ISSN (Print) : 0974-6846
Indian Journal of Science and Technology, *Vol 9(45), DOI: 10.17485/ijst/2016/v9i45/106507, December 2016* ISSN (Online) : 0974-5645

Internet of Things Architecture and Applications: A Survey

Tabassum Ara[1*], Pritam Gajkumar Shah[2] and M. Prabhakar[3]

[1]School of Engineering Science and Technology, Reva University, Bangalore – 560064, Karanataka, India; tabuara@gmail.com

[2]Department of Electronics and Communication Engineering, Jyothy Institute of Technology, Bangalore – 560082, Karanataka, India;

[3]School of Computing and Information Technology, REVA University, Bangalore – 560064, Karanataka, India;

Abstract

The Internet of Things (IoT) is a novel paradigm which is rapidly gaining ground in the scenario of modern wireless telecommunications among devices associated with Internet. **Objectives:** The main objective of this paper is to discuss the various architectures of IoT from the RFC perspective and layered approach. It also focuses on applications of IOT in various areas and analysis of security protocols of IoT for the resource constrained devices. **Method/Analysis:** In view of this, the study is carried out by systematic review of scholarly articles and research papers. **Findings:** The device can communicate with each other directly within the same network, through the cloud services or indirectly through some gateway application and even through some third party where aggregation and analysis of data can take place. When the cloud services are used to communicate, interoperability among the IP and Non-IP based devices is the major concern. In case of layered architecture the number of layers decides the complexity of the architecture. Five layered architecture is the ideal architecture from the perspective of security as well as compatibility. In all the architectures discussed it is observed that, there is a need to focus more on interoperability and standardization which is essential for the security features.

Keywords: Applications, Architecture, Internet of Things, Interoperrability, Securit, Standardization

1. Introduction

The internet of things (IoT) is an expansion of Internet where all the physical objects like home appliances, vehicles, sensors, actuators, mobile phones etc. are also gaining the ability to sense and communicate with each other without any involvement of human being[1]. Once every physical object around us is connected to the network, most elegant services in the area of health, education, agriculture, environment, business etc. can be implemented. This will have a great impact on our profession, personal and social life[2]. In IoT each object can be identified by a unique address. Objects can be managed using unique identification using Radio Frequency IDentification (RFID) and with the help of 128 bit IPv6 addressing scheme trillions of objects can have unique identification[3].

IoT devices are classified into resource constrained and resource rich devices. Resource rich devices like a smart phone, standard personal computer or a server have enough hardware, software and memory which support TCP/IP protocol, where as resource constrained devices like microcontroller based devices, sensors and actuators do not have sufficient hardware/software capabilities that support TCP/IP Protocol. Hence these devices cannot communicate with resource rich devices[4].

The remainder of this paper is organized as follows. In Section 2, applications of internet of things are summarized and in Section 3, architectural considerations are discussed.

The IoT security challenges are discussed in Section 4, and several security implementation attempts are described in Section 5 followed by the conclusion in Section 6.

* *Author for correspondence*

2. Applications of Internet of Things

Internet of things is touching every facet of our life. In Gubbi et.al.[5] have categorized the applications in to four different domains.

- Personal and home
- Enterprises
- Utilities
- Mobile

Ala Al-Fuqaha et.al.[4] has identified the applications of IoT in various areas like healthcare, transport, vehicle etc. as shown in the Figure 1. Have classified[6] the application of IoT into health care, transportation, energy, manufacturing and government domains. Heath care applications include remote patient monitoring[7].

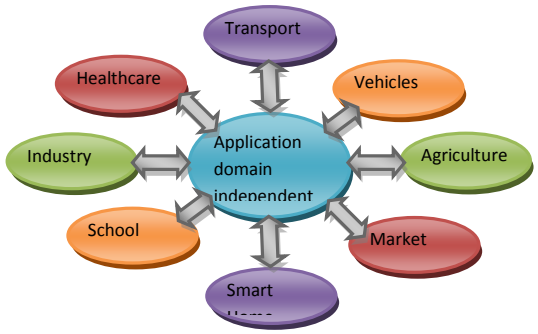

Figure 1. Applications of IoT in various areas.

The authors say, according to the eight nation's survey, more than 50 percent of the respondents are willing to embrace networked medical technology. Network medical devices are classified into four types.

