Towards a Light Weight Internet of Things Platform Architecture

A. Sivabalan[1], M. A. Rajan[2] and P. Balamuralidhar[2]

[1]*NEC India Pvt Ltd,Chennai, India; e-mail: sivabalan.arumugam@necindia.in*
[2]*Tata Consultancy Service, Bangalore, India; e-mail: rajan.ma@tcs.com, balamurali.p@tcs.com*

Received July 2013; Accepted August 2013

Abstract

This paper provides an overview of the activities of Internet of Things (IoT) work group in Global ICT Standardisation Forum for India (GISFI). Objective of this IoT WG is to identify potential standardization areas that can help proliferating the IoT technology and its applications that are relevant to India for the benefit of the society and businesses. The strategy chosen within this WG is to develop application independent generic IoT Framework with well-defined Reference Architecture to achieve interoperability between the various devices/application developed in multi-vendor scenario to achieve cost advantage and pass this advantage to the user group for its mass scale deployment and applicability. The requirements of the same are gathered through the study of various use cases.

Keywords: Internet of Things, Machine to Machine Communications, Service Platform.

1 Introduction

The Internet and World-Wide Web (www) has been a major driver of globalization and has promoted the convergence of electronic communications

Journal of ICT Standardization, Vol. 1, 241–252.
doi:10.13052/jicts2245-800X.12a8

and media services. Internet is continuing to become more pervasive, with the advent of low cost wireless broadband connectivity, by connecting to new embedded devices and handhelds. Further this evolution will continue to emerge as an "Internet of Things (IoT)" where the web will provide a medium for physical world objects to take part in interaction. This way the digital information technology can integrate the physical world to the online world to provide a common interaction platform.

IoT can be viewed as a global infrastructure for the information society, by interconnecting (physical and virtual) things based on, interoperable information and communication technologies towards providing advanced information services. Efficient exploitation of identification, data capture, processing and communication capabilities are integral requirements of IoT.

IoT is an integrated part of the future Internet that could be defined as a dynamic global network infrastructure with self-configuring capabilities linking physical and virtual objects through the exploitation of data capture and standard and inter-operable communication protocols.

This infrastructure includes existing and evolving Internet and will offer specific object-identification and addressing, sensor and connection capability as the basis for the development of independent and/or federated services and applications.

IoT promises to bring smart devices everywhere, from the fridge in your home, to sensors in your car; even in your body. Those applications offer significant benefits: helping users save energy, enhance comfort, get better healthcare and increased independence: in short meaning happier, healthier lives. But they also collect huge amounts of data, raising privacy and identity issues. For IoT to take off people need to feel a degree of comfort and control, and business need stability and predictability to invest. Therefore the issue of ethics and understanding needs, concerns and desires of people and businesses is so important.

These will be characterized by a high degree of autonomous data capture, context and event detection and transfer, network connectivity and interoperability at the protocol and semantic level with the provision of handling security and privacy concerns of the users and the data being communicated.

This paper presents the context and summary of activities in the IoT WG of GISFI highlighting some of the key contributions towards conceptualizing a light-weight service platform architecture. Section 2, discuss the background and scope of IoT WG activities. Section 3, summarizes major achievements of the IoT WG so far. Detailed discussion on GISFI IoT Baseline Light weight Architecture is presented in section 4. This is followed by a summary of a proposal for IoT Security in section 5. Last section briefly outline the planned scheme of future activities of the IoT WG.

2 Background and Scope

2.1 Background Information

As one of the fastest growth market for cellular technologies, India hasdemonstrated its appetite for technologies to revolutionize the life across all its diversity. The value, impact on daily life, and competition has helped the cell phone to reach the masses across all strata of the society.Urbanization of India is happening at a rapid pace. Migration from rural places to cities is ever increasing. One way to address this is to enhance the opportunities at villages to reduce the overburdening of the cities. Experience shows that this is not that easy. We need scalable architectures and funding models for building the city infrastructures to handle large populations.

Need and Challenges of IoT in India

There is a requirement for efficient systems for transportation, utilities, healthcare, safety & security, education, environment, governance and entertainment.Deployment of advanced ICT technologies would be affordable and cost effective considering the improved quality of life of citizens and enhanced GDP growth from the resultant productivity improvements.

A large percentage of Indian population is in rural are as and there is a constant drive for addressing those sections of the society. Majority of themanpower is spent on agriculture and farming. Many cases they are resource-constrained in terms of water, energy, fertilizers, and market opportunities.

