metering and monitoring of utilities, waste management, Oil & Gas, Power generating from different source and so on**.**

REFERENCES

[1] Huansheng Ning, *Unit and Ubiquitous Internet of Things*, CRC Press, New York, USA, 2013.

[2] P. Barnaghi, W. Wang, C. Henson, K. Taylor, “Semantics for the Internet of Things: early progress and back to the future”, *International Journal on Semantic Web and Information Systems,* **8**, 1-21, 2012

[3] Martín Serrano, Payam Barnaghi and et.al, “IoT Semantic Interoperability”, *European Research Clusters*, **4**, 450-500, 2015.

[4] Lara Srivastava, “The Internet of Things: Back to the Future”, *European Commission Internet of Things Conference*, **9**, 567-620, 2011.

[5] Giancarlo Fortino and Paolo Trunfio, *Internet of Things based on Smart Objects*, Springer, New York, USA, 2014.

[6] Gartner’s hype cycle special report for 2011, Gartner Inc., 2012. http://www.gartner.com/technology/research/hype-cycles/

[7] J. C. Calbimonte, “Enabling ontology-based access to streaming data sources”, *9th International Semantic Web Conference*, **1**, 764-780, 2010.

[8] Soma Bandyopadhyay, Munmun Sengupta, Souvik Maiti and Subhajit Dutta, “ Role of Middleware for Internet of Things: A study”, *International Journal of Computer Science & Engineering Survey (IJCSES)*, **2**, 94-105, 2011.

[9] Francis daCosta, *Rethinking the Internet of Things*, Apress, California, USA, 2013.

[10] P. Parwekar, “From Internet of Things towards cloud of things”, *2nd IEEE International Conference on Computer and Communication Technology (ICCCT)*, **56**, 684-700, 2011.

[11] Adrian McEwen, Hakim Cassimally, *Designing the Internet of Things*, Wiley, 2014.

[12] Ajith Abraham, Azah Kamilah Muda, Yun-Huoy Choo, *Pattern Analysis, Intelligent Security and the Internet of Things*, Springer, 2015.

[13] Alessandro Bassi, Martin Bauer, *Enabling Things to Talk: Designing IoT solutions with the IoT Architectural Reference Model,* Springer, 2013.

[14] Anh Le Tuan, Hoan N. Mau Quoc, Martin Serrano and Et.al, “Global Sensor Modeling and Constrained Application Methods Enabling Cloud-Based Open Space Smart Services”, *IEEE 9th Intl Conference on Ubiquitous Intelligence and Computing (IEEE UIC)*, **1**, 196-203, 2012.

[15] Bennaceur, V. Issarny, R. Spalazzese, S. Tyagi, “Achieving Interoperability through Semantics-based Technologies: The Instant Messaging Case”, *Proc. of ISWC 2012 - 11th International Semantic Web Conference*, **2**, 17-33, 2012.

[16] D. Bandyopadhyay, & J. Sen, “Internet of things: Applications and challenges in technology and standardization”, *Wireless Personal Communications*, **58**, 49-69, 2011.

[17] Feng Wang, Liang Hu, Jin Zhou, and Kuo Zhao, “A Data Processing Middleware Based on SOA for the Internet of Things,” *Journal of Sensors*, **8**, 20-28, 2015.

[18] Flavia and Paulo, *Middleware Solutions for the Internet of Things*, Springer, New York, USA, 2013.

[19] G. Blair, A. Bennaceur, N. Georgantas, P. Grace, V. Issarny, V. Nundloll, M. Paolucci, “The Role of Ontologies in Emergent Middleware: Supporting Interoperability in Complex Distributed Systems”, *Proc. of 12th International Middleware Conference*, **7049**, 410-430, 2011.

[20] G. Jayavardhana, B. Rajkumar and Et.al, “Internet of Things: A Vision, Architectural Elements, and future Direction”, *Journal on Future Generation*, **64**, 456-467, 2013.

[21] Honbo Zhou, *The Internet of Things in the Cloud*, CRC Press, Florida, USA, 2013.

[22] https://en.wikipedia.org/wiki/Internet_of_things.

[23] L. Xu, W. He, and S. Li, "Internet of Things in industries: a survey," *IEEE Transactions on industrial Informatics,* **10**, 2233–2243, 2014.

[24] L.Atzori, A. Iera, G. Morabito, "The Internet of Things: A survey", Computer Networks, **54**, 2787-2805, 2010.

[25] Michael Compton, "The SSN Ontology of the Semantic Sensor Networks Incubator Group", *Journal of Web Semantics*, **17**, 2-32, 2012.

[26] Myriam Leggieri, Martin Serrano, Manfred Hauswirth, "Data Modeling for Cloud-Based Internet-of-Things Systems", *IEEE International Conference on Internet of Things*, **6**, 20-35, 2012.

[27] O. Corcho, R. Castro, "Five Challenges for the Semantic Sensor Web", *Semantic Web Journal*, **76**, 56-68, 2010.

[28] Ovidiu Vermesan, Peter Friess, *Building the Hyperconnected Society*, River Publishers Series in Communications, 2015.

[29] Ovidiu Vermesan, Peter Friess, *Converging Technologies for Smart environments and Integrated Ecosystems*, River Publishers Series in Communications, 2013.

[30] S. De, P. Barnaghi, M. Bauer, S. Meissner, "Service modelling for the Internet of Things", *in Proceedings of the Conference on Computer Science and Information Systems (FedCSIS),* **20**, 145-155, 2011.

[31] S. De, T. Elsaleh, P. Barnaghi, S. Meissner, "An Internet of Things Platform for Real-World and Digital Objects", *Journal of Scalable Computing*, **13**, 55-70, 2012.

[32] Stephan Haller, "The Things in the Internet of Things", *in Proceedings of the Internet of Things Conference*, **89**, 945-978, 2010.

[33] Subhas Chandra Mukhopadhyay, *Internet of Things: Challenges and Opportunities*, Springer, 2014.

[34] Tariq, Radouane, Hassan, "Interoperability of LoWPANs Based on the IEEE802.15.4 Standard through IPV6", *IJCSI International Journal of Computer Science*, **8**, 315-323, 2011.

[35] Omar Said, Mehedi Masud, "Towards Internet of Things: Survey and Future Vision", *International Journal of Computer Networks (IJCN),* **5**, 1-17, 2013.

[36] Minkeun Ha, Seong Hoon Kim, and et.al, "SNAIL Gateway: Dual-mode Wireless Access Points for WiFi and IP-based Wireless Sensor Networks in the Internet of Things", *The 9th Annual IEEE Consumer Communications and Networking Conference - Smart Spaces and Personal Area Networks*, **12**, 169-173, 2012.

[37] 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*, **99**, 533-545,2012.

[38] Zhanjie, Guoyuan, Keqiu, "Research on the Real-time of the Perception between Objects in Internet of Things based on Image", *The Fifth IEEE Annual China Grid Conference*, **5**, 92-97, 2012.

[39] Runian L, "Study on the Internet of Things Based on RFID Technique", Journal of CAEIT, **6**, 594-597, 2009.