- Consumer products for health monitoring
- Wearable external medical devices
- Internally embedded medical devices
- Stationary medical device.

There are many challenges with respect to these devices; protecting patient privacy and their sensitive data, intentional disruption etc.

The emerging wearable devices are one have given a different dimension to IoT. Shivayogi Hiremath et.al.[8] has proposed design, function and applications of wearable Internet of things. In the next few years it will possible to detect the diseases in their early stages, efficient treatment and remote administration. Gigli et.al.[9] has attempted to categorize IoT services into Identity-Related Services, Information Aggregation Services, Collaborative-Aware Services and Ubiquitous Services.

Li Da Xu et.al.[10] has focused mainly on industrial IoT applications. Authors have investigated applications in health care, food supply chain, safer mining production, transportation, logistics and firefighting. IoT for food chain supply has three parts; filed devices, backbone system and communication infrastructure.

Andrea Zanella et.al.[11] has attempted to analyze the solutions which are available for the implementation of urban IoT. They have given a complete overview of system architecture for an urban IoT, services with communication protocols. A brief conceptual design is given for various applications like air quality, noise monitoring, traffic congestion, city energy consumption, smart parking and smart lighting etc.

The authors[12,13] have applied IoT technology in agriculture area. IoT based monitoring system is developed to gather environmental information to increase the growth of the crop. Agricultural information cloud is implemented based on cloud computing and smart agriculture is developed by combining IOT and RFID.

J. John Livingston et.al.[14] demonstrated one of the efficient methods to acquire and monitor the environment data, where the server is connecter to Wi Fi router and sensor data is updated dynamically through WebPages.

3. Architectural Considerations

RFC 7452[15] "Architectural considerations for smart object networking" describes how resource constrained embedded devices can make use of IP based protocols. Refrigerator, car, front doors, bulbs etc have been hacked. Internet of things is becoming a playground for the hackers. Everything can be hacked if they are internet connected. To understand better the security aspects of internet of things it is important to understand the architecture of these smart objects.

3.1 RFC 7452 Describes Four Different Communication Patterns for IoT

3.1.1 Device-to-Device from Different Manufacturers within the Same Network

In general for any kind of system, the devices are manufactured by different companies. These devices are required to interoperate and communicate with each other directly. As shown in the Figure 2, in a

building network, a new light bulb/fan installed should interoperate with existing switch board of the building irrespective of the manufacturer of the bulb/fan and switch/switch board. Similarly in IoT for example, with the help of a mobile phone one should be able to monitor or control home appliances. Communication among these devices requires the different vendors to agree on the protocol stack and their design aspects like protocols, information model used, data model used to encode, IP address configuration mechanism etc.

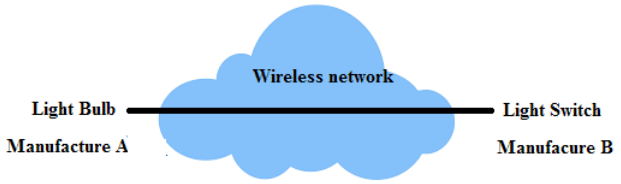

Figure 2. device to device.

3.2 Device-to-Cloud

In this pattern, devices and the cloud service both may be from the same vendor and devices upload the data to a single application service provider, where the data can be gathered and analyzed for further monitoring and control. Hence there are no issues of interoperability as shown in the Figure 3. The devices can make use of available technologies; wired or wireless technologies like TCP/IP, HTTP, and UDP etc. to connect to the network. The user may be restricted to use specific cloud service which prevents them to use alternative services. And a change in the business model makes the devices unusable. Source code for the IoT device might be available or allow installing other IoT operating system and application software.

Figure 3. Device to cloud.

This pattern is useful for the devices like television to control via a smart phone or web interfaces[16].

3.3 Device-to-Application-Layer Gateway

This pattern is quite similar to the device to cloud pattern. In device to cloud pattern, security is not considered between the devices and the cloud. In this pattern a local gateway is introduced between IoT devices and the application service provider. The communication between gateway and the cloud is through IPv4/Ipv6.

The devices uses application layer gateways to access the cloud services which requires interoperability with non-IP devices. In most these cases, smart phone acts as a local gateway device as shown in Figure 4. The phone runs an app to communicate with a device and transmit data to a cloud service. Since the application-layer gateway approach supports IPv6, complexity and cost to the development process is more.