Systems for monitoring and improving the efficiency of resource utilizationwill be highly beneficial. Health care is another area of attention here where remote monitoring can enable the skilled doctors in cities to extend their services to villages.

There are many challenges for successful adoption of IoT in India.

Scalability: As the size of the systems tends to be large in size, the solutions should be scalable. Also many times the deployments happen in stages and the architecture should be able to scale-up incrementallywithout taking too much overhead.

Affordability of products and services: Affordability is one of the major aspect for success. It may not be low cost always, but the right cost for a specified target group with a clear business case or cost benefit. Standardized platforms, tools and manufacturing processes can bring thecost down with increased volumes.

Integration with Legacy systems: Since there are no widely deployed IoT applications, there may not be any major challenge with legacytechnologies in that space. However there may be legacy devices andsystems which are not amenable for new standardization and need to coexist.

Robustness: While there is a pressure for low cost, there is a strong demand for robustness and reliability of products and services. One of the approaches for addressing this is to build upgradable/disposable systemswhich take care of current requirements and strip of the low priority features to reduce cost. A Robust solution will get a buy-in even if it isless sophisticated.

Social and Cultural Sensitivity: Social response to an IoT application has many aspects. It can have cultural, linguistic, geographic, political dependencies for the acceptance. Help of awareness and regulations areto be explored for the success of large scale social applications

Over the last three years, the IoT WG along with stakeholders has put forth significant efforts to carry out detailed study of the IoT/ Machine to Machine (M2M) standards landscape,regulations and Indian needs on IoT. Major participating industrial organizations in this work group include Tata Consultancy Services (TCS),NEC, Ericsson, Cisco, I2TB-SPPL, Wirefreecom, ILS Technologies andOPC Foundation. TCS holds the current chair of the workgroup and Ericsson is the Vice Chair. There have been more than thirteen WG meetings till date [13].

2.2 Scope and Objectives

Objective of this IoT WG is to identify potential standardization areas that can help prolife rating the IoT technology and its applications that are relevant to India for the benefit of the society and businesses.

The strategy chosen within IoT Working Group of GISFI is to develop application independent Generic IoT Framework with well-defined Reference Architecture to achieve interoperability between the various devices/ application developed in multi-vendor scenario to achieve cost advantage-and pass this advantage to the user group for its mass scale deployment and applicability.

The examples of such IoT applications include: fleet management, smart metering, home automation, e-health, e-agriculture, smart cities, smart manufacturing,environment and natural resources management etc.

3 IoT WG Achievements

Achievements of IoT WG so far are in the following aspects:

- Study of the requirements of IoT for use cases that are relevant to India.These studies resulted into a number of technical reports.
- Reference Architecture for IoT for organizing and synergizing various-standardization requirements of IoT.
- A light weight security scheme for IoT applications

3.1 Use case scenarios presented

There are several use case scenarios presented in workgroup that motivates the requirement of a common standard across multiple application domains,with relevance to India. These use cases were submitted by different participants and some of the major ones are:

(i) Agriculture monitoring [1]
(ii) mHealth [7,11], Connected Health Care [3,4]
(iii) Landslide detection [6]
(iv) Food Supply Chain Management [8]
(v) Security,Surveillance [9]
(vi) Smart metering and control [10]
(vii) Smart Cities [12]

4 GISFI IoT Baseline Light weight Architecture

In this section, we present more details on a reference architecture for IoT which discusses a functional architecture of the IoT stack [2]. The scope of the architecture is from sensors/devices to applications. The IoT stack is expected to capture the heterogeneity of devices and communication protocolsat the lower layer and to provide uniform interfaces to the upper layers.

Objectives of formulating reference architecture are multi-fold and are explained as follows:

- It identifies major reference points / interface points which can be considered for standardization to encourage interoperability of products and-services from multiple stake holders.
- It helps in explaining various IoT use case scenarios and gathering respective requirements of these interfaces

- Developing consistency in information exchange and contributions frommultiple participants of this standards development effort

4.1 Requirements

The reference architecture should be able to identify key architectural components and interfaces so that multiple stake holders providing products and there are several legacy devices, technologies and standards existing at thelower layer of TCP/IP layering in the immediate vicinity of objects and devices. The architecture should support them optimally.

In addition to the above requirements, some of the India specific requirements that need to be considered are discussed below.