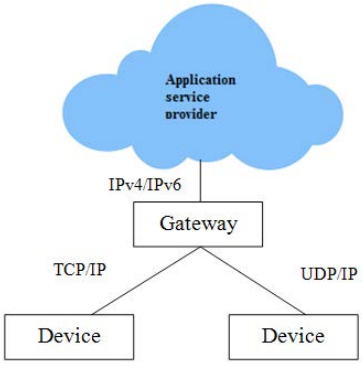

Figure 4. Device to gateway.

3.4 Back-End Data Sharing

Normally users required to export and analyze data in combination with data from other sources. This architecture supports granting access to the uploaded sensor data to third parties. It allows the data collected from single IoT device to be aggregated and analyzed.

Organizes[17,18] IoT architecture into three different layers; Perception layer, network layer and application layer as shown in Figure 5. Perception layer deals with physical devices. Network layer collects data from these devices and transmit to the application layer, where all the processing and decision making takes place.

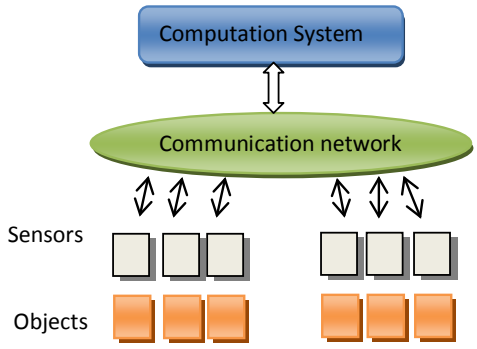

Figure 5. Basic IoT architecture.

Describes[19] the architecture in terms of four major layers where data is collected from sensors and the same is relayed with the help of communication layer. Computation layer process and analyze the data and actions taken by the top most layer called service layer. Miao, Wu et.al.[20] suggested five layer architecture of Internet of Things since with the help of three/four layer structure all the features of IoT can't be expressed. According to Paul Fremantle et.al.[21] reference architecture of IoT consists of five layers as shown in the Figure 6.

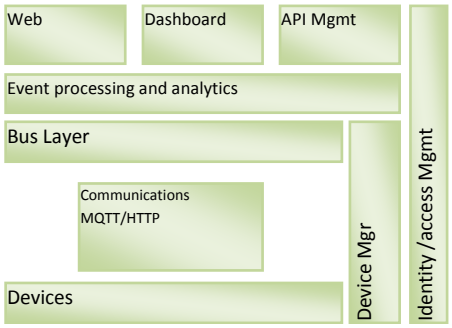

Figure 6. Reference Architecture of IoT.

The Device layer which may include: Arduino, Raspberry Pi, ZigBee and Bluetooth etc. Every device will have its own UUID. Communication layer supports the connectivity of these devices. The layer includes protocols like http/https and MQTT

Aggregation layer aggregates and combine communications from different devices and to route communications to a specific device Analytical layer stores data into database, takes the events from the aggregation layer to process and act upon the events. Client layer provides a way for the devices to communicate with outside world.

International Telecommunication Union (ITU)[22] recommends that architecture of Internet of Things may consists of five layers; Sensing Layer, Access Layer, Network Layer, Middleware Layer and the Application Layer.

Rafiullah Khan et.al.[23] describes the architecture of IoT as combination of five different layers as shown in Figure 7; perception layer which deals with physical objects. It identifies and collects the object specific information like location, temperature, motion etc and is passed to transmission layer. Transmission layer comprises a wired or wireless with different technologies like Wifi, Bluetooth ZigBee etc. This layer is responsible for secure transmission of physical object data to processing system on middleware layer.

Middleware layer stores the data in database, performs information processing and based the result it takes required decision.

Application layer deals with the management of application like smart home, smart city etc. The top most layer business layer responsible for the analysis and it determines the future actions.