India has a huge population with diversity in terms of geography, culture and other socio-economic factors. The architecture should support the IoT services that can scale, at the same time support multiple levels of sophistication in terms of technologies and devices coexisting.Even within a single application domain such diversity needs are to be supported.

The nationwide coverage of candidate networks for IoT Core connectivityis not uniform, rather patchy. This unreliability in communication needs to be taken into account and suitable measures for robustness of IoT connectivity needs to be incorporated. Moreover the large numberof IoT devices can lead to unexpected peak requirements and that may bring down the network due to congestion and limited capacity.This requires advanced management techniques for the IoT network and services.

Affordability of IoT services is an important aspect where low cost technologies should form the part of the baseline services. In certain large scaleapplications, massive deployment of sensing devices may not be feasible dueto cost considerations.

In consideration with such scenarios a human enabled sensing mechanism is included in this scope where a device such as mobile phone carried by a person is used for communication with objects/persons and integrate with the IoT services. Further the architecture should enable thereduction of cost of intellectual properties and encourage IPR development and competition in the country towards better control of affordable services.

4.2 IoT Architecture

The scope of the reference architecture discussed here (refer Fig. 1) includes the entire cycle of IoT applications, from sensing to application services [2].

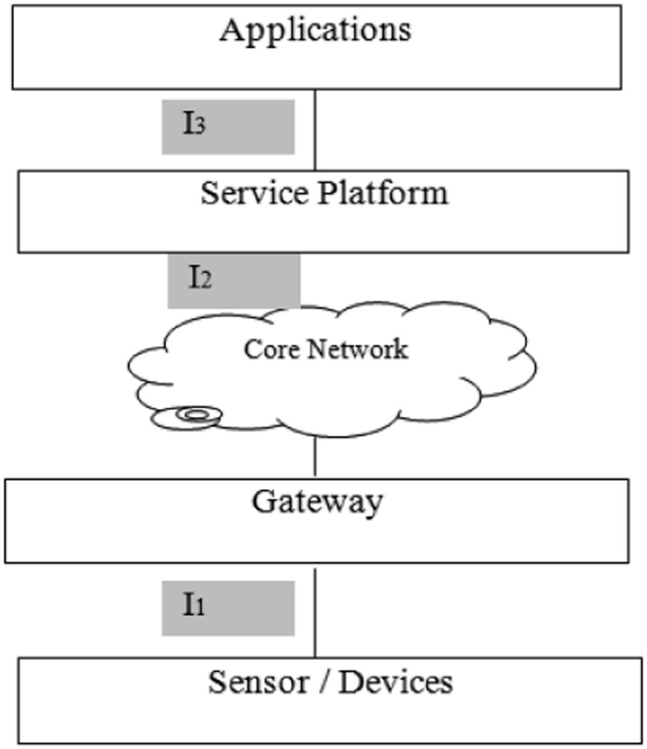

Figure 1 IoT reference architecture.

It is partitioned into three layers namely Device layer, Gateway layer, and Service Platform layer. This paper also discusses issues involving IoT core network asfollows.

IoT Device Layer: IoT devices are included in this layer. This layer consists of individual sensors, network enabled objects and capillary networks consisting of datasources that are near to the physical environment. It includes heterogeneous devices (including sensors and actuators) supporting diverse communication standards such as Zigbee, ZWave, ANTS and Wi-Fi, etc.

IoT Gateway Layer: This layer consists of IoT gateways. The substantial heterogeneity of devices and technologies hosted by the device layer is abstracted using gateways that can provide a more uniform interface to IoT service platform layer. It is also possible that a capable device can implement both IoT device andgateway layer/functionality into a single physical entity and connects to the IoT service platform layer through the core network

IoT Service Platform Layer: This defines and provides different IoT service abstractions that can be used by multiple applications. There can be a set of platform services from the IoT platform infrastructure. Further the same framework can be extended to application services where some of the reusable application components are available as services.

IoT Core Network: The physical entities involved in the above three layers need suitable communication infrastructure for information exchange. While the device layer addresses this requirement using various legacy technologies which are outof scope for this paper, the gateway layer and service platform layer are expected to be connected over an IoT Core / Backbone network. The IoT Coreis envisaged to be predominantly an IP based network and that is in line with the vision of IoT. This IP connectivity could be supported over multitudes oftelecommunication infrastructures such as DSL, Cellular networks (2G, 3G, 4G) etc.