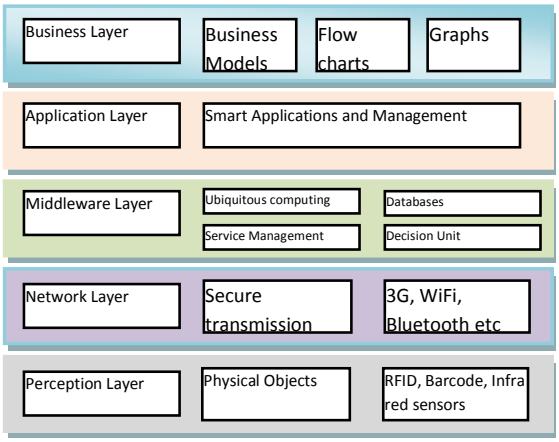

Figure 7. Five Layered architecture of IoT.

Indu Bala Thingam[24] has proposed six layer architecture as shown in the Figure 8. In addition to sensing layer, networking layer, service and Business layer, two more layers MAC layers and processing and storage layer have been introduced. Since most of the IoT devices are resource constrained in nature, MAC layer takes care of device monitoring and control. It makes the devices to sleep in their idle time to save the energy. The processing and storage layer is responsible for query processing, analysis and storage, and security.

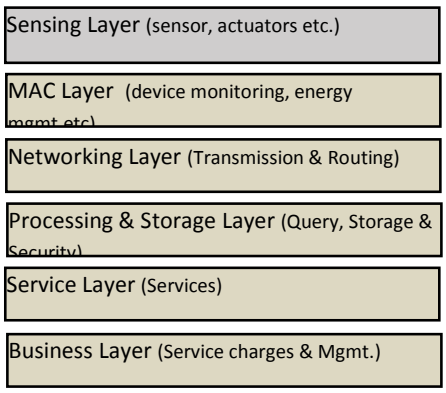

Figure 8. Six layered architecture of IoT.

4. IoT Security Challenges

Sathish Kumar et.al.[25] has identified security concern in IoT in terms of front end sensors and equipments, network and back end of IoT systems. And privacy concern at device, processing and communication level. Identifies[2] three main key challenge areas like privacy, Identity Management, Security, Access control Standardization and Interoperability and data deluge: they conclude that trust and privacy are likely to be the major hurdles in IoT uptake. Authors[18] discuss the challenges in each layer. In future the number of devices connected will be much more than the human beings, hence security and privacy issues grow more.

Have[26] reviewed security threats for RFID based IoT system. The authors have classified into two categories;

RFID system threats, which includes abuse of tags, reader risks and personal privacy leak. And communication security threats like wired and wireless communication risk and denial of services. Few counter measures with respect to authentication and the security of RFID are also discussed, which includes tag killing, tag sleeping and blocking of tags. The authors[27] have identified various security challenges including authentication, authorization, encryption and cache poisoning etc. they have pointed out that IoT naming and discovery techniques may be enhanced with security schemes to address these challenges.

Shivayogi Hiremath et.al.[8] have pointed out that wearable IoT collects sensitive information like location and movement activities which compromises the privacy of the user. This requires strong security infrastructure. Jason Healey[7] has pointed out those human internally embedded medical devices like pacemaker which can be communicated from outside world using wireless protocols or Bluetooth. These kinds of devices require more security since it is literally embedded internet into human lives.

Raza Shahid[28] have pointed out some open security issues and challenges in the IoT which includes Certificate based mutual authentication using public key cryptography, secure bootstrapping of things, security and privacy of sensor data in the cloud environment etc.

The authors have proposed use of IPsec and DTLS for secure communication in the IoT, they have proposed and developed lightweight IDS for 6LoWPAN networks that use RPL as routing protocol in the IoT.

5. Security Implementation Attempts

Sachin Babar et.al.[29] has proposed a cube structure as a modeling mechanism for security, trust and privacy in the IoT. This structure has three dimensions; security, trust and privacy for the IoT as shown in Figure 9.

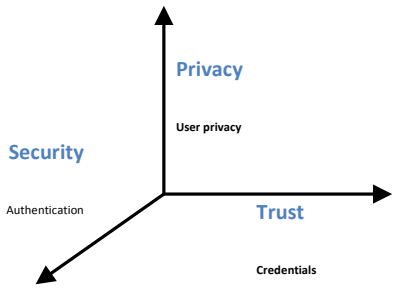

Figure 9. Security Model for IoT.

Shivraj VL, et.al. have proposed[30] OTP scheme based on identity based elliptic curve. Where hash function is replaced by a new function which is based on Identity Based Encryption (IBE) scheme. In this function the secret key of the device is taken as initial torsion group point and x component of this point and the time is considered to determine a new torsion point. This process is repeated desired number of times. This scheme requires fewer resources for the operations, since the keys are not stored.