4.3 Interface Reference Points

Further to the identification of major domains we identify three reference points at the interfaces of these layers. They are

I1: Interface from device layer to gateway layer,
I2: Interface from gateway layer to service platform layer through IoT core network
I3: Interface from service platform to layer specific vertical applications

Each of these interface points will benefit from a standardized information exchange because of the diversity of devices, manufacturers, serviceproviders, and service consumers involved. Each of these interface points are expected to support a set of specialized capabilities which may form aset of standardized adapters designed for the purpose. These adapters may implement existing protocols or needs new developments or extension based on the requirements gathered from various IoT use cases.

5 IoT Security

For secure communication and authentication between the devices, cryptography is an essential tool. In general, cryptography with PKI is very popular, wherein the certificates containing the public and private keys are issued to the users and users using these keys encrypt and decrypt their data and thus security is enabled. The same scheme is not viable for IoT scenario. The crypto system for IoT security has the following requirements. The requirements are broadly classified into two categories to ensure Confidentiality, Integrity and Availability.

- Communication Security.
- Storage Security.

5.1 Communication Security

The communication security deals to handle the security for the IoT communications. It has following requirements:

- Secure Device to Device Communication: Here the cryptographic technique should enable secure IoT communication across I1, I2 and I3 interfaces. The cryptographic technique should be lightweight.
- No Public Key Infrastructure (PKI):Number of devices in IoT is very large, maintaining keys at PKI is not feasible. So cryptographic technique with no PKI is very essential
- Certificate less cryptography: IoT demands less infrastructure for security, hence the requirement here is to design crypto systems with no certificates.
- No Key Exchange: One of goal of IoT is to reduce number of control/communication messages. This is relevant to secure communications also. Since device to device communications in IoT are very prevalent, to minimize the message overheads, crypto system should support no key exchanges.
- Anonymity: In IoT, prominently in the area of disaster management/mission critical operations, to avoid attacks from the intruders, anonymity is required. So it is desirable that crypto system should support security as well as anonymity also.
- Variable security requirement: Handling of heterogeneous devices with differing protocols.
- Group Communication: In IoT, very often the Application (layer 4) requires data from different devices and also need to control them

5.2 Storage Security

IoT is poised to be the largest source of data generator from a wide range of diversified applications. How to store and archive the data at devices, platform, and service providers robustly is a big challenge. Thusdata should be delivered or distributed to the intended users/applications only in a secured and anonymized way to satisfy privacy requirements. Therefore it is desirable to have a lightweight crypto system for secure collection, storage, and archive and distribution of data.

Hence a scalable, lightweight, with no infrastructure, certificate less and no key exchange cryptographic technique is essential for secure IoT communication. Thus using IBE, we can envisage the requirements of the secure communication for IoT.

5.3 Applicability of Identity based Encryption for IoT

Identity based Encryption (IBE) is a secure certificate-less cryptography scheme, wherein the devices can generate the public key of the other devices by using publicly known identity of the devices such as device's, owner's id, mac-id, etc. and encrypt the message with this public key and on the other hand the device which receives the encrypted message shall decrypt the message using its' private key (obtained during device registration/bootstrapping in IoT).Key revocation is an issue in IBE that needs to be addressed. The techniques such as Lattice based IBE and Attribute Based IBE schemes to enable key revocation.

There are a few IBE based standards which are still evolving. IEEE has a draft standard on IBE cryptography IEEE P1363, which is very generic and not specific to IoT/M2M communication.

For M2M and IoT, the existing schemes proposed by EuropeanTelecommunications Standards Institute (ETSI) based on IBE are through key exchange algorithms (Diffie–Hellman algorithm) and authentication using IBAKE algorithm and uses Weil paring in cryptography. The proposal made in the Working Group (WG) is to use IBE cryptographic schemes with or without key exchanges along with anonymity, authentication and signature schemes.

6 Going Forward

Elaboration of the interfaces specified in the GISFI IoT reference architecture that addresses the major requirements of various use-case scenarios is the work in progress in the work group. The specification is oriented towards the specification of a Light Weight IoT/M2M Framework with a focus on the impact use cases relevant to India. It requires the identification of baseline requirements those are categorized into mandatory, desirable, and optional.The inputs for requirements are sourced from various GISFI documents (use case scenarios, framework document), and international standards such as ETSI. This selection need to be guided by the India specific challenges.