Elliptic Curve Cryptography (ECC) has much more benefits in public key cryptosystems which are small key length, lower consumption power, faster computation, and small bandwidth. Pinol et.al.[31] have implemented a light weight cryptography model for resource constrained IoT using ECC for Contiki OS. A mathematical model is developed in which all the primitive functions of ECC are implemented. The authors have evaluated that Jacobian coordinate system is the better choice with respect to the improvement in performance.

IoT interconnects heterogeneous devices manufactured by various companies. Marin et.al.[32] have proposed a novel key negotiation protocol where elliptic curve cryptographic algorithm is used with 32 bit processor; NXP/Jennic 5148- and 16 bit processor; MSP430-based IoT devices as shown in the Figure 10.

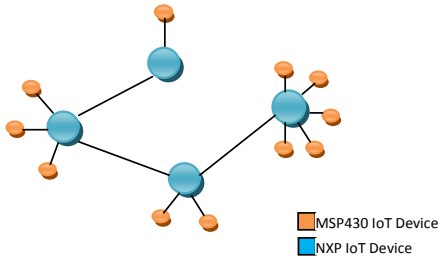

Figure 10. Start topology.

The protocol uses twisted Edwards curve, which is a projective curve given by the equation $ax^2+y^2=1+dx^2y^2$ where 'a' and 'd' are parameters of the curve.

Antonio et al. have proposed a distributed capability-based access control mechanism which is built on asymmetric key cryptography as shown in Figure 11.

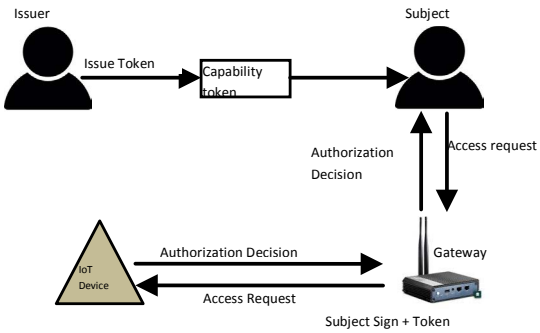

Figure 11. Access control mechanism.

The issuer issues a capability token to the subject to access the device. This token is signed by the issuer using ECDSA. With the help of this token the subject generates and sends a CoAP request the device. The device checks the validity of the token and verifies the signature and then it generates the CoAP response and sends it to the subject. The protocol is tested on JN5139 mote equipped with Contiki OS. And the evaluation results says, the total time taken is only 480.96 ms which includes, validation of issuer signature, subject signature and the other processing.

6. Conclusion

The IoT embraces the guarantee of improving human lives through amplification and automation. The facility offered by the IoT can make our life simple and comfortable. It also helps to improve decision making and outcomes in a various application areas like medical, manufacturing, transportation, education etc. The key observations in the literature are interoperability, security for IP based and non-IP based device, building standard protocols and universal architecture which can support the heterogeneity of the device. Standardization at the architectural level and interoperability is required, since every vendor is using different technology. However by integrating various existing technologies together in a novel way, the IoT has the high potential to reshape human life.