References

[1] GISFI_IoT_20110680, “Agriculture Application Requirements”, June 2011

[2] GISFI_IoT_201206218, “Internet of Things Reference Architecture”, June 2012.

[3] GISFI_IoT_201206221, “Indian relevance to Healthcare Service Delivery mechanism based on Generic IoT Framework”, June 2012

[4] GISFI_IoT_201206222, “Healthcare Service Delivery mechanism based on Generic IOT Framework”, June 2012.

[5] GISFI_IoT_201206227, “IoT Service Capabilities”, June 2012

[6] GISFI_IoT_201206228, “Landslide Detection Use-case”, June 2012

[7] GISFI_IoT_201203179, “mHealth Use Cases”, March 2012.

[8] GISFI_IoT_201203180, “Food Supply Chain Management (FSCM) Use Cases”, March 2012.

[9] GISFI_IoT_201203181, “Surveillance Security System Use cases”, March 2012.

[10] GISFI_IoT_20110677, “Privacy Requirements of User Data in Smart Grids”, June 2011

[11] GISFI_IoT_20110687, “Frame-work Document for TR on e-Health Use Case”, June 2011

[12] GISFI_IoT_201209291, “Smart City Usecase”, Sep 2012.

[13] GISFI_IoT_201212335, “Security Requirements and Proposal for IoT”, Dec 2012.[13] GISFI Meeting Documents: IoT URL: http://gisfi.org/workinggroups.php?wg=IOT [Last accessed: 12th August, 2013]

Biographies

Sivabalan A is working as a Manager – Research in NEC Mobile network Excellence Centre(NMEC), at NEC India Pvt Ltd, Chennai India. He has 13 years of experience in Industrial and academic research. Prior to NEC, he was the Associate Scientist in Industrial Communication Research Group, INCRC at ABB Global Services and Industries Limited, Bangalore, India. He received Ph.D in Electrical Engineering from Indian Institute of Technology, Kanpur (IITK) and also carried-out Postdoctoral research with Physical and Digital Realisation Research Group at Applied Technology Research Centre, Motorola India Research Lab, Bangalore India. He has around 30 Journals and International Conferences publications.His current role includes representing NEC in Global ICT Standards forum of India (GISFI). He research interest includes Free space Optical Communication, 802.xx Physical Layer, Device communication and Integration.

Rajan M A, who obtained B.E., M.Tech.and PhD Degrees in Computer Science and Engineering and Mathematics, M.Sc., M.Phil in Mathematics. He, is currently employed as a Scientist at TCS Innovation Labs, Bengaluru. He also worked as a Scientist in Indian Space Research organization from December 2000 to September 2005 and was actively involved in realization of several spacecrafts.. Apart from industrial experience he is also working as a visiting academic faculty in SJCIT, Chikkaballapur and also in UVCE, Bengaluru for over 12 years. In an overall he is having 13+ years of both industry and academic experience in the field of computer science and engineering. His research activities involves Cryptography, information security, Privacy preserving techniques, Computer Networks, Cross layer design, Number Theory, Graph Theory, Combinatorics, coding theory and Functional Analysis. He has National and International patents and also published several research papers in national and international conferences and journals.

Balamuralidhar P is a Principal Scientist and Head of TCS Innovation Lab at Tata Consultancy Services Ltd (TCS), Bangalore. He has obtained Bachelor of Technology from Kerala University and Master of Technology (MTech) from IIT Kanpur. His PhD is from Aalborg University, Denmark in the area of Cognitive Wireless Networks. Major areas of current research include different aspects of Cyber Physical Systems, Sensor Informatics and Networked Embedded Systems. Before TCS his research careers were with Society for Applied Microwave Electronics Engineering & Research (SAMEER) Mumbai and Sasken Communications Ltd Bangalore.

He has over 25 years of research and development experience in Signal Processing, Embedded Systems and Wireless Communications. He has over 60 publications in various international journals and conferences and over 20 patent applications. Balamuralidhar was the leading TCS participation in two EU FP6 research consortium projects namely My Adaptive Global NET (MAGNET) and End to End Reconfigurability (E2R) in the area of next generation wireless communications. He is also contributing to TCS participation in National bodies like Broadband Wireless Consortium India (BWCI), Global ICT Standards for India (GISFI). In GISFI he is chairing the Internet of Things Workgroup.