7. References

1. Luigi Atzori AI, Giacomo Morabito. The Internet of Things: A Survey. Comput. Netw. 2010; 54(15);2787–805.
2. Coetzee LE. The Internet of Things - Promise for the Future? An Introduction, IST-Africa Conference Proceedings, 2011.
3. Sarita Agrawal MLD. Internet of Things – A Paradigm Shift of Future Internet Applications, International Conference on Current Trends in Technology, 2 Nuicone, 2011.
4. Al-Fuqaha AG, Mohammadi M. Aledhari M, Ayyash M. Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications, Communications Surveys and Tutorials, IEEE, 2015; 17(4):2347–76.
5. Gubbi J, et.al. Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions, Future Generation Computer Systems. 2013; 29(7):1645–60.
6. Realizing the Potential of the Internet of Things. Tele-communications Industry Association, 2015.
7. Jason Healey NP, Beau Woods. The Healthcare Internet of Things -Rewards and Risks, Intel Security, 2015.
8. Shivayogi Hiremath, Geng Yang, Kunal Mankodiya. Wearable Internet of Things, in International Conference on Wireless Mobile Communication and Healthcare. 2014.
9. Gigli MK, Simon. Internet of Things: Services and Applications Categorization, Advances in Internet of Things. 2011; 1(02):27.
10. Da Xu L, He W, Li S. Internet of Things in Industries: A Survey, Industrial Informatics, IEEE Transactions. 2014; 10(4):2233–43.
11. Zanella A, et.al. Internet of Things for Smart Cities, Internet of Things Journal, IEEE. 2014; 1(1):22–32.
12. Yoe MLJHH. Agricultural Production System Based on IoT. In: Computational Science and Engineering (CSE), 2013 IEEE 16th International Conference, 2013.
13. Ma J, et.al. Connecting Agriculture to the Internet of Things Through Sensor Networks. In: Internet of Things (iThings/CPSCom), 2011 International Conference on and 4th International Conference on Cyber, Physical and Social Computing, 2011.
14. Livingston J John, Umamakeswari A. Internet of Things Application using IP-Enabled Sensor Node and Web Server, Indian Journal of Science and Technology. 2015; 8.S9:207–12.

15. Tschofenig H, et.al. Architectural Considerations in Smart Object Networking, Tech. No. RFC 7452, Internet Architecture Board, 2015. https://www.rfc-editor.org/rfc/rfc7452.txt.
16. Samsung Privacy Policy—Smart TV Supplement, Samsung Corp. Web, 2015. http://www.samsung.com/sg/info/privacy/smarttv.html.
17. Zhihong Y, et.al. Study and Application on the Architecture and Key Technologies for IOT. In: Multimedia Technology (ICMT), 2011 International Conference, 2011.
18. Xiaobin H. Application and Practice on the Internet of Things, Information Construction, 2009, p. 21-22.
19. Chen Y-K. Challenges and Opportunities of Internet of Things. In: Design Automation Conference (ASP-DAC), 2012 17th Asia and South Pacific, 2012. IEEE.
20. Miao W, et.al. Research on The Architecture of Internet of Things. In: Advanced Computer Theory and Engineering (ICACTE), 2010 3rd International Conference on, 2010.
21. Fremantle Paul. A Reference Architecture for the Internet of Things, 2015.
22. Somayya Madakam R, Ramaswamy, Siddharth Tripathi. Internet of Things (IoT): A Literature Review. SciRes, 2015.
23. Rafiullah Khan SUK, Rifaqat Zaheer, Shahid Khan. Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges, 10th International Conference on Frontiers of Information Technology, 2012.
24. Thingom IB. Internet of Things: Design of a New Layered Architecture and Study of Some Existing Issues, IOSR Journal of Computer Engineering (IOSR-JCE), 2015.
25. Kumar JS, Patel DR. A Survey on Internet of Things: Security and Privacy Issues, International Journal of Computer Applications. 2014; 90(11).
26. Nie Xiao, Zhong Xiong. Security in the Internet of Things Based on RFID: Issues and Current Countermeasures 2013, In: Proceedings of the 2nd International Conference on Computer Science and Electronics Engineering, Atlantis Press, 2013.
27. Claudio Pastrone DR. Internet of Things. EU-China Joint White Paper on Internet-of-Things Identification, 2014.
28. Raza S. Lightweight Security Solutions for the Internet of Things, Mälardalen University, Västerås, Sweden, 2013.
29. Babar S, et.al. Proposed Security Model and Threat Taxonomy for the Internet of Things (IoT), In: Recent Trends in Network Security and Applications. 2010, Springer. p. 420–29.
30. Shivraj Rajan VL, Singh MA, Balamuralidhar M. One Time Password Authentication Scheme Based on Elliptic Curves for Internet of Things (IoT). In Information Technology: Towards New Smart World (NSITNSW), 5th National Symposium, 2015.
31. Pinol OP, et.al. BSD-Based Elliptic Curve Cryptography for the Open Internet of Things. In: New Technologies, Mobility and Security (NTMS), 2015, 7th International Conference, 2015.
32. Marin L, Piotr Pawlowski M, Jara A. Optimized ECC Implementation for Secure Communication between Heterogeneous IoT Devices, Sensors (Basel, Switzerland). 2015; 15(9):21478–99.